APPENDIX 1B
OF THE ANNEX TO THE AETR

REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION, AND INSPECTION OF THE DIGITAL CONTROL DEVICE USED IN ROAD TRANSPORT

(Consolidated version)

CONTENTS

CONTENTS (continued)

PAGE

CONTENTS (continued)

CONTENTS (continued)

SUB-APPENDIXES

I. DEFINITIONS

In this Appendix:

a) "activation" means:

phase where the control device becomes fully operational and implements all functions, including security functions;

Activating a control device requires the use of a workshop card and the entry of its PIN code.

b) "authentication" means:

A function intended to establish and verify a claimed identity;

c) "authenticity" means:

The property that an information is coming from a party whose identity can be verified;

d) "built-in-test (BIT)" means:

Tests run at request, triggered by the operator or by an external equipment;

e) "calendar day" means:

a day ranging from 00.00 hours to 24.00 hours. All calendar days relate to UTC time (Universal Time Co-ordinated);

f) "calibration" means:

updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Contracting Party) and vehicle characteristics (w, k, l, tyre size, speed limiting device setting (if applicable), current UTC time, current odometer value);

Calibrating a control device requires the use of a workshop card.

g) "card number" means:

a 16 alpha-numerical characters number that uniquely identifies a tachograph card within a Contracting Party. The card number includes a consecutive index (if applicable), a replacement index and a renewal index;

A card is therefore uniquely identified by the code of the issuing Contracting Party and the card number.

h) "card consecutive index" means:

the 14th alpha-numerical character of a card number that is used to differentiate the different cards issued to a company or a body entitled to be issued several tachograph cards. The company or the body is uniquely identified by the 13 first characters of the card number;

i) **"card renewal index" means:**

the 16th alpha-numerical character of a card number which is incremented each time a tachograph card is renewed;

j) **"card replacement index" means:**

the 15th alpha-numerical character of a card number which is incremented each time a tachograph card is replaced;

k) **"characteristic coefficient of the vehicle" means:**

the numerical characteristic giving the value of the output signal emitted by the part of the vehicle linking it with the control device (gearbox output shaft or axle) while the vehicle travels a distance of one kilometre under standard test conditions (see Chapter VI.-5.). The characteristic coefficient is expressed in impulses per kilometre (w = ... imp/km);

l) **"company card" means:**

a tachograph card issued by the authorities of a Contracting Party to the owner or holder of vehicles fitted with control devices

The company card identifies the company and allows for displaying, downloading and printing of the data stored in the control device which has been locked by this company.

m) **"constant of the control device" means:**

the numerical characteristic giving the value of the input signal required to show and record a distance travelled of one kilometre; this constant shall be expressed in impulses per kilometre (k = ... imp/km);

n) **"continuous driving time" is computed within the control device as**[1] the continuous driving time is computed as the current accumulated driving times of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN[2] period of 45 minutes or more (this period may have been split in several periods of 15 minutes or more). The computations involved take into account, as needed, past activities stored on the driver card. When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot;

o) **"control card" means:**

a tachograph card issued by the authorities of a Contracting Party to a national competent control authority;

The control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading.

---

[1] This way of computing the continuous driving time and the cumulative break time serves into the control device for computing the continuous driving time warning. It does not prejudge the legal interpretation to be made of these times.

[2] UNKNOWN periods correspond to periods where the driver's card was not inserted in a control device and for which no manual entry of driver activities was made.

p) "cumulative break time" is computed within the control device as:

the cumulative break from driving time is computed as the current accumulated AVAILABILITY or BREAK/REST or UNKNOWN[2] times of 15 minutes or more of a particular driver, since the end of his last AVAILABILITY or BREAK/REST or UNKNOWN[2] period of 45 minutes or more(this period may have been split in several periods of 15 minutes or more).

The computations involved take into account, as needed, past activities stored on the driver card. Unknown periods of negative duration (start of unknown period > end of unknown period) due to time overlaps between two different control devices, are not taken into account for the computation.

When the driver has not inserted his card, the computations involved are based on the data memory recordings related to the current period where no card was inserted and related to the relevant slot;

q) "data memory" means:

an electronic data storage device built into the control device;

r) "digital signature" means:

data appended to, or a cryptographic transformation of, a block of data that allows the recipient of the block of data to prove the authenticity and integrity of the block of data;

s) "downloading" means:

copying together with digital signature of a part or of a complete set of data stored in the data memory of the vehicle or in the memory of a tachograph card;

Downloading may not alter or delete any stored data.

t) "driver card" means:

a tachograph card issued by the authorities of a Contracting Party to a particular driver;

The driver card identifies the driver and allows for storage of driver activity data.

u) "effective circumference of the wheel tyres" means:

the average of the distances travelled by each of the wheels moving the vehicle (driving wheels) in the course of one complete rotation. The measurement of these distances shall be made under standard test conditions (Chapter VI-5.) and is expressed in the form "l = ... mm". Vehicle manufacturers may replace the measurement of these distances by a theoretical calculation which takes into account the distribution of the weight on the axles, vehicle unladen in normal running order[3]. The methods for such theoretical calculation will be approved by a competent Contracting Party authority;

---

[3] The measurement of distances conforms to the provisions of Council Directive No. 97/27/EC of 22 July 1997 relating to the masses and dimensions of certain categories of motor vehicles and their trailers and amending Directive 70/156/EEC (OJ L 233, 25.08.97).

v) **"event" means:**

abnormal operation detected by the control device which may come from a fraud attempt;

w) **"fault" means:**

abnormal operation detected by the control device which may come from an equipment malfunction or failure;

x) **"installation" means:**

mounting of the control device in a vehicle;

y) **"motion sensor" means:**

part of the control device, providing a signal representative of vehicle speed and/or distance travelled;

z) **"non valid card" means:**

a card detected as faulty, or which initial authentication failed, or which start of validity date is not yet reached, or which expiry date has passed;

aa) **"out of scope" means:**

when the use of the control device is not required, according to the provisions of this Agreement.

bb) **"over speeding" means:**

exceeding the authorised speed of the vehicle, defined as any period of more than 60 seconds during which the vehicle's measured speed exceeds the limit for setting the speed limitation device[4].

cc) **"periodic inspection" means:**

set of operations performed to control that the control device works properly and that its settings correspond to the vehicle parameters;

dd) **"printer" means:**

component of the control device which provides printouts of stored data;

ee) **"control device"means:**

the total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers;

---

[4] The limit for setting the speed limitation device conforms to the provisions of Council Directive No. 92/6/EEC of 10 February 1992 on the installation and use of speed limitation devices for certain categories of motor vehicles in the Community (OJ No L 057, 02/03/1992)

ff) "renewal" means:

issue of a new tachograph card when an existing card reaches its expiry date, or is malfunctioning and has been returned to the issuing authority. Renewal always implies the certainty that two valid cards do not co-exist;

gg) "repair" means:

any repair of a motion sensor or of a vehicle unit that requires disconnection of its power supply, or disconnection from other control device components, or opening of it;

hh) "replacement" means:

issue of a tachograph card in replacement of an existing card, which has been declared lost, stolen or malfunctioning and has not been returned to the issuing authority. Replacement always implies a risk that two valid cards may co-exist;

ii) "security certification" means:

process to certify, by a certification authority [5] that the control device (or component) or the tachograph card under investigation fulfils the security requirements defined in sub-appendix 10 Generic security targets;

jj) "self test" means:

tests run cyclically and automatically by the control device to detect faults;

kk) "tachograph card" means:

smart card intended for use with the control device. Tachograph cards allow for identification by the control device of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types:

- driver card,
- control card,
- workshop card,
- company card;

ll) "type approval" means:

Process to certify, by a Contracting Party, that the control device (or component) or the tachograph card under investigation fulfils the requirements of the AETR;

mm) "tyre size" means:

the designation of the dimensions of the tyres (external driving wheels) in accordance with ECE Regulation N°54[6];.

---

[5] The provisions on security shall conform with the provisions laid out in Council Recommendation 95/144/CE of 7 April 1995 on common information technology security evaluation criteria (O.J. No L093, 26/04/1995).

[6] Reference text in the EU is Directive 92/23/EEC of 31 March 1992 relating to tyres for motor vehicles and their trailers and to their fitting (OJ No L 129, 14/05/1992).

nn) "vehicle identification" means:

numbers identifying the vehicle: Vehicle Registration Number (VRN) with indication of the registering Contracting Party and Vehicle Identification Number (VIN)[7];

oo) "vehicle unit (VU)" means:

the control device excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of the AETR;

pp) for computing sake in the control device "week" means:

the period between 00.00 hours UTC on Monday and 24.00 UTC on Sunday;

qq) "workshop card" means:

a tachograph card issued by the authorities of a Contracting Party to a control device manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Contracting Party.

The workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the control device.

---

[7] Vehicle identification conforms to the provisions of Council Directive No. 76/114/EEC of 18 December 1975 on the approximation of the laws of the Member States relating to statutory plates and inscriptions for motor vehicles and their trailers, and their location and method of attachment (OJ, No. L 24, 30/01/1976).

II. GENERAL CHARACTERISTICS AND FUNCTIONS OF THE RECORDING EQUIPMENT

000 Any vehicle fitted with the control device complying with the provisions of this Appendix, must include a speed display and an odometer. These functions may be included within the control device.

1. General characteristics

The purpose of the control device is to record, store, display, print, and output data related to driver activities.

001 The control device includes cables, a motion sensor, and a vehicle unit.

002 The vehicle unit includes a processing unit, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration/downloading connector, and facilities for entry of user's inputs.

The control device may be connected to other devices through additional connectors.

003 Any inclusion in or connection to the control device of any function, device, or devices, approved or otherwise, shall not interfere with, or be capable of interfering with, the proper and secure operation of the control device and the provisions of this Agreement.

Control device users identify themselves to the equipment via tachograph cards.

004 The control device provides selective access rights to data and functions according to user's type and/or identity.

The control device records and stores data in its data memory and in tachograph cards.

This is done in accordance with the European provisions on the protection of individuals with regard to the processing of personal data and on the free movement of such data[8].

2. Functions

005 The control device shall ensure the following functions:

- monitoring cards insertions and withdrawals,
- speed and distance measurement,
- time measurement,
- monitoring driver activities,
- monitoring driving status,
- drivers manual entries:
  - entry of places where daily work periods begin and/or end,
  - manual entry of driver activities,
  - entry of specific conditions,

[8] The protection of individuals with regard to the processing of personal data and the free movement of such data conform to the provisions of Council Directive No. 95/46/EC of 24 October 1995, as last amended (OJ, No. L 281, 23/11/1995).

- company locks management,
- monitoring control activities,
- detection of events and/or faults,
- built-in and self tests,
- reading from data memory,
- recording and storing in data memory,
- reading from tachograph cards,
- recording and storing in tachograph cards,
- displaying,
- printing,
- warning,
- data downloading to external media,
- output data to additional external devices,
- calibration,
- time adjustment.

3. Modes of operation

006 The control device shall possess four modes of operation:
- operational mode,
- control mode,
- calibration mode,
- company mode.

007 The control device shall switch to the following mode of operation according to the valid tachograph cards inserted into the card interface devices:

Mode of operation		Driver slot				
		No card	Driver card	Control card	Workshop card	Company card
Co-driver slot	No card	Operational	Operational	Control	Calibration	Company
	Driver card	Operational	Operational	Control	Calibration	Company
	Control card	Control	Control	Control (*)	Operational	Operational
	Workshop card	Calibration	Calibration	Operational	Calibration (*)	Operational
	Company card	Company	Company	Operational	Operational	Company (*)

008 (*) In these situations the control device shall use only the tachograph card inserted in the driver slot.

009 The control device shall ignore non valid cards inserted, except displaying, printing or downloading data held on an expired card which shall be possible.

010 All functions listed in II.2. shall work in any mode of operation with the following exceptions:

- the calibration function is accessible in the calibration mode only,
- the time adjustment function is limited when not in the calibration mode,
- the driver manual entries functions are accessible in operational or calibration modes only,
- the company locks management function is accessible in the company mode only,
- the monitoring of control activities function is operational in the control mode only,
- the downloading function is not accessible in the operational mode (except as provided for in Requirement 150).

011 The control device can output any data to display, printer or external interfaces with the following exceptions:

- in the operational mode, any personal identification (surname and first name(s)) not corresponding to a tachograph card inserted shall be blanked and any card number not corresponding to a tachograph card inserted shall be partially blanked (every odd character – from left to right - shall be blanked),
- in the company mode, driver related data (requirements 081, 084 and 087) can be output only for periods not locked by another company (as identified by the first 13 digits of the company card number),
- when no card is inserted in thecontrol device, driver related data can be output only for the current and 8 previous calendar days.

4. Security

The system security aims at protecting the data memory in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts, protecting the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit, protecting the integrity and authenticity of data exchanged between the control device and the tachograph cards, and verifying the integrity and authenticity of data downloaded.

012 In order to achieve the system security, the control device shall meet the security requirements specified in the motion sensor and vehicle unit generic security targets (sub-appendix 10).

III. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR RECORDING EQUIPMENT

1. Monitoring cards insertion and withdrawal

013 The control device shall monitor the card interface devices to detect card insertions and withdrawals.

014 Upon card insertion the control device shall detect whether the card inserted is a valid tachograph card and in such a case identify the card type.

015 The control device shall be so designed that the tachograph cards are locked in position on their proper insertion into the card interface devices.

016 The release of tachograph cards may function only when the vehicle is stopped and after the relevant data have been stored on the cards. The release of the card shall require positive action by the user.

2. Speed and distance measurement

017 This function shall continuously measure and be able to provide the odometer value corresponding to the total distance travelled by the vehicle.

018 This function shall continuously measure and be able to provide the speed of the vehicle.

019 The speed measurement function shall also provide the information whether the vehicle is moving or stopped. The vehicle shall be considered as moving as soon as the function detects more than 1 imp/sec for at least 5 seconds from the motion sensor, otherwise the vehicle shall be considered as stopped.

Devices displaying speed (speedometer) and total distance travelled (odometer) installed in any vehicle fitted with a control device complying with the provisions of this Ageement, shall comply with the requirements relating to maximum tolerances laid down in this Appendix (Chapters III.2.1 and III.2.2).

2.1 Measurement of distance travelled

020 The distance travelled may be measured either:
- so as to cumulate both forward and reverse movements, or
- so as to include only forward movement.

021 The control device shall measure distance from 0 to 9 999 999.9 km.

022 Distance measured shall be within the following tolerances (distances of at least 1000 m.):
- ± 1% before installation,
- ± 2% on installation and periodic inspection,
- ± 4% in use.

023 Distance measured shall have a resolution better than or equal to 0.1 km.

2.2 Measurement of speed

024 The control device shall measure speed from 0 to 220 km/h.

025 To ensure a maximum tolerance on speed displayed of ± 6 km/h in use, and taking into account:

- a ± 2 km/h tolerance for input variations (tyre variations, ...),
- a ± 1 km/h tolerance in measurements made during installation or periodic inspections,

the control device shall, for speeds between 20 and 180 km/h, and for characteristic coefficients of the vehicle between 4000 and 25000 imp/km, measure the speed with a tolerance of ± 1 km/h (at constant speed).

Note: The resolution of data storage brings an additional tolerance of ± 0.5 km/h to speed stored by the control device.

025a The speed shall be measured correctly within the normal tolerances within 2 seconds of the end of a speed change when the speed has changed at a rate up to $2m/s^2$.

026 Speed measurement shall have a resolution better than or equal to 1 km/h.

3. Time measurement

027 The time measurement function shall measure permanently and digitally provide UTC date and time.

028 UTC date and time shall be used for dating throughout the control device (recordings, printouts, data exchange, display, ...).

029 In order to visualise the local time, it shall be possible to change the offset of the time displayed, in half hour steps.

030 Time drift shall be within ± 2 seconds per day in type approval conditions.

031 Time measured shall have a resolution better than or equal to 1 second.

032 Time measurement shall not be affected by an external power supply cut-off of less than 12 months in type approval conditions.

4 Monitoring driver activities

033 This function shall permanently and separately monitor the activities of one driver and one co-driver.

034 Driver activity shall be DRIVING, WORK, AVAILABILITY, or BREAK/REST.

035 It shall be possible for the driver and/or the co-driver to manually select WORK, AVAILABILITY, or BREAK/REST.

036 When the vehicle is moving, DRIVING shall be selected automatically for the driver and AVAILABILITY shall be selected automatically for the co-driver.

037 When the vehicle stops, WORK shall be selected automatically for the driver.

038 The first change of activity arising within 120 seconds of the automatic change to WORK due to the vehicle stop shall be assumed to have happened at the time of vehicle stop (therefore possibly cancelling the change to WORK).

039 This function shall output activity changes to the recording functions at a resolution of one minute.

040 Given a calendar minute, if any DRIVING activity has occurred within the minute, the whole minute shall be regarded as DRIVING.

041 Given a calendar minute, if any DRIVING activity has occurred within both the immediately preceding and the immediately succeeding minute, the whole minute shall be regarded as DRIVING.

042 Given a calendar minute that is not regarded as DRIVING according to previous requirements, the whole minute shall be regarded to be of the same type of activity as the longest continuous activity within the minute (or the latest of the equally longests).

043 This function shall also permanently monitor the continuous driving time and the cumulative break time of the driver.

5. Monitoring driving status

044 This function shall permanently and automatically monitor the driving status.

045 The driving status CREW shall be selected when two valid driver cards are inserted in the equipment, the driving status SINGLE shall be selected in any other case.

6. Drivers manual entries

6.1 Entry of places where daily work periods begin and/or end

046 This function shall allow for the entry of places where the daily work periods begin and/or end for a driver and/or a co-driver.

047 Places are defined as the country and, in addition where applicable, the region.

048 At the time of a driver (or workshop) card withdrawal, the control device shall prompt the (co-)driver to enter a "place where the daily work period ends".

049 The control device shall allow this request to be disregarded.

050 It shall be possible to input places where daily work periods begin and/or end without card or at times other than card insertion or withdrawal.

6.2 Manual entry of driver activities

050a Upon driver (or workshop) card insertion, and only at this time, the control device shall:

- remind the cardholder the date and time of his last card withdrawal and,
- ask the cardholder to identify if the current insertion of the card represents a continuation of the current daily work period.

The control device shall allow the card holder to disregard the question without answering, or to answer positively, or to answer negatively:

- In the case where the cardholder disregards the question, the control device shall prompt the cardholder for a "place where the daily work period begins". The control device shall allow this request to be disregarded. If a location is entered, then it shall be recorded, in the data memory and in the tachograph card, and related to the card insertion time.
- In the case of a negative or positive answer, the control device shall invite the cardholder to enter activities manually, with their dates and times of beginning and end, among WORK, AVAILABILITY, or BREAK/REST only, strictly included within the period last card withdrawal – current insertion only, and without allowing such activities to overlap mutually. This shall be done in accordance with the following procedures:

- In the case where the cardholder answers positively to the question, the control device shall invite the cardholder to enter activities manually, in chronological order, for the period last card withdrawal – current insertion. The process shall end when the end time of a manually entered activity equals the card insertion time.
- In the case where the cardholder answers negatively to the question, the control device shall:
  - Invite the card holder to enter manually activities in chronological order from the card withdrawal time up to the time of end of the related daily work period (or of the activities related to that vehicle in the case where the daily work period continues on a record sheet). The control device shall therefore, before allowing the cardholder to enter manually each activity, invite the cardholder to identify if the time of end of the last recorded activity represents the end of a previous work period (see note below),

    Note: In the case where the cardholder fails to declare when the previous work period ended, and manually enters an activity which end time equals the card insertion time, the control device shall:

    - Assume that the daily work period ended at the start of the first REST (or remaining UNKNOWN) period after card withdrawal or at the time of card withdrawal if no rest period has been entered (and if no period remains UNKNOWN),
    - Assume that the start time (see below) equals the card insertion time,
    - Proceed through the steps below.
  - Then, if the time of end of the related work period is different from the time of card withdrawal , or if no place of end of daily work period had been entered at that time, prompt the cardholder to "confirm or enter the place where the daily work period ended" (the control device shall allow this request to be disregarded). If a location is entered, it shall be recorded in the tachograph card only and only if different from the one entered at card withdrawal (if one was entered), and related to the time of end of the work period,
  - Then invite the cardholder to "enter a start time" of the current daily work period (or of the activities related to the current vehicle in the case where the card holder previously used a record sheet during this period), and prompt the cardholder for a "place where the daily work period begins" (the control device shall allow this request to be disregarded). If a location is entered, it shall be recorded in the tachograph card and related to this start time. If this start time is equal to the card insertion time, the location shall also be recorded in the data memory,
  - Then, if this start time is different from the card insertion time, invite the cardholder to enter manually activities in chronological order from this start time up to the time of card insertion. The process shall end when the end time of a manually entered activity equals the card insertion time.
- The control device shall then allow the card holder to modify any activity manually entered, until validation by selection of a specific command, and thereafter forbid any such modification.
- Such answers to the initial question followed by no activity entries, shall be interpreted by the as if the cardholder had disregarded the question.

During this whole process, the control device shall wait for entries no longer than the following time-outs:

- if no interaction with the equipment's human machine interface is happening during 1 minute (with a visual, and possibly audible, warning after 30 seconds) or,
- if the card is withdrawn or another driver (or workshop) card is inserted or,
- as soon as the vehicle is moving,

in this case the control device shall validate any entries already made.

6.3 Entry of specific conditions

050b The shall allow the driver to enter, in real time, the following two specific conditions:

- "OUT OF SCOPE" (begin, end)
- "FERRY / TRAIN CROSSING"

A "FERRY / TRAIN CROSSING" may not occur if an "OUT OF SCOPE" condition is opened.

An opened "OUT OF SCOPE" condition must be automatically closed, by the control device , if a driver card is inserted or withdrawn.

7. Company locks management

051 This function shall allow the management of the locks placed by a company to restrict data access in company mode to itself.

052 Company locks consist in a start date/time (lock-in) and an end date/time (lock-out) associated with the identification of the company as denoted by the company card number (at lock-in).

053 Locks may be turned "in" or "out" in real time only.

054 Locking-out shall only be possible for the company whose lock is "in" (as identified by the first 13 digits of the company card number), or,

055 locking-out shall be automatic if another company locks in.

055a In the case where a company locks in and where the previous lock was for the same company, then it will be assumed that the previous lock has not been turned "out" and is still "in".

8. Monitoring control activities

056 This function shall monitor DISPLAYING, PRINTING, VU and card DOWNLOADING activities carried while in control mode.

057 This function shall also monitor OVER SPEEDING CONTROL activities while in control mode. An over speeding control is deemed to have happened when, in control mode, the "over speeding" printout has been sent to the printer or to the display, or when "events and faults" data have been downloaded from the VU data memory.

9. Detection of events and/or faults

058 This function shall detect the following events and/or faults:

9.1 "Insertion of a non valid card" event

059 This event shall be triggered at the insertion of any non valid card and/or when an inserted valid card expires.

9.2 "Card conflict" event

060 This event shall be triggered when any of the valid cards combination noted X in the following table arise:

Card conflict		Driver slot				
		No card	Driver card	Control card	Workshop card	Company card
Co-driver slot	No card					
	Driver card				X	
	Control card			X	X	X
	Workshop card		X	X	X	X
	Company card			X	X	X

9.3 "Time overlap" event

061 This event shall be triggered when the date / time of last withdrawal of a driver card, as read from the card, is later than the current date / time of the control device in which the card is inserted.

9.4 "Driving without an appropriate card" event

062 This event shall be triggered for any tachograph cards combination noted X in the following table, when driver activity changes to DRIVING, or when there is a change of the mode of operation while driver activity is DRIVING:

Driving without an appropriate card		Driver slot				
		No (or non valid) card	Driver card	Control card	Workshop card	Company card
Co-driver slot	No (or non valid) card	X		X		X
	Driver card	X		X	X	X
	Control card	X	X	X	X	X
	Workshop card	X	X	X		X
	Company card	X	X	X	X	X

9.5 "Card insertion while driving" event

063 This event shall be triggered when a tachograph card is inserted in any slot, while driver activity is DRIVING.

9.6 "Last card session not correctly closed" event

064 This event shall be triggered when at card insertion the control device detects that, despite the provisions laid down in paragraph III.1., the previous card session has not been correctly closed (the card has been withdrawn before all relevant data have been stored on the card). This event shall be triggered by driver and workshop cards only.

9.7 "Over speeding" event

065 This event shall be triggered for each over speeding.

9.8 "Power supply interruption" event

066 This event shall be triggered, while not in calibration mode, in case of any interruption exceeding 200 milliseconds of the power supply of the motion sensor and/or of the vehicle unit. The interruption threshold shall be defined by the manufacturer. The drop in power supply due to the starting of the engine of the vehicle shall not trigger this event.

9.9 "Motion data error" event

067 This event shall be triggered in case of interruption of the normal data flow between the motion sensor and the vehicle unit and/or in case of data integrity or data authentication error during data exchange between the motion sensor and the vehicle unit.

9.10 "Security breach attempt" event

068 This event shall be triggered for any other event affecting the security of the motion sensor and/or of the vehicle unit as specified within the generic security targets of these components, while not in calibration mode.

9.11 "Card" fault

069 This fault shall be triggered when a tachograph card failure occurs during operation.

9.12 "Control device " fault

070 This fault shall be triggered for any of these failures, while not in calibration mode:

- VU internal fault
- Printer fault
- Display fault
- Downloading fault
- Sensor fault

10 Built-in and self tests

071 The control device shall self-detect faults through self tests and built-in-tests, according to the following table:

Sub-assembly to test	self test	Built-in-test
Software		Integrity
Data memory	Access	Access, data integrity
Card interface devices	Access	Access
Keyboard		Manual check
Printer	(up to manufacturer)	Printout
Display		Visual check
Downloading (performed only during downloading)	Proper operation	
Sensor	Proper operation	Proper operation

11. Reading from data memory

072 The control device shall be able to read any data stored in its data memory.

12. Recording and storing in the data memory

For the purpose of this paragraph,

- "365 days" is defined as 365 calendar days of average drivers activity in a vehicle. The average activity per day in a vehicle is defined as at least 6 drivers or co-drivers, 6 card insertion withdrawal cycles, and 256 activity changes. "365 days" therefore include at least 2190 (co-)drivers, 2190 card insertion withdrawal cycles, and 93440 activity changes.
- times are recorded with a resolution of one minute, unless otherwise specified,
- odometer values are recorded with a resolution of one kilometre.
- speeds are recorded with a resolution of 1 km/h.

073 Data stored into the data memory shall not be affected by an external power supply cut-off of less than twelve months in type approval conditions.

074 The control device shall be able to record and store implicitly or explicitly in its data memory the following:

12.1 Equipment identification data

12.1.1 Vehicle Unit identification data

075 The control device shall be able to store in its data memory the following vehicle unit identification data:

- name of the manufacturer,
- address of the manufacturer,
- part number,
- serial number,
- software version number,
- software version installation date,
- year of equipment manufacture,
- approval number,

076 Vehicle unit identification data are recorded and stored once and for all by the vehicle unit manufacturer, except the software related data and the approval number which may be changed in case of software upgrade.

12.1.2 Motion sensor identification data

077 The motion sensor shall be able to store in its memory the following identification data:

- name of the manufacturer,
- part number,
- serial number,
- approval number,
- embedded security component identifier (e.g. internal chip/processor part number),
- operating system identifier (e.g. software version number).

078 Motion sensor identification data are recorded and stored once and for all in the motion sensor, by the motion sensor manufacturer.

079 The vehicle unit shall be able to record and store in its data memory the following currently paired motion sensor identification data:

- serial number,
- approval number,
- first pairing date,

12.2 Security elements

080 The control device shall be able to store the following security elements:

- European? public key,
- Contracting Party certificate,
- equipment certificate,
- equipment private key.

Control device security elements are inserted in the equipment by the vehicle unit manufacturer.

12.3 Driver card insertion and withdrawal data

081 For each insertion and withdrawal cycle of a driver or workshop card in the equipment, the control device shall record and store in its data memory:

- the card holder's surname and first name(s) as stored in the card,
- the card's number, issuing Contracting Party and expiry date as stored in the card,
- the insertion date and time,
- the vehicle odometer value at card insertion,
- the slot in which the card is inserted,
- the withdrawal date and time,
- the vehicle odometer value at card withdrawal,
- the following information about the previous vehicle used by the driver, as stored in the card:
  - VRN and registering Contracting Party,
  - card withdrawal date and time,
- a flag indicating whether, at card insertion, the card holder has manually entered activities or not.

082 The data memory shall be able to hold these data for at least 365 days.

083 When storage capacity is exhausted, new data shall replace oldest data.

12.4 Driver activity data

084 The control device shall record and store in its data memory whenever there is a change of activity for the driver and/or the co-driver, and/or whenever there is a change of driving status, and/or whenever there is an insertion or withdrawal of a driver or workshop card:

- the driving status (CREW, SINGLE)
- the slot (DRIVER, CO-DRIVER),
- the card status in the relevant slot (INSERTED, NOT INSERTED)(See Note),
- the activity (DRIVING, AVAILABILITY, WORK, BREAK/REST).
- the date and time of the change,

Note: INSERTED means that a valid driver or workshop card is inserted in the slot. NOT INSERTED means the opposite i.e. no valid driver or workshop card is inserted in the slot (e.g. a company card is inserted or no card is inserted)

Note: Activity data manually entered by a driver are not recorded in the data memory.

085 The data memory shall be able to hold driver activity data for at least 365 days.

086 When storage capacity is exhausted, new data shall replace oldest data.

12.5 Places where daily work periods start and/or end

087 The control device shall record and store in its data memory whenever a (co-)driver enters the place where a daily work period begins and/or ends:

- If applicable, the (co-)driver card number and card issuing Contracting Party,
- the date and time of the entry (or the date/time related to the entry when the entry is made during the manual entry procedure),
- the type of entry (begin or end, condition of entry),
- the country and region entered,
- the vehicle odometer value.

088 The data memory shall be able to hold daily work periods start and/or end data for at least 365 days (with the assumption that one driver enters two records per day).

089 When storage capacity is exhausted, new data shall replace oldest data.

12.6 Odometer data

090 The control device shall record in its data memory the vehicle odometer value and the corresponding date at midnight every calendar day.

091 The data memory shall be able to store midnight odometer values for at least 365 calendar days.

092 When storage capacity is exhausted, new data shall replace oldest data.

12.7 Detailed speed data

093 The control device shall record and store in its data memory the instantaneous speed of the vehicle and the corresponding date and time at every second of at least the last 24 hours that the vehicle has been moving.

12.8 Events data

For the purpose of this subparagraph, time shall be recorded with a resolution of 1 second.

094 The control device shall record and store in its data memory the following data for each event detected according to the following storage rules:

Event	Storage rules	Data to be recorded per event
Card conflict	- the 10 most recent events.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Contracting Party of the two cards creating the conflict.
Driving without an appropriate card	- the longest event for each of the 10 last days of occurrence, - the 5 longest events over the last 365 days.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Contracting Party of any card inserted at beginning and/or end of the event, - number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	- date and time of the event, - card's type, number and issuing Contracting Party, - number of similar events that day

Last card session not correctly closed	- the 10 most recent events.	- date and time of card insertion,
		- card's type, number and issuing Contracting Party,
		- last session data as read from the card:
		  - date and time of card insertion,
		  - VRN and Contracting Party of registration.

Event	Storage rules	Data to be recorded per event
Over speeding (1)	- the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed), - the 5 most serious events over the last 365 days. - the first event having occurred after the last calibration	- date and time of beginning of event, - date and time of end of event, - maximum speed measured during the event, - arithmetic average speed measured during the event, - card's type, number and issuing Contracting Party of the driver (if applicable), - number of similar events that day.
Power supply interruption (2)	- the longest event for each of the 10 last days of occurrence, - the 5 longest events over the last 365 days.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Contracting Party of any card inserted at beginning and/or end of the event, - number of similar events that day.
Motion data error	- the longest event for each of the 10 last days of occurrence, - the 5 longest events over the last 365 days.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Contracting Party of any card inserted at beginning and/or end of the event, - number of similar events that day.
Security breach attempt	- the 10 most recent events per type of event.	- date and time of beginning of event, - date and time of end of event (if relevant), - cards' type, number and issuing Contracting Party of any card inserted at beginning and/or end of the event, - type of event.

095 (1) The control device shall also record and store in its data memory :

- the date and time of the last OVER SPEEDING CONTROL,
- the date and time of the first over speeding following this OVER SPEEDING CONTROL,
- the number of over speeding events since the last OVER SPEEDING CONTROL.

(2) These data may be recorded at power supply reconnection only, times may be known with an accuracy to the minute.

12.9 Faults data

For the purpose of this subparagraph, time shall be recorded with a resolution of 1 second.

096 The control device shall attempt to record and store in its data memory the following data for each fault detected according to the following storage rules:

Fault	Storage rules	Data to be recorded per fault
Card fault	- the 10 most recent driver card faults.	- date and time of beginning of fault, - date and time of end of fault, - card's type number and issuing Contracting Party
Control device faults	- the 10 most recent faults for each type of fault, - the first fault after the last calibration.	- date and time of beginning of fault, - date and time of end of fault, - type of fault, - cards' type, number and issuing Contracting Party of any card inserted at beginning and/or end of the fault.

12.10 Calibration data

097 The control device shall record and store in its data memory data relevant to:

- known calibration parameters at the moment of activation,
- its very first calibration following its activation,
- its first calibration in the current vehicle (as identified by its VIN),
- the 5 most recent calibrations (If several calibrations happen within one calendar day, only the last one of the day shall be stored).

098 The following data shall be recorded for each of these calibrations:

- Purpose of calibration (activation, first installation, installation, periodic inspection)
- workshop name and address,
- workshop card number, card issuing Contracting Party and card expiry date,
- vehicle identification,
- parameters updated or confirmed: w, k, l, tyre size, speed limiting device setting, odometer (old and new values), date and time (old and new values).

099 The motion sensor shall record and store in its memory the following motion sensor installation data:

- first pairing with a VU (date, time, VU approval number, VU serial number),
- last pairing with a VU (date, time, VU approval number, VU serial number).

12.11 Time adjustment data

100 The control device shall record and store in its data memory data relevant to:

- the most recent time adjustment,
- the 5 largest time adjustments, since last calibration,

performed in calibration mode outside the frame of a regular calibration (def. f)).

101 The following data shall be recorded for each of these time adjustments:

- date and time, old value,
- date and time, new value,
- workshop name and address,
- workshop card number, card issuing Contracting Party and card expiry date.

12.12 Control activity data

102 The control device shall record and store in its data memory the following data relevant to the 20 most recent control activities:

- date and time of the control,
- control card number and card issuing Contracting Party,
- type of the control (displaying and/or printing and/or VU downloading and/or card downloading).

103 In case of downloading, the dates of the oldest and of the most recent days downloaded shall also be recorded.

12.13 Company locks data

104 The control device shall record and store in its data memory the following data relevant to the 20 most recent company locks:

- lock-in date and time,
- lock-out date and time,
- company card number and card issuing Contracting Party,
- company name and address.

12.14 Download activity data

105 The control device shall record and store in its data memory the following data relevant to the last data memory downloading to external media while in company or in calibration mode:

- date and time of downloading,
- company or workshop card number and card issuing Contracting Party,
- company or workshop name.

12.15 Specific conditions data

105a The control device shall record in its data memory the following data relevant to specific conditions:

- Date and time of the entry,
- Type of specific condition.

105b The data memory shall be able to hold specific conditions data for at least 365 days (with the assumption that on average, 1 condition is opened and closed per day). When storage capacity is exhausted, new data shall replace oldest data.

13. Reading from tachograph cards

106 The control device shall be able to read from tachograph cards, where applicable, the necessary data:

- to identify the card type, the card holder, the previously used vehicle, the date and time of the last card withdrawal and the activity selected at that time,
- to check that last card session was correctly closed,
- to compute the driver's continuous driving time, cumulative break time and cumulated driving times for the previous and the current week,
- to print requested printouts related to data recorded on a driver card,
- to download a driver card to external media.

107 In case of a reading error, the recording equipment shall try again, three times maximum, the same read command, and then if still unsuccessful, declare the card faulty and non valid.

14. Recording and storing on tachograph cards

108 The control device shall set the "card session data" in the driver or workshop card right after the card insertion.

109 The control device shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

109a The control device shall update driver activity and location data (as specified in Chapter IV paragraphs 5.2.5 and 5.2.6), stored on valid driver and/or workshop cards, with activity and location data manually entered by the cardholder.

110 Tachograph cards data update shall be such that, when needed and taking into account card actual storage capacity, most recent data replace oldest data.

111 In the case of a writing error, the control device shall try again, three times maximum, the same write command, and then if still unsuccessful, declare the card faulty and non valid.

112 Before releasing a driver card, and after all relevant data have been stored on the card, the control device shall reset the "card session data".

15. Displaying

113 The display shall include at least 20 characters.

114 The minimum character size shall be 5 mm high and 3.5 mm wide.

114a The display shall support the Latin1 and Greek character sets defined by ISO 8859 parts 1 and 7, as specified in sub-appendix 1, Chapter 4 'Character sets'. The display may use simplified glyphs (e.g. accented characters may be displayed without accent, or lower case letters may be shown as upper case letters).

115 The display shall be provided with adequate non-dazzling lighting.

116 Indications shall be visible from outside the control device.

117 The control device shall be able to display:

- default data,
- data related to warnings,
- data related to menu access,
- other data requested by a user.

Additional information may be displayed by the control device, provided that it is clearly distinguishable from information required above.

118 The display of the control device shall use the pictograms or pictograms combinations listed in sub-appendix 3. Additional pictograms or pictograms combinations may also be provided by the display, if clearly distinguishable from the aforementioned pictograms or pictograms combinations.

119 The display shall always be ON when the vehicle is moving.

120 The control device may include a manual or automatic feature to turn the display OFF when the vehicle is not moving.

Displaying format is specified in sub-appendix 5.

15.1 Default display

121 When no other information needs to be displayed, the control device shall display, by default, the following:

- the local time (as a result of UTC time + offset as set by the driver),
- the mode of operation,
- the current activity of the driver and the current activity of the co-driver,
- information related to the driver:
  - if his current activity is DRIVING, his current continuous driving time and his current cumulative break time,
  - if his current activity is not DRIVING, the current duration of this activity (since it was selected) and his current cumulative break time,
- information related to the co-driver:
  - the current duration of his activity (since it was selected).

122 Display of data related to each driver shall be clear, plain and unambiguous. In the case where the information related to the driver and the co-driver cannot be displayed at the same time, the control device shall display by default the information related to the driver and shall allow the user to display the information related to the co-driver.

123 In the case where the display width does not allow to display by default the mode of operation, the control device shall briefly display the new mode of operation when it changes.

124 The control device shall briefly display the card holder name at card insertion.

124a When an "OUT OF SCOPE" condition is opened, then the default display must show using the relevant pictogram that the condition is opened (It is acceptable that the driver's current activity may not be shown at the same time).

15.2 Warning display

125 The control device shall display warning information using primarily the pictograms of sub-appendix 3, completed where needed by an additional numerically coded information. A literal description of the warning may also be added in the driver's preferred language.

15.3 Menu access

126 The control device shall provide necessary commands through an appropriate menu structure.

15.4 Other displays

127 It shall be possible to display selectively on request:

- the UTC date and time,
- the mode of operation (if not provided by default)
- the continuous driving time and cumulative break time of the driver,
- the continuous driving time and cumulative break time of the co-driver,
- the cumulated driving time of the driver for the previous and the current week,
- the cumulated driving time of the co-driver for the previous and the current week,
- the content of any of the six printouts under the same formats as the printouts themselves.

128 Printout content display shall be sequential, line by line. If the display width is less than 24 characters the user shall be provided with the complete information through an appropriate mean (several lines, scrolling, ...). Printout lines devoted to hand-written information may be omitted for display.

16. Printing

129 The control device shall be able to print information from its data memory and/or from tachograph cards in accordance with the six following printouts:

- driver activities from card daily printout,
- driver activities from Vehicle Unit daily printout,
- events and faults from card printout,
- events and faults from Vehicle Unit printout,
- technical data printout,
- over speeding printout.

The detailed format and content of these printouts are specified in sub-appendix 4.

Additional data may be provided at the end of the printouts

Additional printouts may also be provided by the control device, if clearly distinguishable from the six aforementioned printouts.

130 The "driver activities from card daily printout" and "Events and faults from card printout" shall be available only when a driver card or a workshop card is inserted in the control device. The control device shall update data stored on the relevant card before starting printing.

131 In order to produce the "driver activities from card daily printout" or the "events and faults from card printout", the control device shall:

- either automatically select the driver card or the workshop card if one only of these cards is inserted,
- or provide a command to select the source card or select the card in the driver slot if two of these cards are inserted in thecontrol device.

132 The printer shall be able to print 24 characters per line.

133 The minimum character size shall be 2.1 mm high and 1.5 mm wide.

133a The printer shall support the Latin1 and Greek character sets defined by ISO 8859 parts 1 and 7, as specified in sub-appendix 1, Chapter 4 'Character sets'.

134 Printers shall be so designed as to produce these printouts with a degree of definition likely to avoid any ambiguity when they are read.

135 Printouts shall retain their dimensions and recordings under normal conditions of humidity (10-90%) and temperature.

136 The paper for use by the control device shall bear the relevant type approval mark and the indication of the type(s) of control device with which it may be used. Printouts shall remain clearly legible and identifiable under normal conditions of storage, in terms of light intensity, humidity and temperature, for at least one year.

137 It shall also be possible to add hand-written notes, such as the driver's signature, to these documents.

138 The control device shall manage "paper out" events while printing by, once paper has been re-loaded, restarting printing from printout beginning or by continuing printing and providing an unambiguous reference to previously printed part.

17. Warnings

139 The control device shall warn the driver when detecting any event and/or fault.

140 Warning of a power supply interruption event may be delayed until the power supply is reconnected.

141 The control device shall warn the driver 15 minutes before and at the time of exceeding 4 h. 30 min. continuous driving time.

142 Warnings shall be visual. Audible warnings may also be provided in addition to visual warnings.

143 Visual warnings shall be clearly recognisable by the user, shall be situated in the driver's field of vision and shall be clearly legible both by day and by night.

144 Visual warnings may be built into the control device and/or remote from the control device.

145 In the latter case it shall bear a "T" symbol and shall be amber or orange.

146 Warnings shall have a duration of at least 30 seconds, unless acknowledged by the user by hitting any key of the control device. This first acknowledgement shall not erase warning cause display referred to in next paragraph.

147 Warning cause shall be displayed on the control device and remain visible until acknowledged by the user using a specific key or command of the control device.

148 Additional warnings may be provided, as long as they do not confuse drivers in relation to previously defined ones.

18. Data downloading to external media

149 The control device shall be able to download on request data from its data memory or from a driver card to external storage media via the calibration/downloading connector. The control device shall update data stored on the relevant card before starting downloading.

150 In addition and as an optional feature, the control device may, in any mode of operation, download data through another connector to a company authenticated through this channel. In such a case, company mode data access rights shall apply to this download.

151 Downloading shall not alter or delete any stored data.

The calibration/downloading connector electrical interface is specified in sub-appendix 6.

Downloading protocols are specified in sub-appendix 7.

19. Output data to additional external devices

152 When the control device does not include speed and/or odometer display functions, the control device shall provide output signal(s) to allow for displaying the speed of the vehicle (speedometer) and/or the total distance travelled by the vehicle (odometer).

153 The vehicle unit shall also be able to output the following data using an appropriate dedicated serial link independent from an optional CAN bus connection (ISO 11898 Road vehicles – Interchange of digital information – Controller Area Network (CAN) for high speed communication), to allow their processing by other electronic units installed in the vehicle:

- current UTC date and time,
- speed of the vehicle,
- total distance travelled by the vehicle (odometer),
- currently selected driver and co-driver activity,
- information if any tachograph card is currently inserted in the driver slot and in the co-driver slot and (if applicable) information about the corresponding cards identification (card number and issuing Contracting Party).

Other data may also be output in addition to this minimum list.

When the ignition of the vehicle is ON, these data shall be permanently broadcasted. When the ignition of the vehicle is OFF, at least any change of driver or co-driver activity and/or any insertion or withdrawal of a tachograph card shall generate a corresponding data output. In the event that data output has been withheld whilst the ignition of the vehicle is OFF, that data shall be made available once the ignition of the vehicle is ON again.

20. Calibration

154 The calibration function shall allow:

- to automatically pair the motion sensor with the VU,
- to digitally adapt the constant of the control device (k) to the characteristic coefficient of the vehicle (w) (vehicles with two or more axle ratios shall be fitted with a switch device whereby these various ratios will automatically be brought into line with the ratio for which the equipment has been adapted to the vehicle),
- to adjust (without limitation) the current time,
- to adjust the current odometer value,
- to update motion sensor identification data stored in the data memory,
- to update or confirm other parameters known to the control device: vehicle identification, w, l, tyre size and speed limiting device setting if applicable.

155 Pairing the motion sensor to the VU shall consist, at least, in:

- updating motion sensor installation data held by the motion sensor (as needed),
- copying from the motion sensor to the VU data memory necessary motion sensor identification data.

156 The calibration function shall be able to input necessary data through the calibration/downloading connector in accordance with the calibration protocol defined in sub-appendix 8. The calibration function may also input necessary data through other connectors.

21. Time adjustment

157 The time adjustment function shall allow for adjusting the current time in amounts of 1 minute maximum at intervals of not less than 7 days.

158 The time adjustment function shall allow for adjusting the current time without limitation, in calibration mode.

22. Performance characteristics

159 The Vehicle Unit shall be fully operational in the temperature range -20°C to 70°C, and the motion sensor in the temperature range -40°C to 135°C. Data memory content shall be preserved at temperatures down to -40°C.

160 The control device shall be fully operational in the humidity range 10% to 90%.

161 The control device shall be protected against over-voltage, inversion of its power supply polarity, and short circuits.

162 The control device shall conform with ECE Regulation N°10[9] related to electromagnetic compatibility and shall be protected against electrostatic discharges and transients.

---

[9] Reference text in the EU is Commission Directive 95/54/EC of 31 October 1995 adapting to technical progress Council Directive 72/245/EEC on the approximation of the laws of the Member States relating to the suppression of radio interference produced by spark-ignition engines fitted to motor vehicles (OJ No L 266, 08/11/1995).

23. Materials

163 All the constituent parts of the control device shall be made of materials of sufficient stability and mechanical strength and with stable electrical and magnetic characteristics.

164 For normal conditions of use, all the internal parts of the equipment shall be protected against damp and dust.

165 The Vehicle Unit shall meet the protection grade IP 40 and the motion sensor shall meet the protection grade IP 64, as per standard IEC 529.

166 The control device shall conform to applicable technical specifications related to ergonomic design.

167 The control device shall be protected against accidental damage.

24. Markings

168 If the control device displays the vehicle odometer value and speed, the following details shall appear on its display:

- near the figure indicating the distance, the unit of measurement of distance, indicated by the abbreviation "km",
- near the figure showing the speed, the entry "km/h".

The control device may also be switched to display the speed in miles per hour, in which case the unit of measurement of speed shall be shown by the abbreviation "mph".

169 A descriptive plaque shall be affixed to each separate component of the control device and shall show the following details:

- name and address of the manufacturer of the equipment,
- manufacturer's part number and year of manufacture of the equipment,
- equipment serial number,
- approval mark for the equipment type,

170 When physical space is not sufficient to show all above mentioned details, the descriptive plaque shall show at least: the manufacturer's name or logo, and the equipment's part number.

IV. CONSTRUCTION AND FUNCTIONAL REQUIREMENTS FOR TACHOGRAPH CARDS

1. Visible data

The front page will contain:

171 the words "Driver card" or "Control card" or "Workshop card" or "Company card" printed in large type in the official language or languages of the Contracting Party issuing the card, according to the type of the card.[10]

172 the same words in the UNECE official languages, printed to form the background of the card (see models under 178):

EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
RU	КАРТОЧКА ВОДИТЕЛЯ	КАРТОЧКА КОНТРОЛЕРА	КАРТОЧКА МАСТЕРСКОЙ	КАРТОЧКА ПРЕДПРИЯТИЯ

173 the name of the Contracting Party issuing the card (optional);

174 the distinguishing sign of the Contracting Party issuing the card. The official distinguishing signs of Contracting Parties are those drawn up in accordance with the 1968 Vienna Convention on Road Traffic or the 1949 Geneva Convention on Road Traffic. The distinguishing signs of AETR Contracting Parties shall be as follows:

AL	Albania	**GR**	Greece	**MD**	Republic of Moldova
AND	Andorra	**H**	Hungary	**RO**	Romania
A	Austria	**IR**	Ireland	**SRB**	Serbia
AM	Armenia	**I**	Italy	**SK**	Slovakia
AZ	Azerbaijan	**KZ**	Kazakhstan	**SLO**	Slovenia
BY	Belarus	**LV**	Latvia	**E**	Spain
B	Belgium	**FL**	Liechtenstein	**S**	Sweden
BIH	Bosnia and Herzegovina	**LT**	Lithuania	**CH**	Switzerland
BG	Bulgaria	**L**	Luxembourg	**MK**	The FYR of Macedonia
HR	Croatia	**M**	Malta	**TR**	Turkey
CY	Cyprus	**MNE**	Montenegro	**TM**	Turkmenistan
CZ	Czech Republic	**NL**	Netherlands	**UK**	United Kingdom
DK	Denmark	**N**	Norway	**UA**	Ukrainia
EST	Estonia	**PL**	Poland	**UZ**	Uzbekistan
FIN	Finland	**P**	Portugal		
F	France	**RUS**	Russian Federation		
D	Germany	**RSM**	San Marino		

[10] The Contracting Parties will communicate to the UNECE secretariat the words used in their national language.

175 information specific to the card issued, numbered as follows:

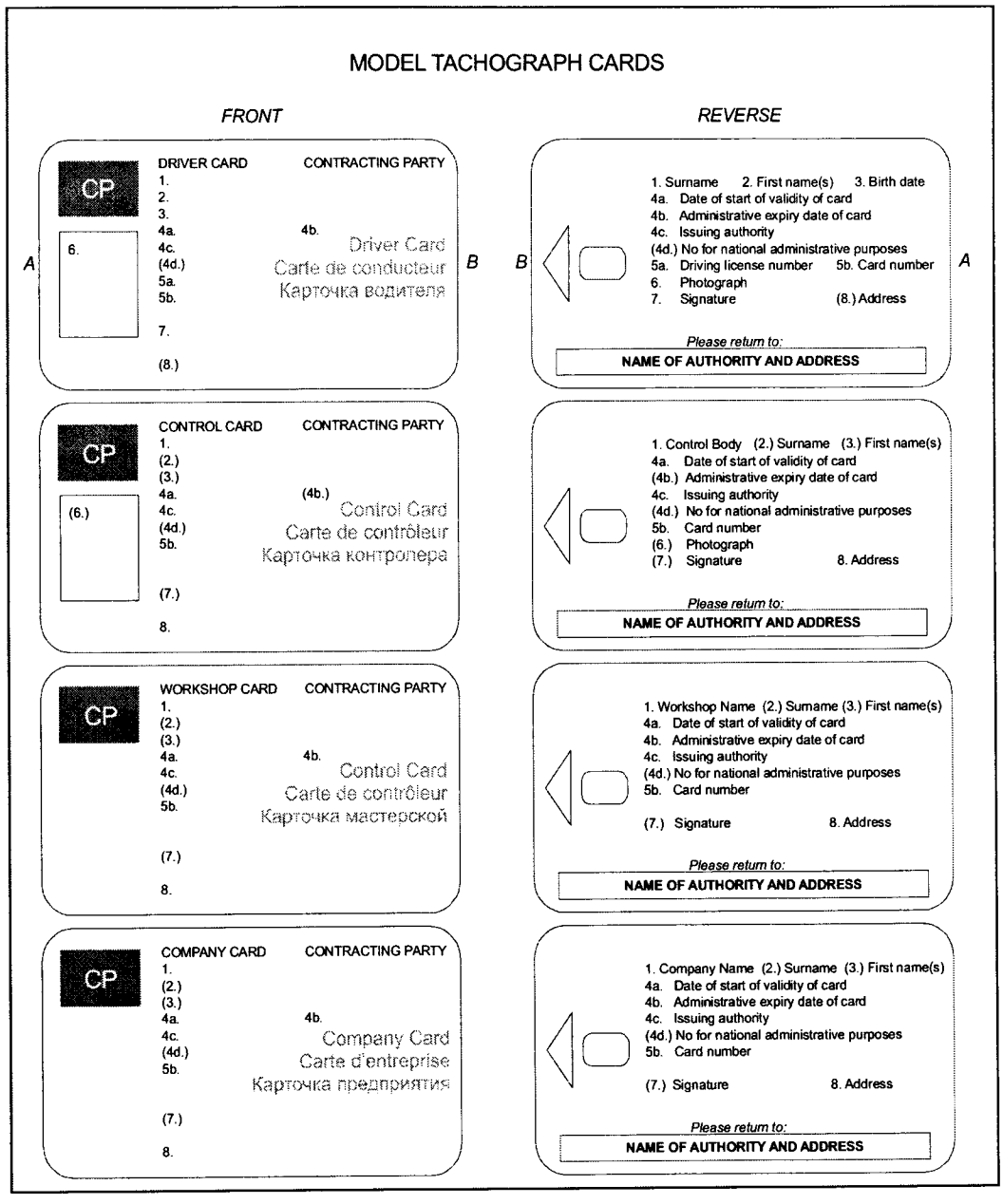
	Driver card	Control Card	Company or Workshop card
1.	surname of the driver	control body name	company or workshop name
2.	first name(s) of the driver	surname of the controller (if applicable)	surname of card holder (if applicable)
3.	birth date of the driver	first name(s) of the controller (if applicable)	first name(s) of card holder (if applicable)
4.(a)	card start of validity date		
(b)	card expiry date (if any)		
(c)	the name of the issuing authority (may be printed on page 2)		
(d)	a different number from the one under heading 5, for administrative purposes (optional)		
5. (a)	Driving licence number (at the date of issue of the driver card)	-	-
5. (b)	Card number		
6.	Photograph of the driver	photograph of the controller (optional)	-
7.	Signature of the driver	Signature of the holder (optional)	
8.	Normal place of residence, or postal address of the holder (optional).	Postal address of control body	postal address of company or workshop

176 dates shall be written using a "dd/mm/yyyy" or "dd.mm.yyyy" format (day, month, year).

The reverse page will contain:

177 an explanation of the numbered items which appear on the front page of the card;

178 with the specific written agreement of the holder, information which is not related to the administration of the card may also be added, such addition will not alter in any way the use of the model as a tachograph card.



179 Tachograph cards shall be printed with the following background predominant colours:

- driver card: white,
- control card: blue,
- workshop card: red,
- company card: yellow.

180 Tachograph cards shall bear at least the following features for protection of the card body against counterfeiting and tampering:

- a security design background with fine guilloche patterns and rainbow printing,
- in the area of the photograph, the security design background and the photograph shall overlap,
- at least one two-coloured microprint line.

181 After consulting the UNECE secretariat, Contracting Parties may add colours or markings, such as national symbols and security features, without prejudice to the other provisions of this Appendix'.

2. Security

The system security aims at protecting integrity and authenticity of data exchanged between the cards and the control device, protecting the integrity and authenticity of data downloaded from the cards, allowing certain write operations onto the cards to control device only, ruling out any possibility of falsification of data stored in the cards, preventing tampering and detecting any attempt of that kind

182 In order to achieve the system security, the tachograph cards shall meet the security requirements defined in the tachograph cards generic security target (sub-appendix 10).

183 Tachograph cards shall be readable by other equipment such as personal computers.

3. Standards

184 The tachograph cards shall comply with the following standards:

- ISO/IEC 7810 Identification cards – Physical characteristics,
- ISO/IEC 7816 Identification cards - Integrated circuits with contacts:
  - Part 1: Physical characteristics,
  - Part 2: Dimensions and location of the contacts,
  - Part 3: Electronic signals and transmission protocols,
  - Part 4: Inter-industry commands for interchange,
  - Part 8: Security related inter-industry commands,
- ISO/IEC 10373 Identification cards – Test methods,

4. Environmental and electrical specifications

185 The tachograph cards shall be capable of operating correctly in all the climatic conditions normally encountered in the territory of Contracting Parties and at least in the temperature range -25°C to +70°C with occasional peaks of up to +85°C, "occasional" meaning not more than 4 hours each time and not over 100 times during the life time of the card.

186 The tachograph cards shall be capable of operating correctly in the humidity range 10% to 90%.

187 The tachograph cards shall be capable of operating correctly for a five-year period if used within the environmental and electrical specifications.

188 During operation, the tachograph cards shall conform ECE Regulation N°10[11] related to electromagnetic compatibility, and shall be protected against electrostatic discharges.

5. Data storage

For the purpose of this paragraph,
- times are recorded with a resolution of one minute, unless otherwise specified,
- odometer values are recorded with a resolution of one kilometre,
- speeds are recorded with a resolution of 1 km/h.

The tachograph cards functions, commands and logical structures, fulfilling data storage requirements are specified in sub-appendix 2.

189 This paragraph specifies minimum storage capacity for the various application data files. The tachograph cards shall be able to indicate to the control device the actual storage capacity of these data files.

Any additional data that may be stored on tachograph cards, related to other applications eventually borne by the card, shall be stored in accordance with the European provisions[12].on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

5.1 Card identification and security data

5.1.1 Application identification

190 The tachograph cards shall be able to store the following application identification data:
- tachograph application identification,
- type of tachograph card identification.

5.1.2 Chip identification

191 The tachograph cards shall be able to store the following Integrated Circuit (IC) identification data:
- IC serial number,
- IC manufacturing references.

5.1.3 IC card identification

192 The tachograph cards shall be able to store the following smart card identification data:
- card serial number (including manufacturing references),
- card type approval number,
- card personaliser identification (ID),
- embedder ID,
- IC identifier.

---

[11] Reference text in the EU is Commission Directive 95/54/EC of 31 October 1995 adapting to technical progress Council Directive 72/245/EEC on the approximation of the laws of the Member States relating to the suppression of radio interference produced by spark-ignition engines fitted to motor vehicles (OJ No L 266, 08/11/1995).

[12] The protection of individuals with regard to the processing of personal data and the free movement of such data conform to the provisions of Council Directive No. 95/46/EC of 24 October 1995, as last amended (OJ No. L 281, 23/11/1995).

5.1.4 Security elements

193 The tachograph cards shall be able to store the following security elements data:

- European public key,
- Contracting Party certificate,
- card certificate,
- card private key.

5.2 Driver card

5.2.1 Card identification

194 The driver card shall be able to store the following card identification data:

- card number,
- issuing Contracting Party, issuing authority name, issue date,
- card beginning of validity date, card expiry date.

5.2.2 Card holder identification

195 The driver card shall be able to store the following card holder identification data:

- surname of the holder,
- first name(s) of the holder,
- date of birth,
- preferred language.

5.2.3 Driving licence information

196 The driver card shall be able to store the following driving licence data:

- issuing Contracting Party, issuing authority name,
- driving licence number (at the date of the issue of the card).

5.2.4 Vehicles used data

197 The driver card shall be able to store, for each calendar day where the card has been used, and for each period of use of a given vehicle that day (a period of use includes all consecutive insertion / withdrawal cycle of the card in the vehicle, as seen from the card point of view), the following data:

- date and time of first use of the vehicle (i.e. first card insertion for this period of use of the vehicle, or 00h00 if the period of use is on-going at that time),
- vehicle odometer value at that time,
- date and time of last use of the vehicle, (i.e. last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time),
- vehicle odometer value at that time,
- VRN and registering Contracting Party of the vehicle.

198 The driver card shall be able to store at least 84 such records.

5.2.5 Driver activity data

199 The driver card shall be able to store, for each calendar day where the card has been used or for which the driver has entered activities manually, the following data:

- the date,
- a daily presence counter (increased by one for each of these calendar days),
- the total distance travelled by the driver during this day,
- a driver status at 00:00,
- whenever the driver has changed of activity, and/or has changed of driving status, and/or has inserted or withdrawn his card:
  - the driving status (CREW, SINGLE)
  - the slot (DRIVER, CO-DRIVER),
  - the card status (INSERTED, NOT INSERTED),
  - the activity (DRIVING, AVAILABILITY, WORK, BREAK/REST).
  - the time of the change,

200 The driver card memory shall be able to hold driver activity data for at least 28 days (the average activity of a driver is defined as 93 activity changes per day).

201 The data listed under requirements 197 and 199 shall be stored in a way allowing the retrieval of activities in the order of their occurrence, even in case of a time overlap situation.

5.2.6 Places where daily work periods start and/or end

202 The driver card shall be able to store the following data related to places where daily work periods begin and/or end, entered by the driver:
- the date and time of the entry (or the date/time related to the entry if the entry is made during the manual entry procedure),
- the type of entry (begin or end, condition of entry),
- the country and region entered,
- the vehicle odometer value.

203 The driver card memory shall be able to hold at least 42 pairs of such records.

5.2.7 Events data

For the purpose of this subparagraph, time shall be stored with a resolution of 1 second.

204 The driver card shall be able to store data related to the following events detected by the control device while the card was inserted:
- Time overlap (where this card is the cause of the event),
- Card insertion while driving (where this card is the subject of the event),
- Last card session not correctly closed (where this card is the subject of the event),
- Power supply interruption,
- Motion data error,
- Security breach attempts.

205 The driver card shall be able to store the following data for these events:

- Event code,
- Date and time of beginning of the event (or of card insertion if the event was on-going at that time),
- Date and time of end of the event (or of card withdrawal if the event was on-going at that time),
- VRN and registering Contracting Party of vehicle in which the event happened.

Note: For the "Time overlap" event:

- Date and time of beginning of the event shall correspond to the date and time of the card withdrawal from the previous vehicle,
- Date and time of end of the event shall correspond to the date and time of card insertion in current vehicle,
- Vehicle data shall correspond to the current vehicle raising the event.

Note: For the "Last card session not correctly closed" event:

- date and time of beginning of event shall correspond to the card insertion date and time of the session not correctly closed,
- date and time of end of event shall correspond to the card insertion date and time of the session during which the event was detected (current session),
- Vehicle data shall correspond to the vehicle in which the session was not correctly closed.

206 The driver card shall be able to store data for the six most recent events of each type (i.e. 36 events).

5.2.8 Faults data

For the purpose of this subparagraph, time shall be recorded with a resolution of 1 second.

207 The driver card shall be able to store data related to the following faults detected by the control device while the card was inserted:

- Card fault (where this card is the subject of the event),
- Control device fault.

208 The driver card shall be able to store the following data for these faults:

- Fault code,
- Date and time of beginning of the fault (or of card insertion if the fault was on-going at that time),
- Date and time of end of the fault (or of card withdrawal if the fault was on-going at that time),
- VRN and registering Contracting Party of vehicle in which the fault happened.

209 The driver card shall be able to store data for the twelve most recent faults of each type (i.e. 24 faults).

5.2.9 Control activity data

210 The driver card shall be able to store the following data related to control activities:

- date and time of the control,
- control card number and card issuing Contracting Party,
- type of the control (displaying and/or printing and/or VU downloading and/or card downloading (see note)),
- Period downloaded, in case of downloading,
- VRN and registering Contracting Party of the vehicle in which the control happened.

Note: security requirements imply that card downloading will only be recorded if performed through a control device.

211 The driver card shall be able to hold one such record.

5.2.10 Card session data

212 The driver card shall be able to store data related to the vehicle which opened its current session:

- date and time the session was opened (i.e. card insertion) with a resolution of one second,
- VRN and registering Contracting Party.

5.2.11 Specific conditions data

212a The driver card shall be able to store the following data related to specific conditions entered while the card was inserted (whatever the slot):

- Date and time of the entry,
- Type of specific condition.

212b The driver card shall be able to hold 56 such records.

5.3 Workshop card

5.3.1 Security elements

213 The workshop card shall be able to store a Personal Identification Number (PIN code).

214 The workshop card shall be able to store the cryptographic keys needed for pairing motion sensors to vehicle units.

5.3.2 Card identification

215 The workshop card shall be able to store the following card identification data:

- card number,
- issuing Contracting Party, issuing authority name, issue date,
- card beginning of validity date, card expiry date.

5.3.3 Card holder identification

216 The workshop card shall be able to store the following card holder identification data:

- workshop name,
- workshop address,
- surname of the holder,
- first name(s) of the holder,
- preferred language.

5.3.4 Vehicles used data

217 The workshop card shall be able to store vehicles used data records in the same manner as a driver card.

218 The workshop card shall be able to store at least 4 such records.

5.3.5 Driver activity data

219 The workshop card shall be able to store driver activity data in the same manner as a driver card.

220 The workshop card shall be able to hold driver activity data for at least 1 day of average driver activity.

5.3.6 Daily work periods start and/or end data

221 The workshop card shall be able to store daily works period start and/or end data records in the same manner as a driver card.

222 The workshop card shall be able to hold at least 3 pairs of such records.

5.3.7 Events and faults data

223 The workshop card shall be able to store events and faults data records in the same manner as a driver card.

224 The workshop card shall be able to store data for the three most recent events of each type (i.e. 18 events) and the six most recent faults of each type (i.e. 12 faults).

5.3.8 Control activity data

225 The workshop card shall be able to store a control activity data record in the same manner as a driver card.

5.3.9 Calibration and time adjustment data

226 The workshop card shall be able to hold records of calibrations and/or time adjustments performed while the card is inserted in a control device.

227 Each calibration record shall be able to hold the following data:

- Purpose of calibration (activation, first installation, installation, periodic inspection,),
- Vehicle identification,
- Parameters updated or confirmed (w, k, l, tyre size, speed limiting device setting, odometer (new and old values), date and time (new and old values),
- Control device identification (VU part number, VU serial number, motion sensor serial number).

228 The workshop card shall be able to store at least 88 such records.

229 The workshop card shall hold a counter indicating the total number of calibrations performed with the card.

230 The workshop card shall hold a counter indicating the number of calibrations performed since its last download.

5.3.10 Specific conditions data

230a The workshop card shall be able to store data relevant to specific conditions in the same manner as the driver card. The workshop card shall be able to store 2 such records.

5.4 Control card

5.4.1 Card identification

231 The control card shall be able to store the following card identification data:

- card number,
- issuing Contracting Party, issuing authority name, issue date,
- card beginning of validity date, card expiry date (if any).

5.4.2 Card holder identification

232 The control card shall be able to store the following card holder identification data:

- control body name,
- control body address,
- surname of the holder,
- first name(s) of the holder,
- preferred language.

5.4.3 Control activity data

233 The control card shall be able to store the following control activity data:

- date and time of the control,
- type of the control (displaying and/or printing and/or VU downloading and/or card downloading)
- period downloaded (if any),
- VRN and Contracting Party registering authority of the controlled vehicle,
- card number and card issuing Contracting Party of the driver card controlled.

234 The control card shall be able to hold at least 230 such records.

5.5 Company card

5.5.1 Card identification

235 The company card shall be able to store the following card identification data:

- card number,
- issuing Contracting Party, issuing authority name, issue date,
- card beginning of validity date, card expiry date (if any).

5.5.2 Card holder identification

236 The company card shall be able to store the following card holder identification data:

- company name,
- company address.

5.5.3 Company activity data

237 The company card shall be able to store the following company activity data:

- date and time of the activity,
- type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading)
- period downloaded (if any),
- VRN and Contracting Party registering authority of vehicle,
- card number and card issuing Contracting Party (in case of card downloading).

238 The company card shall be able to hold at least 230 such records.

V. INSTALLATION OF CONTROL DEVICE

1. Installation

239 New control devices shall be delivered non-activated to fitters or vehicle manufacturers, with all calibration parameters, as listed in Chapter III.20, set to appropriate and valid default values. Where no particular value is appropriate, literal parameters shall be set to strings of "?" and numeric parameters shall be set to "0".

240 Before its activation, the control device shall give access to the calibration function even if not in calibration mode.

241 Before its activation, the control device shall neither record nor store data referred by points III.12.3. to III.12.9. and III.12.12 to III.12.14. inclusive.

242 During installation, vehicle manufacturers shall pre-set all known parameters.

243 Vehicle manufacturers or fitters shall activate the installed control device before the vehicle leaves the premises where the installation took place.

244 The activation of the control device shall be triggered automatically by the first insertion of a workshop card in either of its card interface devices.

245 Specific pairing operations required between the motion sensor and the vehicle unit, if any, shall take place automatically before or during activation.

246 After its activation, the control device shall fully enforce functions and data access rights.

247 The recording and storing functions of the control device shall be fully operational after its activation.

248 Installation shall be followed by a calibration. The first calibration will include entry of VRN and will take place within 2 weeks of this installation or of VRN allocation whichever comes last.

248a The control device must be positioned in the vehicle in such a way as to allow the driver to access the necessary functions from his seat.

2. Installation plaque

249 After the control device has been checked on installation, an installation plaque which is clearly visible and easily accessible shall be affixed on, in or beside the control device. After every inspection by an approved fitter or workshop, a new plaque shall be affixed in place of the previous one.

250 The plaque shall bear at least the following details:

- Name, address or trade name of the approved fitter or workshop,
- Characteristic coefficient of the vehicle, in the form "w = ... imp/km",
- Constant of the control device, in the form "k = ... imp/km",
- Effective circumference of the wheel tyres in the form "l = ... mm",
- Tyre size,
- The date on which the characteristic coefficient of the vehicle was determined and the effective circumference of the wheel tyres measured,
- The Vehicle Identification Number.

3. Sealing

251 The following part shall be sealed:

- Any connection which, if disconnected, would cause undetectable alterations to be made or undetectable data loss;
- The installation plaque, unless it is attached in such a way that it cannot be removed without the markings thereon being destroyed.

252 The seals mentioned above may be removed:

- In case of emergency,
- To install, to adjust or to repair a speed limitation device or any other device contributing to road safety, provided that the control device continues to function reliably and correctly and is resealed by an approved fitter or workshop (in accordance with Chapter VI) immediately after fitting the speed limitation device or any other device contributing to road safety or within seven days in other cases.

253 On each occasion that these seals are broken a written statement giving the reasons for such action shall be prepared and made available to the competent authority.

VI. CHECKS, INSPECTIONS AND REPAIRS

Requirements on the circumstances in which seals may be removed, as referred to in article 9, paragraph 5 of the Annex to this Agreement. are defined in Chapter V, part 3 of this Appendix.

1. Approval of fitters or workshops

The Contracting Parties will approve, regularly control and certify the bodies to carry out:

- installations,
- checks,
- inspections,
- repairs.

In the framework of article 9, paragraph 1 of the Annex to this Agreement workshop cards will be issued only to fitters and/or workshops approved for the activation and/or the calibration of control device in conformity with this Appendix and, unless duly justified:

- who are not eligible for a company card;
- and whose other professional activities do not present a potential compromise of the overall security of the system as defined in sub-appendix 10.

2. Check of new or repaired instruments

254 Every individual device, whether new or repaired, shall be checked in respect of its proper operation and the accuracy of its reading and recordings, within the limits laid down in Chapter III.2.1. and III.2.2 by means of sealing in accordance with Chapter V.3. and calibration.

3. Installation inspection

255 When being fitted to a vehicle, the whole installation (including the control device) shall comply with the provisions relating to maximum tolerances laid down in Chapter III.2.1 and III.2.2.

4. Periodic inspections

256 Periodic inspections of the equipment fitted to the vehicles shall take place after any repair of the equipment, or after any alteration of the characteristic coefficient of the vehicle or of the effective circumference of the tyres, or after equipment UTC time is wrong by more than 20 minutes, or when the VRN has changed, and at least once within two years (24 months) of the last inspection.

257 These inspections shall include the following checks:

- that the control device is working properly, including the data storage in tachograph cards function,
- that compliance with the provisions of chapter III.2.1 and III.2.2 on the maximum tolerances on installation is ensured,
- that the control device carries the type approval mark,
- that the installation plaque is affixed,
- that the seals on the equipment and on the other parts of the installation are intact,
- the tyre size and the actual circumference of the wheel tyres.

258 These inspections shall include a calibration.

5. Measurement of errors

259 The measurement of errors on installation and during use shall be carried out under the following conditions, which are to be regarded as constituting standard test conditions:

- vehicle unladen, in normal running order,
- tyre pressures in accordance with the manufacturer's instructions,
- tyre wear, within the limits allowed by national law,
- vehicle movement:
  - the vehicle shall advance under its own engine power in a straight line on level ground and at a speed of 50 ± 5 km/h. The measuring distance shall be at least 1000m.
- provided that it is of comparable accuracy, alternative methods, such as a suitable test bench, may also be used for the test.

6. Repairs

260 Workshops shall be able to download data from the control device to give the data back to the appropriate transport company.

261 Approved workshops shall issue to transport companies a certificate of data un-downloadability where the malfunction of the control device prevents previously recorded data to be downloaded, even after repair by this workshop. The workshops will keep a copy of each issued certificate for at least one year.

VII. CARD ISSUING

The card issuing processes set-up by the Contracting Parties shall conform to the following:

262 The card number of the first issue of a tachograph card to an applicant shall have a consecutive index (if applicable) and a replacement index and a renewal index set to "0".

263 The card numbers of all non personal tachograph cards issued to a single control body or a single workshop or a single transport company shall have the same first 13 digits, and shall all have a different consecutive index.

264 A tachograph card issued in replacement of an existing tachograph card shall have the same card number than the replaced one except the replacement index which shall be raised by "1" (in the order 0, ..., 9, A, ..., Z).

265 A tachograph card issued in replacement of an existing tachograph card shall have the same card expiry date as the replaced one.

266 A tachograph card issued in renewal of an existing tachograph card shall have the same card number as the renewed one except the replacement index which shall be reset to "0" and the renewal index which shall be raised by "1" (in the order 0, ..., 9, A, ..., Z).

267 The exchange of an existing tachograph card, in order to modify administrative data, shall follow the rules of the renewal if within the same Contracting Party or the rules of a first issue if performed by another Contracting Party.

268 The "card holder surname" for non personal workshop or control cards shall be filled with workshop or control body name.

VIII. Type approval of control device and tachograph cards

1. General points

For the purpose of this chapter, the words "control device" mean control device or its components". No type approval is required for the cable(s) linking the motion sensor to the VU. The paper, for use by the control device, shall be considered as a component of the control device.

269 Control devices shall be submitted for approval complete with any integrated additional devices.

270 Type approval of control devices and of tachograph cards shall include security related tests, functional tests and interoperability tests. Positive results to each of these tests are stated by an appropriate certificate.

271 Contracting Parties type approval authorities will not grant a type approval certificate in accordance with article 2 of the annex to the AETR. as long as they do not hold:

- a security certificate,
- a functional certificate,
- and an interoperability certificate,

for the control device or the tachograph card, subject of the request for type approval.

272 Any modification in software or hardware of the equipment or in the nature of materials used for its manufacture shall, before being used, be notified to the authority which granted type-approval for the equipment. This authority shall confirm to the manufacturer the extension of the type approval, or may require an update or a confirmation of the relevant functional, security and/or interoperability certificates.

273 Procedures to upgrade in-situ control device software shall be approved by the authority which granted type approval for the control device. Software upgrade must not alter nor delete any driver activity data stored in the control device. Software may be upgraded only under the responsibility of the equipment manufacturer.

2. Security certificate

274 The security certificate is delivered in accordance with the provisions of sub-appendix 10 of this Appendix.

3. Functional certificate

275 Each candidate for type approval shall provide the Contracting Party's type approval authority with all the material and documentation that the authority deems necessary.

276 A functional certificate shall be delivered to the manufacturer only after all functional tests specified in sub-appendix 9, at least, have been successfully passed.

277 The type approval authority delivers the functional certificate. This certificate shall indicate, in addition to the name of its beneficiary and the identification of the model, a detailed list of the tests performed and the results obtained.

4. Interoperability certificate

278 Interoperability tests are carried out by a single competent laboratory recognised at the international level.

279 The laboratory shall register interoperability test requests introduced by manufacturers in the chronological order of their arrival.

280 Requests will be officially registered only when the laboratory is in possession of:

- the entire set of material and documents necessary for such interoperability tests,
- the corresponding security certificate,
- the corresponding functional certificate,

The date of the registration of the request shall be notified to the manufacturer.

281 No interoperability tests shall be carried out by the laboratory, for a control device or a tachograph card that have not been granted a security certificate and a functional certificate.

282 Any manufacturer requesting interoperability tests shall commit to leave to the laboratory in charge of these tests the entire set of material and documents which he provided to carry out the tests.

283 The interoperability tests shall be carried out, in accordance with the provisions of paragraph 5 of sub-appendix 9 of this Appendix, with respectively all the types of control devices or tachograph cards:

- for which type approval is still valid or,
- for which type approval is pending and that have a valid interoperability certificate.

284 The interoperability certificate shall be delivered by the laboratory to the manufacturer only after all required interoperability tests have been successfully passed.

285 If the interoperability tests are not successful with one or more of the control device(s) or tachograph card(s), as requested by requirement 283, the interoperability certificate shall not be delivered, until the requesting manufacturer has realised the necessary modifications and has succeeded the interoperability tests. The laboratory shall identify the cause of the problem with the help of the manufacturers concerned by this interoperability fault and shall attempt to help the requesting manufacturer in finding a technical solution. In the case where the manufacturer has modified its product, it is the manufacturer's responsibility to ascertain from the relevant authorities that the security certificate and the functional certificates are still valid.

286 The interoperability certificate is valid for six months. It is revoked at the end of this period if the manufacturer has not received a corresponding type approval certificate. It is forwarded by the manufacturer to the type approval authority of the Contracting Party who has delivered the functional certificate.

287 Any element that could be at the origin of an interoperability fault shall not be used for profit or to lead to a dominant position.

5. Type approval certificate

288 The type approval authority of the Contracting Party may deliver the type approval certificate as soon as it holds the three required certificates.

289 The type approval certificate shall be copied by the type approval authority to the laboratory in charge of the interoperability tests at the time of deliverance to the manufacturer.

290 The laboratory competent for interoperability tests shall run a public web site on which will be updated the list of control devices or tachograph cards models:

- for which a request for interoperability tests have been registered,
- having received an interoperability certificate (even provisional),
- having received a type approval certificate.

6. Reserved

This part (Exceptional procedure: first interoperability certificates) does not concern the AETR.

SUB-APPENDIX I

DATA DICTIONARY

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

I. Introduction

This sub-appendix specifies data formats, data elements, and data structures for use within the control devices and tachograph cards.

1.1 Approach for definitions of data types

This sub-appendix uses Abstract Syntax Notation One (ASN.1) to define data types. This enables simple and structured data to be defined without implying any specific transfer syntax (encoding rules) which will be application and environment dependent.

ASN.1 type naming conventions are done in accordance with ISO/IEC 8824-1. This implies that:

- where possible, the meaning of the data type is implied through the names being selected,
- where a data type is a composition of other data types, the data type name is still a single sequence of alphabetical characters commencing with a capital letter, however capitals are used within the name to impart the corresponding meaning,
- in general, the data types names are related to the name of the data types from which they are constructed, the equipment in which data is stored and the function related to the data.

If an ASN.1 type is already defined as part of another standard and if it is relevant for usage in the control device, then this ASN.1 type will be defined in this sub-appendix.

To enable several types of encoding rules, some ASN.1 types in this sub-appendix are constrained by value range identifiers. The value range identifiers are defined in paragraph 3.

1.2 References

The following references are used in this sub-appendix:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
EN 726-3	Identification cards systems - Telecommunications integrated circuit(s) cards and terminals - Part 3 : Application independent card requirements. December 1994.
ISO 3779	Road vehicles - Vehicle identification number (VIN) - Content and structure. Edition 3: 1983.
ISO/IEC 7816-5	Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996.
ISO/IEC 8824-1	Information technology - Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998.
ISO/IEC 8825-2	Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998.
ISO/IEC 8859-1	Information technology - 8 bit single-byte coded graphic character sets - Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology - 8 bit single-byte coded graphic character sets - Part 7: Latin/Greek alphabet. First edition: 1987.

ISO 16844-3 Road vehicles - Tachograph systems - Motion Sensor Interface. WD 3-20/05/99.

2. Data Type Definitions

For any of the following data types, the default value for an "unknown" or a "not applicable" content will consist in filling the data element with 'FF' bytes.

2.1 ActivityChangeInfo

This data type enables to code, within a two bytes word, a slot status at 00:00 and/or a driver status at 00:00 and/or changes of activity and/or changes of driving status and/or changes of card status for a driver or a co-driver. This data type is related to requirements 084, 109a, 199 and 219.

ActivityChangeInfo ::= OCTET STRING (SIZE(2))

Value assignment – Octet Aligned : 'scpaatttttttttt'B (16 bits)

For Data Memory recordings (or slot status):

's'B Slot:
'0'B: DRIVER,
'1'B: CO-DRIVER,

'c'B Driving status:
'0'B: SINGLE,
'1'B: CREW,

'p'B Driver (or workshop) card status in the relevant slot:
'0'B: INSERTED, a card is inserted,
'1'B: NOT INSERTED, no card is inserted (or a card is withdrawn),

'aa'B Activity:
'00'B: BREAK/REST,
'01'B: AVAILABILITY,
'10'B: WORK,
'11'B: DRIVING,

'ttttttttttt'B Time of the change: Number of minutes since 00h00 on the given day.

For Driver (or Workshop) card recordings (and driver status):

's'B Slot (not relevant when 'p'=1 except note below):
'0'B: DRIVER,
'1'B: CO-DRIVER,

'c'B Driving status (case 'p'=0) or Following activity status (case 'p'=1):
'0'B: SINGLE, '0'B: UNKNOWN
'1'B: CREW, '1'B: KNOWN (=manually entered)

'p'B Card status:
'0'B: INSERTED, the card is inserted in a control device,
'1'B: NOT INSERTED, the card is not inserted (or the card is withdrawn),

'aa'B Activity (not relevant when 'p'=1 and 'c'=0 except note below):
'00'B: BREAK/REST,
'01'B: AVAILABILITY,
'10'B: WORK,
'11'B: DRIVING,

'ttttttttttt'B Time of the change: Number of minutes since 00h00 on the given day.

Note for the case 'card withdrawal':

When the card is withdrawn:

- 's' is relevant and indicates the slot from which the card is withdrawn,
- 'c' must be set to 0,
- 'p' must be set to 1,
- 'aa' must code the current activity selected at that time,

As a result of a manual entry, the bits 'c' and 'aa' of the word (stored in a card) may be overwritten later to reflect the entry.

2.2 Address

An address.

```
Address ::= SEQUENCE {
   codePage                    INTEGER (0..255),
   address                     OCTET STRING (SIZE(35))
}
```

codePage specifies the part of the ISO/IEC 8859 used to code the address,

address is an address coded in accordance with ISO/IEC 8859-codePage.

2.3 BCDString

BCDString is applied for Binary Code Decimal (BCD) representation. This data type is used to represent one decimal digit in one semi octet (4 bits). BCDString is based on the ISO/IEC 8824-1 'CharacterStringType'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString uses an "hstring" notation. The leftmost hexadecimal digit shall be the most significant semi octet of the first octet. To produce a multiple of octets, zero trailing semi octets shall be inserted, as needed, from the leftmost semi octet position in the first octet.

Permitted digits are : 0, 1, .. 9.

2.4 CalibrationPurpose

Code explaining why a set of calibration parameters was recorded. This data type is related to requirements 097 and 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Value assignment:

'00'H reserved value,

'01'H activation: recording of calibration parameters known, at the moment of the VU activation,

'02'H first installation: first calibration of the VU after its activation,

'03'H installation: first calibration of the VU in the current vehicle,

'04' Hperiodic inspection.

2.5 CardActivityDailyRecord

Information, stored in a card, related to the driver activities for a particular calendar day. This data type is related to requirements 199 and 219.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength        INTEGER(0..CardActivityLengthRange),
   activityRecordLength                INTEGER(0..CardActivityLengthRange),
   activityRecordDate                  TimeReal,
   activityDailyPresenceCounter        DailyPresenceCounter,
   activityDayDistance                 Distance,
   activityChangeInfo                  SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength is the total length in bytes of the previous daily record. The maximum value is given by the length of the OCTET STRING containing these records (see CardActivityLengthRange paragraph 3). When this record is the oldest daily record, the value of activityPreviousRecordLength must be set to 0.

activityRecordLength is the total length in bytes of this record. The maximum value is given by the length of the OCTET STRING containing these records.

activityRecordDate is the date of the record.

activityDailyPresenceCounter is the daily presence counter for the card this day.

activityDayDistance is the total distance travelled this day.

activityChangeInfo is the set of ActivityChangeInfo data for the driver this day. It may contain at maximum 1440 values (one activity change per minute). This set always includes the activityChangeInfo coding the driver status at 00:00.

2.6 CardActivityLengthRange

Number of bytes in a driver or a workshop card, available to store driver activity records.

CardActivityLengthRange ::= INTEGER(0..$2^{16}-1$)

Value assignment: see paragraph 3.

2.7 CardApprovalNumber

Type approval number of the card.

Card Approval Number ::= IA5String(SIZE(8))

Value assignment: Unspecified.

2.8 CardCertificate

Certificate of the public key of a card.

CardCertificate ::= Certificate

2.9 CardChipIdentification

Information, stored in a card, related to the identification of the card's Integrated Circuit (IC) (requirement 191).

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                  OCTET STRING (SIZE(4)),
   icManufacturingReferences       OCTET STRING (SIZE(4))
}
```

icSerialNumber is the IC serial number as defined in EN 726-3.

icManufacturingReferences is the IC manufacturer identifier and fabrication elements as defined in EN 726-3.

2.10 CardConsecutiveIndex

A card consecutive index (definition h)).

CardConsecutiveIndex : : = IA5String(SIZE(1))

Value assignment: (see this Appendix, chapter VII)

Order for increase: '0 , ..., 9, A , ... , Z , a , ... , z'

2.11 CardControlActivityDataRecord

Information, stored in a driver or workshop card, related to the last control the driver has been subject to (requirements 210 and 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                     ControlType,
   controlTime                     TimeReal,
   controlCardNumber               FullCardNumber,
   controlVehicleRegistration      VehicleRegistrationIdentification,
   controlDownloadPeriodBegin      TimeReal,
   controlDownloadPeriodEnd        TimeReal
}
```

controlType is the type of the control.

controlTime is the date and time of the control.

controlCardNumber is the FullCardNumber of the control officer having performed the control.

controlVehicleRegistration is the VRN and registering Contracting Party of the vehicle in which the control happened.

controlDownloadPeriodBegin and **controlDownloadPeriodEnd** is the period downloaded, in case of downloading.

2.12 CardCurrentUse

Information about the actual usage of the card (requirement 212).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                  TimeReal,
   sessionOpenVehicle               VehicleRegistrationIdentification
}
```

sessionOpenTime is the time when the card is inserted for the current usage. This element is set to zero at card removal.

sessionOpenVehicle is the identification of the currently used vehicle, set at card insertion. This element is set to zero at card removal.

2.13 CardDriverActivity

Information, stored in a driver or a workshop card, related to the activities of the driver (requirements 199 and 219).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord is the specification of the begin of the storage place (number of bytes from the beginning of the string) of the oldest complete day record in the activityDailyRecords string. The maximum value is given by the length of the string.

activityPointerNewestRecord is the specification of the begin of the storage place (number of bytes from the beginning of the string) of the most recent day record in the activityDailyRecords string. The maximum value is given by the length of the string.

activityDailyRecords is the space available to store the driver activity data (data structure: CardActivityDailyRecord) for each calendar day where the card has been used.

Value assignment: this octet string is cyclically filled with records of CardActivityDailyRecord. At the first use storing is started at the first byte of the string. All new records are appended at the end of the previous one. When the string is full, storing continues at the first byte of the string independently of a break being inside a data element. Before placing new activity data in the string (enlarging current activityDailyRecord, or placing a new activityDailyRecord) that replaces older activity data, activityPointerOldestDayRecord must be updated to reflect the new location of the oldest complete day record, and activityPreviousRecordLength of this (new) oldest complete day record must be reset to 0.

2.14 CardDrivingLicenceInformation

Information, stored in a driver card, related to the card holder driver licence data (requirement 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority        Name,
   drivingLicenceIssuingNation           NationNumeric,
   drivingLicenceNumber                  IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority is the authority responsible for issuing the driving licence.

drivingLicenceIssuingNation is the nationality of the authority that issued the driving licence.

drivingLicenceNumber is the number of the driving licence.

2.15 CardEventData

Information, stored in a driver or workshop card, related to the events associated with the card holder (requirements 204 and 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                      SET SIZE(NoOfEventsPerType) OF
                                         CardEventRecord
}
```

CardEventData is a sequence, ordered by ascending value of EventFaultType, of cardEventRecords (except security breach attempts related records which are gathered in the last set of the sequence).

cardEventRecords is a set of event records of a given event type (or category for security breach attempts events).

2.16 CardEventRecord

Information, stored in a driver or a workshop card, related to an event associated to the card holder (requirements 205 and 223).

```
CardEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   eventVehicleRegistration              Vehicle RegistrationI dentification
}
```

eventType is the type of the event.

eventBeginTime is the date and time of beginning of event.

eventEndTime is the date and time of end of event.

eventVehicleRegistration is the VRN and registering Contracting Party of vehicle in which the event happened.

2.17 CardFaultData

Information, stored in a driver or a workshop card, related to the faults associated to the card holder (requirements 207 and 223).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                    SET SIZE(NoOfFaultsPerType) OF
                                       CardFaultRecord
}
```

CardFaultData is a sequence of control device faults set of records followed by card faults set of records.

cardFaultRecords is a set of fault records of a given fault category (Control device or card).

2.18 CardFaultRecord

Information, stored in a driver or a workshop card, related to a fault associated to the card holder (requirement 208 and 223).

```
CardFaultRecord ::= SEQUENCE {
   faultType                           EventFaultType,
   faultBeginTime                      TimeReal,
   faultEndTime                        TimeReal,
   faultVehicleRegistration            VehicleRegistrationIdentification
}
```

faultType is the type of the fault.

faultBeginTime is the date and time of beginning of fault.

faultEndTime is the date and time of end of fault.

faultVehicleRegistration is the VRN and registering Contracting Party of vehicle in which the fault happened.

2.19 CardIccIdentification

Information, stored in a card, related to the identification of the integrated circuit (IC) card (requirement 192).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                           OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardApprovalNumber                  CardApprovalNumber
   cardPersonaliserID                  OCTET STRING (SIZE(1)),
   embedderIcAssemblerId               OCTET STRING (SIZE(5)),
   icIdentifier                        OCTET STRING (SIZE(2))
}
```

clockStop is the Clockstop mode as defined in EN 726-3.

cardExtendedSerialNumber is the IC card serial number and IC card manufacturing reference as defined in EN 726-3 and as further specified by the ExtendedSerialNumber data type.

cardApprovalNumber is the type approval number of the card.

cardPersonaliserID is the card personaliser ID as defined in EN 726-3.

embedderIcAssemblerId is the embedder/IC assembler identifier as defined in EN 726-3.

icIdentifier is the Identifier of the IC on the card and its IC manufacturer as defined in EN 726-3.

2.20 CardIdentification

Information, stored in a card, related to the identification of the card (requirements 194, 215, 231, 235).

```
CardIdentification ::= SEQUENCE {
   CardIssuingMemberState          NationNumeric,
   cardNumber                      CardNumber,
   cardIssuingAuthorityName        Name,
   cardIssueDate                   Time Real,
   cardValidityBegin               Time Real,
   cardExpiryDate                  Time Real
}
```

cardIssuingMemberState is the code of the Contracting Party issuing the card.

cardNumber is the card number of the card.

cardIssuingAuthorityName is the name of the authority having issued the Card.

cardIssueDate is the issue date of the Card to the current holder.

cardValidityBegin is the first date of validity of the card.

cardExpiryDate is the date when the validity of the card ends.

2.21 CardNumber

A card number as defined by definition (g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification         IA5String(SIZE(14)),
      cardReplacementIndex         CardReplacementIndex,
      cardRenewalIndex             CardRenewalIndex
   },
```

```
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification is the unique identification of a driver in a Contracting Party.

ownerIdentification is the unique identification of a company or a workshop or a control body within a Contracting Party.

cardConsecutiveIndex is the card consecutive index.

cardReplacementIndex is the card replacement index.

cardRenewalIndex is the card renewal index.

The first sequence of the choice is suitable to code a driver card number, the second sequence of the choice is suitable to code workshop, control, and company card numbers.

2.22 CardPlaceDailyWorkPeriod

Information, stored in a driver or a workshop card, related to the places where daily work periods begin and/or end (requirements 202 and 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord is the index of the last updated place record.
Value assignment: Number corresponding to the numerator of the place record, beginning with '0' for the first occurrence of the place records in the structure.

placeRecords is the set of records containing the information related to the places entered..

2.23 CardPrivateKey

The private key of a card.

CardPrivateKey ::= RSAKeyPrivateExponent

2.24 CardPublicKey

The public key of a card.

CardPublicKey ::= PublicKey

2.25 CardRenewalIndex

A card renewal index (definition i)).

CardRenewalIndex ::= IA5String(SIZE(1))

Value assignment: (see this Appendix,chapter VII).
'0' First issue.
Order for increase: '0 , ... , 9 , A , ... , Z'

2.26 CardReplacementIndex

A card replacement index (definition j)).

CardReplacementIndex ::= IA5String(SIZE(1))

Value assignment: (see this Appendix, chapter VII).
'0' Original card.
Order for increase: '0 , ... , 9 , A , ... , Z'

2.27 CardSlotNumber

Code to distinguish between the two slots of a Vehicle Unit.

```
CardSlotNumber ::= INTEGER {
   driverSlot                    (0),
   co-driverSlot                 (1)
}
```

Value assignment : not further specified.

2.28 CardSlotsStatus

Code indicating the type of cards inserted in the two slots of the vehicle unit.

CardSlotsStatus ::= OCTET STRING (SIZE(1))

Value assignment – Octet Aligned : 'ccccdddd'B

'cccc'B Identification of the type of card inserted in the co-driver slot,
'dddd'B Identification of the type of card inserted in the driver slot,

with the following identification codes:
'0000'B no card is inserted,
'0001'B a driver card is inserted,
'0010'B a workshop card is inserted,
'0011'B a control card is inserted,
'0100'B a company card is inserted.

2.29 CardStructureVersion

Code indicating the version of the implemented structure in a tachograph card.

CardStructureVersion ::= OCTET STRING (SIZE(2))

Value assignment: 'aabb'H:

'aa'H Index for changes of the structure,
'00h' for this version

'bb'H Index for changes concerning the use of the data elements defined for the structure given by the high byte, '00h' for this version.

2.30 CardVehicleRecord

Information, stored in a driver or workshop card, related to a period of use of a vehicle during a calendar day (requirements 197 and 217).

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin          OdometerShort,
   vehicleOdometerEnd            OdometerShort,
   vehicleFirstUse               TimeReal,
   vehicleLastUse                TimeReal,
   vehicleRegistration           VehicleRegistrationIdentification,
   vuDataBlockCounter            VuDataBlockCounter
}
```

vehicleOdometerBegin is the vehicle odometer value at the beginning of the period of use of the vehicle.

vehicleOdometerEnd is the vehicle odometer value at the end of the period of use of the vehicle.

vehicleFirstUse is the date and time of the beginning of the period of use of the vehicle.

vehicleLastUse is the date and time of the end of the period of use of the vehicle.

vehicleRegistration is the VRN and the registering Contracting Party of the vehicle.

vuDataBlockCounter is the value of the VuDataBlockCounter at last extraction of the period of use of the vehicle.

2.31 CardVehiclesUsed

Information, stored in a driver or workshop card, related to the vehicles used by the card holder (requirements 197 and 217).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord    INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords            SET SIZE(NoOfCardVehicleRecords) OF
                                 CardVehicleRecord
}
```

vehiclePointerNewestRecord is the index of the last updated vehicle record.
Value assignment: Number corresponding to the numerator of the vehicle record, beginning with '0' for the first occurrence of the vehicle records in the structure.

cardVehicleRecords is the set of records containing information on vehicles used.

2.32 Certificate

The certificate of a public key issued by a Certification Authority.

Certificate ::= OCTET STRING (SIZE(194))

Value assignment: digital signature with partial recovery of a CertificateContent according to sub-appendix 11 common security mechanisms: Signature (128 bytes) || Public Key remainder (58 bytes) || Certification Authority Reference (8 bytes).

2.33 CertificateContent

The (clear) content of the certificate of a public key according to sub-appendix 11 common security mechanisms.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier is the version of the corresponding certificate.
Value assignment: '01h' for this version.

certificationAuthorityReference identifies the Certification Authority issuing the certificate. It also references the Public Key of this Certification Authority.

certificateHolderAuthorisation identifies the rights of the certificate holder.

certificateEndOfValidity is the date when the certificate expires administratively.

certificateHolderReference identifies the certificate holder. It also references his Public Key.

publicKey is the public key that is certified by this certificate.

2.34 CertificateHolderAuthorisation

Identification of the rights of a certificate holder.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID               OCTET STRING(SIZE(6))
   equipmentType                         EquipmentType
}
```

tachographApplicationID is the application identifier for the tachograph application.
Value assignment: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. This AID is a proprietary non registered application identifier in accordance with ISO/IEC 7816-5.

equipmentType is the identification of the type of equipment to which the certificate is intended.
Value assignment: in accordance with EquipmentType data type. **0** if certificate is the one of a Contracting Party.

2.35 CertificateRequestID

Unique identification of a certificate request. It can also be used as a Vehicle Unit Public Key Identifier if the serial number of the vehicle Unit to which the key is intended is not known at certificate generation time.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber          INTEGER(0..2^32-1)
   requestMonthYear             BCDString(SIZE(2))
   crIdentifier                 OCTET STRING(SIZE(1))
   manufacturerCode             ManufacturerCode
}
```

requestSerialNumber is a serial number for the certificate request, unique for the manufacturer and the month below.

requestMonthYear is the identification of the month and the year of the certificate request.
Value assignment: BCD coding of Month (two digits) and Year (two last digits).

crIdentifier: is an identifier to distinguish a certificate request from an extended serial number.
Value assignment: 'FFh'.

manufacturerCode: is the numerical code of the manufacturer requesting the certificate.

2.36 CertificationAuthorityKID

Identifier of the Public Key of a Certification Authority (a Contracting Party or the European Certification Authority)

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                NationNumeric
   nationAlpha                  NationAlpha
   keySerialNumber              INTEGER(0..255)
   additionalInfo               OCTET STRING(SIZE(2))
   caIdentifier                 OCTET STRING(SIZE(1))
}
```

nationNumeric is the numerical nation code of the Certification Authority.

nationAlpha is the alphanumerical nation code of the Certification Authority.

keySerialNumber is a serial number to distinguish the different keys of the Certification Authority in the case keys are changed.

additionalInfo is a two byte field for additional coding (Certification Authority specific).

caIdentifier is an identifier to distinguish a Certification Authority Key Identifier from other Key Identifiers.
Value assignment: '01h'.

2.37 CompanyActivityData

Information, stored in a company card, related to activities performed with the card (requirement 237).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord          INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords              SET SIZE(NoOfCompanyActivityRecords) OF
      companyActivityRecord             SEQUENCE {
      companyActivityType                 CompanyActivityType,
      companyActivityTime                 TimeReal,
      cardNumberInformation               FullCardNumber,
      vehicleRegistrationInformation      VehicleRegistrationIdentification,
      downloadPeriodBegin                 TimeReal,
      downloadPeriodEnd                   TimeReal
    }
}
```

companyPointerNewestRecord is the index of the last updated companyActivityRecord.
Value assignment: Number corresponding to the numerator of the company activity record, beginning with '0' for the first occurrence of the company activity record in the structure.

companyActivityRecords is the set of all company activity records.

companyActivityRecord is the sequence of information related to one company activity.

companyActivityType is the type of the company activity.

companyActivityTime is the date and time of the company activity.

cardNumberInformation is the card number and the card issuing Contracting Party of the card downloaded, if any.

vehicleRegistrationInformation is the VRN and registering Contracting Party of the vehicle downloaded or locked in or out..

downloadPeriodBegin and **downloadPeriodEnd** is the period downloaded from the VU, if any.

2.38 CompanyActivityType

Code indicating an activity carried out by a company using its company card..

```
CompanyActivityType ::= INTEGER {
   card downloading          (1),
   VU downloading            (2),
   VU lock-in                (3),
   VU lock-out               (4)
}
```

2.39 CompanyCardApplicationIdentification

Information, stored in a company card related to the identification of the application of the card (requirement 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId is specifying the implemented type of card.

cardStructureVersion is specifying the the version of the structure that is implemented in the card.

noOfCompanyActivityRecords is the number of company activity records the card can store.

2.40 CompanyCardHolderIdentification

Information, stored in a company card, related to the cardholder identification (requirement 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName is the name of the holder company.

companyAddress is the address of the holder company.

cardHolderPreferredLanguage is the preferred language of the card holder.

2.41 ControlCardApplicationIdentification

Information, stored in a control card related to the identification of the application of the card (requirement 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId is specifying the implemented type of card.

cardStructureVersion is specifying the version of the structure that is implemented in the card.

noOfControlActivityRecords is the number of control activity records the card can store.

2.42 ControlCardControlActivityData

Information, stored in a control card, related to control activity performed with the card (requirement 233).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord          INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords              SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord               SEQUENCE {
      controlType                        ControlType,
      controlTime                        TimeReal,
      controlledCardNumber               FullCardNumber,
      controlledVehicleRegistration      VehicleRegistrationIdentification,
      controlDownloadPeriodBegin         TimeReal,
      controlDownloadPeriodEnd           TimeReal
    }
}
```

controlPointerNewestRecord is the index of the last updated control activity record.
Value assignment: Number corresponding to the numerator of the control activity record, beginning with '0' for the first occurrence of the control activity record in the structure.

controlActivityRecords is the set of all control activity records.

controlActivityRecord is the sequence of information related to one control.

controlType is the type of the control.

controlTime is the date and time of the control.

controlledCardNumber is the card number and the card issuing Contracting Party of the card controlled.

controlledVehicleRegistration is the VRN and registering Contracting Party of the vehicle in which the control happened.

controlDownloadPeriodBegin and **controlDownloadPeriodEnd** is the period eventually downloaded.

2.43 ControlCardHolderIdentification

Information, stored in a control card, related to the identification of the cardholder (requirement 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                  Name,
   controlBodyAddress               Address,
   cardHolderName                   HolderName,
   cardHolderPreferredLanguage      Language
}
```

controlBodyName is the name of the control body of the card holder.

controlBodyAddress is the address of the control body of the card holder.

cardHolderName is the name and first name(s) of the holder of the Control Card.

cardHolderPreferredLanguage is the preferred language of the card holder.

2.44 ControlType

Code indicating the activities carried out during a control. This data type is related to requirements 102, 210 and 225.

ControlType ::= OCTET STRING (SIZE(1))

Value assignment – Octet aligned : 'cvpdxxxx'B (8 bits)

'c'B card downloading:
'0'B: card not downloaded during this control activity,
'1'B: card downloaded during this control activity

'v'B VU downloading:
'0'B: VU not downloaded during this control activity,
'1'B: VU downloaded during this control activity

'p'B printing:
'0'B: no printing done during this control activity,
'1'B: printing done during this control activity

'd'B display:
'0'B: no display used during this control activity,
'1'B: display used during this control activity

'xxxx'B Not used.

2.45 CurrentDateTime

The current date and time of the control device.

CurrentDateTime ::= TimeReal

Value assignment: not further specified.

2.46 DailyPresenceCounter

Counter, stored in a driver or workshop card, increased by one for each calendar day the card has been inserted in a VU. This data type is related to requirements 199 and 219.

DailyPresenceCounter ::= BCDString(SIZE(2))

Value assignment: Consecutive Number with maximum value = 9 999, starting again with 0. At the time of first issuing of the card the number is set to 0.

2.47 Datef

Date expressed in a readily printable numeric format.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Value assignment:

yyyy Year
mm Month
dd Day
'00000000'H denotes explicitly no date.

2.48 Distance

A distance travelled (result of the calculation of the difference between two vehicle's odometer value in kilometres).

Distance ::= INTEGER(0..2^{16}-1)

Value assignment: Unsigned binary. Value in km in the operational range 0 to 9 999 km.

2.49 DriverCardApplicationIdentification

Information, stored in a driver card related to the identification of the application of the card (requirement 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId          EquipmentType,
   cardStructureVersion            CardStructureVersion,
   noOfEventsPerType               NoOfEventsPerType,
   noOfFaultsPerType               NoOfFaultsPerType,
   activityStructureLength         CardActivityLengthRange,
   noOfCardVehicleRecords          NoOfCardVehicleRecords,
   noOfCardPlaceRecords            NoOfCardPlaceRecords
}
```

typeOfTachographCardId is specifying the implemented type of card.

cardStructureVersion is specifying the the version of the structure that is implemented in the card.

noOfEventsPerType is the number of events per type of event the card can record.

noOfFaultsPerType is the number of faults per type of fault the card can record.

activityStructureLength indicates the number of bytes available for storing activity records..

noOfCardVehicleRecords is the number of vehicle records the card can contain.

noOfCardPlaceRecords is the number of places the card can record.

2.50 DriverCardHolderIdentification

Information, stored in a driver card, related to the identification of the cardholder (requirement 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                  HolderName,
   cardHolderBirthDate             Datef,
   cardHolderPreferredLanguage     Language
}
```

cardHolderName is the name and first name(s) of the holder of the Driver Card.

cardHolderBirthDate is the date of birth of the holder of the Driver Card.

cardHolderPreferredLanguage is the preferred language of the card holder.

2.51 EntryTypeDailyWorkPeriod

Code to distinguish between begin and end for an entry of a daily work period place and condition of the entry.

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,   related time = card insertion time or time of entry      (0),
   End,     related time = card withdrawal time or time of entry     (1),
   Begin,   related time manually entered (start time)               (2),
   End,     related time manually entered (end of work period)       (3),
   Begin,   related time assumed by VU                               (4),
   End,     related time assumed by VU                               (5)
}
```

Value assignment : according to ISO/IEC8824-1.

2.52 EquipmentType

Code to distinguish different types of equipment for the tachograph application.

```
EquipmentType ::= INTEGER(0..255)
--Reserved                    (0),
--Driver Card                 (1),
--Workshop Card               (2),
--Control Card                (3),
--Company Card                (4),
--Manufacturing Card          (5),
--Vehicle Unit                (6),
--Motion Sensor               (7),
--RFU                         (8..255)
```

Value assignment: According to ISO/IEC8824-1.

Value 0 is reserved for the purpose of designating a Contracting Party or Europe in the CHA field of certificates.

2.53 EuropeanPublicKey

The European public key.

EuropeanPublicKey ::= PublicKey

2.54 EventFaultType

Code qualifying an event or a fault.

EventFaultType ::= OCTET STRING (SIZE(1))

Value assignment:

'0x'H	General events,
'00'H	No further details,
'01'H	Insertion of a non valid card,
'02'H	Card conflict,
'03'H	Time overlap,
'04'H	Driving without an appropriate card,
'05'H	Card insertion while driving,
'06'H	Last card session not correctly closed,
'07'H	Over speeding,

'08'H	Power supply interruption,
'09'H	Motion data error,
'0A'H to '0F'H	RFU,
'1x'H	Vehicle unit related security breach attempt events,
'10'H	No further details,
'11'H	Motion sensor authentication failure,
'12'H	Tachograph card authentication failure,
'13'H	Unauthorised change of motion sensor,
'14'H	Card data input integrity error
'15'H	Stored user data integrity error,
'16'H	Internal data transfer error,
'17'H	Unauthorised case opening,
'18'H	Hardware sabotage,
'19'H to '1F'H	RFU,
'2x'H	Sensor related security breach attempt events,
'20'H	No further details,
'21'H	Authentication failure,
'22'H	Stored data integrity error,
'23'H	Internal data transfer error,
'24'H	Unauthorised case opening,
'25'H	Hardware sabotage,
'26'H to '2F'H	RFU,
'3x'H	Control device faults,
'30'H	No further details,
'31'H	VU internal fault,
'32'H	Printer fault,
'33'H	Display fault,
'34'H	Downloading fault,
'35'H	Sensor fault,
'36'H to '3F'H	RFU,
'4x'H	Card faults,
'40'H	No further details,
'41'H to '4F'H	RFU,
'50'H to '7F'H	RFU,
'80'H to 'FF'H	Manufacturer specific.

2.55 EventFaultRecordPurpose

Code explaining why an event or a fault has been recorded.

EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))

Value assignment:

'00'H	one of the 10 most recent (or last) events or faults
'01'H	the longest event for one of the last 10 days of occurrence
'02'H	one of the 5 longest events over the last 365 days
'03'H	the last event for one of the last 10 days of occurrence
'04'H	the most serious event for one of the last 10 days of occurrence
'05'H	one of the 5 most serious events over the last 365 days
'06'H	the first event or fault having occurred after the last calibration
'07'H	an active/on-going event or fault
'08'H to '7F'H	RFU
'80'H to 'FF'H	manufacturer specific

2.56 ExtendedSerialNumber

Unique identification of an equipment. It can also be used as an equipment Public Key Identifier.

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                    INTEGER(0..2^32-1)
   monthYear                       BCDString(SIZE(2))
   type                            OCTET STRING(SIZE(1))
   manufacturerCode                ManufacturerCode
}
```

serialNumber is a serial number for the equipment, unique for the manufacturer, the equipment's type and the month below.

monthYear is the identification of the month and the year of manufacturing (or of serial number assignment).
Value assignment: BCD coding of Month (two digits) and Year (two last digits).

type is an identifier of the type of equipment.
Value assignment: manufacturer specific, with 'FFh' reserved value.

manufacturerCode: is the numerical code of the manufacturer of the equipment.

2.57 FullCardNumber

Code fully identifying a tachograph card.

```
FullCardNumber ::= SEQUENCE {
   cardType                        EquipmentType,
   cardIssuingMemberState          NationNumeric,
   cardNumber                      CardNumber
}
```

cardType is the type of the tachograph card.

cardIssuingMemberState is the code of the Contracting Party having issued the card.

cardNumber is the card number.

2.58 HighResOdometer

Odometer value of the vehicle: Accumulated distance travelled by the vehicle during its operation.

HighResOdometer ::= INTEGER(0..2^{32}-1)

Value assignment: Unsigned binary. Value in 1/200 km in the operating range 0 to 21 055 406 km.

2.59 HighResTripDistance

A distance travelled during all or part of a journey.

HighResTripDistance ::= INTEGER(0..2^{32}-1)

Value assignment: Unsigned binary. Value in 1/200 km in the operating range 0 to 21 055 406 km.

2.60 HolderName

The surname and first name(s) of a card holder.

```
HolderName ::= SEQUENCE {
   holderSurname                Name,
   holderFirstNames             Name
}
```

holderSurname is the surname (family name) of the holder. This surname does not include titles.

Value assignment: When a card is not personal, holderSurname contains the same information as companyName or workshopName or controlBodyName.

holderFirstNames is the first name(s) and initials of the holder.

2.61 K-ConstantOfRecordingEquipment

Constant of the control device (definition m)).

K-ConstantOfRecordingEquipment ::= INTEGER(0..2^{16}-1)

Value assignment: Pulses per kilometre in the operating range 0 to 64 255 pulses/km.

2.62 KeyIdentifier

A unique identifier of a Public Key used to reference and select the key. It also identifies the holder of the key.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber         ExtendedSerialNumber,
   certificateRequestID         CertificateRequestID,
   certificationAuthorityKID    CertificationAuthorityKID
}
```

The first choice is suitable to reference the public key of a Vehicle Unit or of a tachograph card.

The second choice is suitable to reference the public key of a Vehicle Unit (in the case the serial number of the Vehicle Unit cannot be known at certificate generation time).

The third choice is suitable to reference the public key of a Contracting Party .

2.63 L-TyreCircumference

Effective circumference of the wheel tyres (definition u)).

L-TyreCircumference ::= INTEGER(0.. 2^{16}-1)

Value assignment: Unsigned binary, value in 1/8 mm in the operating range 0 to 8 031 mm.

2.64 Language

Code identifying a language.

Language ::= IA5String(SIZE(2))

Value assignment: Two-letter lower-case coding according to ISO 639.

2.65 LastCardDownload

Date and time, stored on a driver card, of last card download (for other purposes than control). This date is updateable by a VU or any card reader.

LastCardDownload ::= TimeReal

Value assignment : not further specified.

2.66 ManualInputFlag

Code identifying whether a cardholder has manually entered driver activities at card insertion or not (requirement 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                    (0)
   manualEntries              (1)
}
```

Value assignment : not further specified.

2.67 ManufacturerCode

Code identifying a manufacturer.[13]

ManufacturerCode ::= INTEGER(0..255)

Value assignment :

'00'H	No information available
'01'H	Reserved value
'02'H .. '0F'H	Reserved for Future Use
'10'H	ACTIA
'11'H .. '17'H	Reserved for manufacturers which name begins with 'A'
'18'H .. '1F'H	Reserved for manufacturers which name begins with 'B'
'20'H .. '27'H	Reserved for manufacturers which name begins with 'C'
'28'H .. '2F'H	Reserved for manufacturers which name begins with 'D'
'30'H .. '37'H	Reserved for manufacturers which name begins with 'E'
'38'H .. '3F'H	Reserved for manufacturers which name begins with 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus

[13] An updated list of codes identifying the manufacturers is available on the website of the European Certification Authority at this address: http://dtc.jrc.ec.europa.eu/text/cm.html

'42'H .. '47'H	Reserved for manufacturers which name begins with 'G'
'48'H .. '4F'H	Reserved for manufacturers which name begins with 'H'
'50'H .. '57'H	Reserved for manufacturers which name begins with 'I'
'58'H .. '5F'H	Reserved for manufacturers which name begins with 'J'
'60'H .. '67'H	Reserved for manufacturers which name begins with 'K'
'68'H .. '6F'H	Reserved for manufacturers which name begins with 'L'
'70'H .. '77'H	Reserved for manufacturers which name begins with 'M'
'78'H .. '7F'H	Reserved for manufacturers which name begins with 'N'
'80'H	OSCARD
'81'H .. '87'H	Reserved for manufacturers which name begins with 'O'
'88'H .. '8F'H	Reserved for manufacturers which name begins with 'P'
'90'H .. '97'H	Reserved for manufacturers which name begins with 'Q'
'98'H .. '9F'H	Reserved for manufacturers which name begins with 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H.. 'A7'H	Reserved for manufacturers which name begins with 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reserved for manufacturers which name begins with 'T'
'B0'H .. 'B7'H	Reserved for manufacturers which name begins with 'U'
'B8'H .. 'BF'H	Reserved for manufacturers which name begins with 'V'
'C0'H .. 'C7'H	Reserved for manufacturers which name begins with 'W'
'C8'H .. 'CF'H	Reserved for manufacturers which name begins with 'X'
'D0'H .. 'D7'H	Reserved for manufacturers which name begins with 'Y'
'D8'H .. 'DF'H	Reserved for manufacturers which name begins with 'Z'

2.68 MemberStateCertificate

The certificate of the public key of a Contracting Party issued by the European Certification Authority..

MemberStateCertificate ::= Certificate

2.69 MemberStatePublicKey

The public key of a Contracting Party .

MemberStatePublicKey ::= PublicKey

2.70 Name

A name.

```
Name ::= SEQUENCE {
   codePage                    INTEGER (0..255),
   name                        OCTET STRING (SIZE(35))
}
```

codePage specifies the part of the ISO/IEC 8859 used to code the name,

name is a name coded in accordance with ISO/IEC 8859-codePage.

2.71 NationAlpha

Alphabetic reference to a country, in accordance with the conventional coding of countries (distinguishing signs) which is displayed at the rear of vehicles (either separately from the registration plate or incorporated into the registration plate) and/or mentioned in the green cards issued by the insurance companies.

NationAlpha ::= IA5String(SIZE(3))

Value assignment:

' '	No information available,
'A '	Austria,
'AL '	Albania,
'AND'	Andorra,
'ARM'	Armenia,
'AZ '	Azerbaijan,
'B '	Belgium,
'BG '	Bulgaria,
'BIH'	Bosnia and Herzegovina,
'BY '	Belarus,
'CH '	Switzerland,
'CY '	Cyprus,
'CZ '	Czech Republic,
'D '	Germany,
'DK '	Denmark,
'E '	Spain,
'EST'	Estonia,
'F '	France,
'FIN'	Finland,
'FL '	Liechtenstein,
'FR '	Faeroe Islands,
'UK '	United Kingdom, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar,
'GE '	Georgia,
'GR '	Greece,
'H '	Hungary,
'HR'	Croatia,
'I '	Italy,
'IRL'	Ireland,
'IS '	Iceland,
'KZ '	Kazakhstan,
'L '	Luxembourg,
'LT '	Lithuania,
'LV '	Latvia,
'M '	Malta,
'MC '	Monaco,
'MD '	Republic of Moldova,
'MK '	The former Yugoslav Rep. of Macedonia,
'N '	Norway,
'NL '	The Netherlands,
'P '	Portugal,
'PL '	Poland,
'RO '	Romania,

'RSM'	San Marino,
'RUS'	Russian Federation,
'S '	Sweden,
'SK '	Slovakia,
'SLO'	Slovenia,
'SRB'	Serbia,
'TM '	Turkmenistan,
'TR '	Turkey,
'UA '	Ukraine,
'V '	Vatican City,
'UNK'	Unknown,
'EC '	European Community,
'EUR'	Rest of Europe,
'WLD'	Rest of the world.

2.72 NationNumeric

Numerical reference to a country.

NationNumeric ::= INTEGER(0 .. 255)

Value assignment :

-- No information available	(00)H,
-- Austria	(01)H,
-- Albania	(02)H,
-- Andorra	(03)H,
-- Armenia	(04)H,
-- Azerbaijan	(05)H,
-- Belgium	(06)H,
-- Bulgaria	(07)H,
-- Bosnia and Herzegovina	(08)H,
-- Belarus	(09)H,
-- Switzerland	(0A)H,
-- Cyprus	(0B)H,
-- Czech Republic	(0C)H,
-- Germany	(0D)H,
-- Denmark	(0E)H,
-- Spain	(0F)H,
-- Estonia	(10)H,
-- France	(11)H,
-- Finland	(12)H,
-- Liechtenstein	(13)H,
-- Faeroe Islands	(14)H,
-- United Kingdom	(15)H,
-- Georgia	(16)H,
-- Greece	(17)H,
-- Hungary	(18)H,
-- Croatia	(19)H,
-- Italy	(1A)H,
-- Ireland	(1B)H,
-- Iceland	(1C)H,
-- Kazakhstan	(1D)H,

```
-- Luxembourg                          (1E)H,
-- Lithuania                           (1F)H,
-- Latvia                              (20)H,
-- Malta                               (21)H,
-- Monaco                              (22)H,
-- Republic of Moldova                 (23)H,
-- The former Yugoslav Rep.
   of Macedonia                        (24)H,
-- Norway                              (25)H,
-- Netherlands                         (26)H,
-- Portugal                            (27)H,
-- Poland                              (28)H,
-- Romania                             (29)H,
-- San Marino                          (2A)H,
-- Russian Federation                  (2B)H,
-- Sweden                              (2C)H,
-- Slovakia                            (2D)H,
-- Slovenia                            (2E)H,
-- Turkmenistan                        (2F)H,
-- Turkey                              (30)H,
-- Ukraine                             (31)H,
-- Vatican City                        (32)H,
-- Serbia                              (33)H,
-- RFU                                 (34 .. FC)H,
-- European Community                  (FD)H,
-- Rest of Europe                      (FE)H,
-- Rest of the world                   (FF)H
```

2.73 NoOfCalibrationRecords

Number of calibration records, a workshop card can store.

NoOfCalibrationRecords ::= INTEGER(0..255)

Value assignment: see paragraph 3.

2.74 NoOfCalibrationsSinceDownload

Counter indicating the number of calibrations performed with a workshop card since its last download (requirement 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1),

Value assignment: Not specified further.

2.75 NoOfCardPlaceRecords

Number of place records a driver or workshop card can store.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Value assignment: see paragraph 3.

2.76 NoOfCardVehicleRecords

Number of vehicles used records a driver or workshop card can store.

NoOfCardVehicleRecords ::= INTEGER(0.. 2^{16}-1)

Value assignment: see paragraph 3.

2.77 NoOfCompanyActivityRecords

Number of company activity records, a company card can store.

NoOfCompanyActivityRecords ::= INTEGER(0.. 2^{16}-1)

Value assignment: see paragraph 3.

2.78 NoOfControlActivityRecords

Number of control activity records, a control card can store.

NoOfControlActivityRecords ::= INTEGER(0.. 2^{16}-1)

Value assignment: see paragraph 3.

2.79 NoOfEventsPerType

Number of events per type of event a card can store.

NoOfEventsPerType ::= INTEGER(0..255)

Value assignment: see paragraph 3.

2.80 NoOfFaultsPerType

Number of faults per type of fault a card can store.

NoOfFaultsPerType ::= INTEGER(0..255)

Value assignment: see paragraph 3.

2.81 OdometerValueMidnight

The vehicle's odometer value at midnight on a given day (requirement 090).

OdometerValueMidnight ::= OdometerShort

Value assignment: not further specified.

2.82 OdometerShort

Odometer value of the vehicle in a short form.

OdometerShort ::= INTEGER(0..2^{24}-1)

Value assignment: Unsigned binary. Value in km in the operating range 0 to 9 999 999 km.

2.83 OverspeedNumber

Number of over speeding events since the last over speeding control.

OverspeedNumber ::= INTEGER(0..255)

Value assignment : 0 means that no over speeding event has occurred since the last over speeding control , 1 means that one over speeding event has occurred since the last over speeding control ...255 means that 255 or more over speeding events have occurred since the last over speeding control.

2.84 PlaceRecord

Information related to a place where a daily work period begins or ends (requirements 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort
}
```

entryTime is a date and time related to the entry.

entryTypeDailyWorkPeriod is the type of entry.

dailyWorkPeriodCountry is the country entered.

dailyWorkPeriodRegion is the region entered.

vehicleOdometerValue is the odometer value at the time of place entry.

2.85 PreviousVehicleInfo

Information related to the vehicle previously used by a driver when inserting his card in a vehicle unit (requirement 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   cardWithdrawalTime                   TimeReal
}
```

vehicleRegistrationIdentification is the VRN and the registering Contracting Party of the vehicle.

cardWithdrawalTime is the card withdrawal date and time.

2.86 PublicKey

A public RSA key.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus is the Modulus of the key pair.

rsaKeyPublicExponent is the public exponent of the key pair.

2.87 RegionAlpha

Alphabetic reference to a region within a specified country.

RegionAlpha ::= IA5STRING(SIZE(3))

Value assignment:

‘ ’	No information available,
Spain:	
‘AN ’	Andalucía,
‘AR ’	Aragón,
‘AST’	Asturias,
‘C ’	Cantabria,
‘CAT’	Cataluña,
‘CL ’	Castilla-León,
‘CM ’	Castilla-La-Mancha,
‘CV’	Valencia,
‘EXT’	Extremadura,
‘G ’	Galicia,
‘IB ’	Baleares,
‘IC ’	Canarias,
‘LR ’	La Rioja,
‘M ’	Madrid,
‘MU ’	Murcia,
‘NA ’	Navarra,
‘PV ’	País Vasco

2.88 RegionNumeric

Numerical reference to a region within a specified country.

RegionNumeric ::= OCTET STRING (SIZE(1))

Value assignment:

‘00’H	No information available,
Spain:	
‘01’H	Andalucía,
‘02’H	Aragón,
‘03’H	Asturias,
‘04’H	Cantabria,
‘05’H	Cataluña,
‘06’H	Castilla-León,
‘07’H	Castilla-La-Mancha,
‘08’H	Valencia,
‘09’H	Extremadura,
‘0A’H	Galicia,
‘0B’H	Baleares,
‘0C’H	Canarias,
‘0D’H	La Rioja,
‘0E’H	Madrid,
‘0F’H	Murcia,
‘10’H	Navarra,
‘11’H	País Vasco

2.89 RSAKeyModulus

The modulus of a RSA key pair.

RSAKeyModulus ::= OCTET STRING (SIZE(128))

Value assignment: Unspecified.

2.90 RSAKeyPrivateExponent

The private exponent of a RSA key pair.

RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))

Value assignment: Unspecified.

2.91 RSAKeyPublicExponent

The public exponent of a RSA key pair.

RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))

Value assignment: Unspecified.

2.92 SensorApprovalNumber

Type approval number of the sensor.

SensorApprovalNumber ::= IA5String(SIZE(8))

Value assignment: Unspecified.

2.93 SensorIdentification

Information, stored in a motion sensor, related to the identification of the motion sensor (requirement 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber          SensorSerialNumber,
   sensorApprovalNumber        SensorApprovalNumber,
   sensorSCIdentifier          SensorSCIdentifier,
   sensorOSIdentifier          SensorOSIdentifier
}
```

sensorSerialNumber is the extended serial number of the motion sensor (includes part number and manufacturer code).

sensorApprovalNumber is the approval number of the motion sensor.

sensorSCIdentifier is the identifier of the security component of the motion sensor.

sensorOSIdentifier is the identifier of the operating system of the motion sensor.

2.94 SensorInstallation

Information, stored in a motion sensor, related to the installation of the motion sensor (requirement 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst          SensorPairingDate,
   firstVuApprovalNumber           VuApprovalNumber,
   firstVuSerialNumber             VuSerialNumber,
   sensorPairingDateCurrent        SensorPairingDate,
   currentVuApprovalNumber         VuApprovalNumber,
   currentVUSerialNumber           VuSerialNumber
}
```

sensorPairingDateFirst is the date of the first pairing of the motion sensor with a vehicle unit.

firstVuApprovalNumber is the approval number of the first vehicle unit paired with the motion sensor.

firstVuSerialNumber is the serial number of the first vehicle unit paired with the motion sensor.

sensorPairingDateCurrent is the date of the current pairing of the motion sensor with the vehicle unit.

currentVuApprovalNumber is the approval number of the vehicle unit currently paired with the motion sensor.

currentVUSerialNumber is the serial number of the vehicle unit currently paired with the motion sensor.

2.95 SensorInstallationSecData

Information, stored in a workshop card, related to the security data needed for pairing motion sensors to vehicle units (requirement 214).

SensorInstallationSecData ::= TDesSessionKey

Value assignment: in accordance with ISO 16844-3.

2.96 SensorOSIdentifier

Identifier of the operating system of the motion sensor.

SensorOSIdentifier ::= IA5String(SIZE(2))

Value assignment: manufacturer specific.

2.97 SensorPaired

Information, stored in a vehicle unit, related to the identification of the motion sensor paired with the vehicle unit (requirement 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber              SensorSerialNumber,
   sensorApprovalNumber            SensorApprovalNumber,
   sensorPairingDateFirst          SensorPairingDate
}
```

sensorSerialNumber is the serial number of the motion sensor currently paired with the vehicle unit.

sensorApprovalNumber is the approval number of the motion sensor currently paired with the vehicle unit.

sensorPairingDateFirst is the date of the first pairing with a vehicle unit of the motion sensor currently paired with the vehicle unit.

2.98 SensorPairingDate

Date of a pairing of the motion sensor with a vehicle unit.

SensorPairingDate ::= TimeReal

Value assignment: Unspecified.

2.99 SensorSerialNumber

Serial number of the motion sensor.

SensorSerialNumber ::= ExtendedSerialNumber

2.100 SensorSCIdentifier

Identifier of the security component of the motion sensor.

SensorSCIdentifier ::= IA5String(SIZE(8))

Value assignment: component manufacturer specific.

2.101 Signature

A digital signature.

Signature ::= OCTET STRING (SIZE(128))

Value assignment: in accordance with sub-appendix 11 Common security mechanisms.

2.102 SimilarEventsNumber

The number of similar events for one given day (requirement 094).

SimilarEventsNumber ::= INTEGER(0..255)

Value assignment : 0 is not used, 1 means that only one event of that type has occurred and has been stored on that day, 2 means that 2 events of that type has occurred on that day (one only has been stored), ...255 means that 255 or more events of that type have occurred on that day.

2.103 SpecificConditionType

Code identifying a specific condition (requirements 050b, 105a, 212a and 230a).

SpecificConditionType ::= INTEGER(0..255)

Value assignment :

'00'H RFU
'01'H Out of scope – Begin
'02'H Out of scope – End
'03'H Ferry / Train crossing
'04'H .. 'FF'HRFU

2.104 SpecificConditionRecord

Information, stored in a driver card, a workshop card or a vehicle unit, related to a specific condition (requirements 105a, 212a and 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                    TimeReal,
   specificConditionType        SpecificConditionType
}
```

entryTime is the date and time of the entry.

specificConditionType is the code identifying the specific condition.

2.105 Speed

Speed of the vehicle (km/h).

Speed ::= INTEGER(0..255)

Value assignment: kilometre per hour in the operational range 0 to 220 km/h.

2.106 SpeedAuthorised

Maximum authorised Speed of the vehicle (definition bb)).

SpeedAuthorised ::= Speed

2.107 SpeedAverage

Average speed in a previously defined duration (km/h).

SpeedAverage ::= Speed

2.108 SpeedMax

Maximum speed measured in a previously defined duration.

SpeedMax ::= Speed

2.109 TDesSessionKey

A triple DES session key.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                     OCTET STRING (SIZE(8))
   tDesKeyB                     OCTET STRING (SIZE(8))
}
```

Value assignment: not further specified.

2.110 TimeReal

Code for a combined date and time field, where the date and time are expressed as seconds past 00h.00m.00s. on 1 January 1970 GMT.

TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)

Value assignment – Octet Aligned: Number of seconds since midnight 1 January 1970 GMT.

The max. possible date/time is in the year 2106.

2.111 TyreSize

Designation of tyre dimensions.

TyreSize ::= IA5String(SIZE(15))

Value assignment: in accordance with ECE Regulation N°54[14].

2.112 VehicleIdentificationNumber

Vehicle Identification Number (VIN) referring to the vehicle as a whole, normally chassis serial number or frame number.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Value assignment: As defined in ISO 3779.

2.113 VehicleRegistrationIdentification

Identification of a vehicle, unique for Europe (VRN and Contracting Party)

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation          NationNumeric,
   vehicleRegistrationNumber          VehicleRegistrationNumber
}
```

vehicleRegistrationNation is the nation where the vehicle is registered.

vehicleRegistrationNumber is the registration number of the vehicle (VRN).

2.114 VehicleRegistrationNumber

Registration number of the vehicle (VRN). The registration number is assigned by the vehicle licensing authority.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                           INTEGER (0..255),
   vehicleRegNumber                   OCTET STRING (SIZE(13))
}
```

codePage specifies the part of the ISO/IEC 8859 used to code the vehicleRegNumber,

vehicleRegNumber is a VRN coded in accordance with ISO/IEC 8859-codePage.

Value assignment: Country specific.

2.115 VuActivityDailyData

Information, stored in a VU, related to changes of activity and/or changes of driving status and/or changes of card status for a given calendar day (requirement 084) and to slots status at 00:00 that day.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

[14] Reference text in the EU is Directive 92/23/EEC relating to tyres for motor vehicles and their trailers and to their fitting of 31 March 1992 (OJ No L 129, 14/05/1992).

noOfActivityChanges is the number of ActivityChangeInfo words in the activityChangeInfos set.

activityChangeInfos is the set of ActivityChangeInfo words stored in the VU for the day. It always includes two ActivityChangeInfo words giving the status of the two slots at 00:00 that day.

2.116 VuApprovalNumber

Type approval number of the vehicle unit.

VuApprovalNumber ::= IA5String(SIZE(8))

Value assignment: Unspecified.

2.117 VuCalibrationData

Information, stored in a vehicle unit, related to the calibrations of the control device (requirement 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords          INTEGER(0..255),
   vuCalibrationRecords              SET SIZE(noOfVuCalibrationRecords) OF
                                     VuCalibrationRecord
}
```

noOfVuCalibrationRecords is the number of records contained in the vuCalibrationRecords set.

vuCalibrationRecords is the set of calibration records.

2.118 VuCalibrationRecord

Information, stored in a vehicle unit, related a calibration of the control device (requirement 098).

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                CalibrationPurpose,
   workshopName                      Name,
   workshopAddress                   Address,
   workshopCardNumber                FullCardNumber,
   workshopCardExpiryDate            TimeReal,
   vehicleIdentificationNumber       VehicleIdentificationNumber,
   vehicleRegistrationIdentification VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant    W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment     K-ConstantOfRecordingEquipment,
   lTyreCircumference                L-TyreCircumference,
   tyreSize                          TyreSize,
   authorisedSpeed                   SpeedAuthorised,
   oldOdometerValue                  OdometerShort,
   newOdometerValue                  OdometerShort,
   oldTimeValue                      TimeReal,
```

```
  newTimeValue                    TimeReal,
  nextCalibrationDate             TimeReal
}
```

calibrationPurpose is the purpose of the calibration.

workshopName, workshopAddress are the workshop name and address.

workshopCardNumber identifies the workshop card used during the calibration.

workshopCardExpiryDate is the card expiry date.

vehicleIdentificationNumber is the VIN.

vehicleRegistrationIdentification contains the VRN and registering Contracting Party .

wVehicleCharacteristicConstant is the characteristic coefficient of the vehicle.

kConstantOfRecordingEquipment is the constant of the control device.

lTyreCircumference is the effective circumference of the wheel tyres.

tyreSize is the designation of the dimension of the tyres mounted on the vehicle

authorisedSpeed is the authorised speed of the vehicle.

oldOdometerValue, newOdometerValue are the old and new values of the odometer.

oldTimeValue, newTimeValue are the old and new values of date and time.

nextCalibrationDate is the date of the next calibration of the type specified in CalibrationPurpose to be carried out by the authorised inspection authority.

2.119 VuCardIWData

Information, stored in a vehicle unit, related to insertion and withdrawal cycles of driver cards or of workshop cards in the vehicle unit (requirement 081).

```
VuCardIWData ::= SEQUENCE {
  noOfIWRecords                   INTEGER(0..2^16-1),
  vuCardIWRecords                 SET SIZE(noOfIWRecords) OF
                                  VuCardIWRecord
}
```

noOfIWRecords is the number of records in the set vuCardIWRecords.

vuCardIWRecords is a set of records related to card insertion withdrawal cycles.

2.120 VuCardIWRecord

Information, stored in a vehicle unit, related to an insertion and withdrawal cycle of a driver card or of a workshop card in the vehicle unit (requirement 081).

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                    HolderName,
   fullCardNumber                    FullCardNumber,
   cardExpiryDate                    TimeReal,
   cardInsertionTime                 TimeReal,
   vehicleOdometerValueAtInsertion   OdometerShort,
   cardSlotNumber                    CardSlotNumber,
   cardWithdrawalTime                TimeReal,
   vehicleOdometerValueAtWithdrawal  OdometerShort,
   previousVehicleInfo               PreviousVehicleInfo
   manualInputFlag                   ManualInputFlag
}
```

cardHolderName is the driver or workshop card holder's surname and first names as stored in the card.

fullCardNumber is the type of card, its issuing Contracting Party and its card number as stored in the card.

cardExpiryDate is the card's expiry date as stored in the card.

cardInsertionTime is the insertion date and time.

vehicleOdometerValueAtInsertion is the vehicle odometer value at card insertion.

cardSlotNumber is the slot in which the card is inserted.

cardWithdrawalTime is the withdrawal date and time.

vehicleOdometerValueAtWithdrawal is the vehicle odometer value at card withdrawal.

previousVehicleInfo contains information about the previous vehicle used by the driver, as stored in the card.

manualInputFlag is a flag identifying if the cardholder has manually entered driver activities at card insertion.

2.121 VuCertificate

Certificate of the public key of a vehicle unit.

```
VuCertificate ::= Certificate
```

2.122 VuCompanyLocksData

Information, stored in a vehicle unit, related to company locks (requirement 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                 INTEGER(0..20),
   vuCompanyLocksRecords     SET SIZE(noOfLocks) OF
                             VuCompanyLocksRecord
}
```

noOfLocks is the number of locks listed in vuCompanyLocksRecords.

vuCompanyLocksRecords is the set of company locks records.

2.123 VuCompanyLocksRecord

Information, stored in a vehicle unit, related to one company lock (requirement 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                    TimeReal,
   lockOutTime                   TimeReal,
   companyName                   Name,
   companyAddress                Address,
   companyCardNumber             FullCardNumber
}
```

lockInTime, lockOutTime are the date and time of lock-in and lock-out.

companyName, companyAddress are the company name and address related with the lock-in.

companyCardNumber identifies the card used at lock-in.

2.124 VuControlActivityData

Information, stored in a vehicle unit, related to controls performed using this VU (requirement 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                  INTEGER(0..20),
   vuControlActivityRecords      SET SIZE(noOfControls) OF
                                 VuControlActivityRecord
}
```

noOfControls is the number of controls listed in vuControlActivityRecords.

vuControlActivityRecords is the set of control activity records.

2.125 VuControlActivityRecord

Information, stored in a vehicle unit, related to a control performed using this VU (requirement 102).

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                   ControlType,
   controlTime                   TimeReal,
   controlCardNumber             FullCardNumber,
   downloadPeriodBeginTime       TimeReal,
   downloadPeriodEndTime         TimeReal
}
```

controlType is the type of the control.

controlTime is the date and time of the control.

controlCardNumber identifies the control card used for the control.

downloadPeriodBeginTime is the begin time of the downloaded period, in case of downloading.

downloadPeriodEndTime is the end time of the downloaded period, in case of downloading.

2.126 VuDataBlockCounter

Counter, stored in a card, identifying sequentially the insertion withdrawal cycles of the card in vehicle units.

VuDataBlockCounter ::= BCDString(SIZE(2))

Value assignment: Consecutive Number with max, value 9 999, starting again with 0.

2.127 VuDetailedSpeedBlock

Information, stored in a vehicle unit, related to the vehicle's detailed speed for a minute during which the vehicle has been moving (requirement 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate is the date and time of the first speed value within the block.

speedsPerSecond is the chronological sequence of measured speeds every seconds for the minute starting at speedBlockBeginDate (included).

2.128 VuDetailedSpeedData

Information, stored in a vehicle unit, related to the detailed speed of the vehicle.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                INTEGER(0.2^16-1),
   vuDetailedSpeedBlocks          SET SIZE(noOfSpeedBlocks) OF
                                  VuDetailedSpeedBlock
}
```

noOfSpeedBlocks is the number of speed blocks in the vuDetailedSpeedBlocks set.

vuDetailedSpeedBlocks is the set of detailed speed blocks.

2.129 VuDownloadablePeriod

Oldest and latest dates for which a vehicle unit holds data related to drivers activities (requirements 081, 084 or 087).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime            TimeReal
   maxDownloadableTime            TimeReal
}
```

minDownloadableTime is the oldest card insertion or activity change or place entry date and time stored in the VU.

maxDownloadableTime is the latest card withdrawal or activity change or place entry date

and time stored in the VU.

2.130 VuDownloadActivityData

Information, stored in a vehicle unit, related to its last download (requirement 105).

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                  TimeReal,
   fullCardNumber                   FullCardNumber,
   companyOrWorkshopName            Name
}
```

downloadingTime is the date and time of downloading.

fullCardNumber identifies the card used to authorise the download.

companyOrWorkshopName is the company or workshop name.

2.131 VuEventData

Information, stored in a vehicle unit, related to events (requirement 094 except over speeding event).

```
VuEventData ::= SEQUENCE {
noOfVuEvents                        INTEGER(0..255),
vuEventRecords                      SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents is the number of events listed in the vuEventRecords set.

vuEventRecords is a set of events records.

2.132 VuEventRecord

Information, stored in a vehicle unit, related to an event (requirement 094 except over speeding event).

```
VuEventRecord ::= SEQUENCE {
   eventType                        EventFaultType,
   eventRecordPurpose               EventFaultRecordPurpose,
   eventBeginTime                   TimeReal,
   eventEndTime                     TimeReal,
   cardNumberDriverSlotBegin        FullCardNumber,
   cardNumberCodriverSlotBegin      FullCardNumber,
   cardNumberDriverSlotEnd          FullCardNumber,
   cardNumberCodriverSlotEnd        FullCardNumber,
   similarEventsNumber              SimilarEventsNumber
}
```

eventType is the type of the event.

eventRecordPurpose is the purpose for which this event has been recorded.

eventBeginTime is the date and time of beginning of event.

eventEndTime is the date and time of end of event.

cardNumberDriverSlotBegin identifies the card inserted in the driver slot at the beginning of the event.

cardNumberCodriverSlotBegin identifies the card inserted in the co-driver slot at the beginning of the event.

cardNumberDriverSlotEnd identifies the card inserted in the driver slot at the end of the event.

cardNumberCodriverSlotEnd identifies the card inserted in the co-driver slot at the end of the event.

similarEventsNumber is the number of similar events that day.

This sequence can be used for all events other than over speeding events.

2.133 VuFaultData

Information, stored in a vehicle unit, related to faults (requirement 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                    INTEGER(0..255),
   vuFaultRecords                  SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults is the number of faults listed in the vuFaultRecords set.

vuFaultRecords is a set of faults records.

2.134 VuFaultRecord

Information, stored in a vehicle unit, related to a fault (requirement 096).

```
VuFaultRecord ::= SEQUENCE {
   faultType                       EventFaultType,
   faultRecordPurpose              EventFaultRecordPurpose,
   faultBeginTime                  TimeReal,
   faultEndTime                    TimeReal,
   cardNumberDriverSlotBegin       FullCardNumber,
   cardNumberCodriverSlotBegin     FullCardNumber,
   cardNumberDriverSlotEnd         FullCardNumber,
   cardNumberCodriverSlotEnd       FullCardNumber
}
```

faultType is the type of control device fault.

faultRecordPurpose is the purpose for which this fault has been recorded.

faultBeginTime is the date and time of beginning of fault.

faultEndTime is the date and time of end of fault.

cardNumberDriverSlotBegin identifies the card inserted in the driver slot at the beginning of the fault.

cardNumberCodriverSlotBegin identifies the card inserted in the co-driver slot at the beginning of the fault.

cardNumberDriverSlotEnd identifies the card inserted in the driver slot at the end of the fault.

cardNumberCodriverSlotEnd identifies the card inserted in the co-driver slot at the end of the fault.

2.135 VuIdentification

Information, stored in a vehicle unit, related to the identification of the vehicle unit (requirement 075).

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName              VuManufacturerName,
   vuManufacturerAddress           VuManufacturerAddress,
   vuPartNumber                    VuPartNumber,
   vuSerialNumber                  VuSerialNumber,
   vuSoftwareIdentification        VuSoftwareIdentification,
   vuManufacturingDate             VuManufacturingDate,
   vuApprovalNumber                VuApprovalNumber
}
```

vuManufacturerName is the name of the manufacturer of the vehicle unit.

vuManufacturerAddress is the address of the manufacturer of the vehicle unit.

vuPartNumber is the part number of the vehicle unit.

vuSerialNumber is the serial number of the vehicle unit.

vuSoftwareIdentification identifies the software implemented in the vehicle unit.

vuManufacturingDate is the manufacturing date of the vehicle unit.

vuApprovalNumber is the type approval number of the vehicle unit.

2.136 VuManufacturerAddress

Address of the manufacturer of the vehicle unit.

VuManufacturerAddress ::= Address

Value assignment: Unspecified.

2.137 VuManufacturerName

Name of the manufacturer of the vehicle unit.

VuManufacturerName ::= Name

Value assignment: Unspecified.

2.138 VuManufacturingDate

Date of manufacture of the vehicle unit.

VuManufacturingDate ::= TimeReal

Value assignment: Unspecified.

2.139 VuOverSpeedingControlData

Information, stored in a vehicle unit, related to over speeding events since the last over speeding control (requirement 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime          TimeReal,
   firstOverspeedSince               TimeReal,
   numberOfOverspeedSince            OverspeedNumber
}
```

lastOverspeedControlTime is the date and time of the last over speeding control.

firstOverspeedSince is the date and time of the first over speeding following this over speeding control.

numberOfOverspeedSince is the number of over speeding events since the last over speeding control.

2.140 VuOverSpeedingEventData

Information, stored in a vehicle unit, related to over speeding events (requirement 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents          INTEGER(0..255),
   vuOverSpeedingEventRecords        SET SIZE(noOfVuOverSpeedingEvents) OF
                                     VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents is the number of events listed in the vuOverSpeedingEventRecords set.

vuOverSpeedingEventRecords is a set of over speeding events records.

2.141 VuOverSpeedingEventRecord

Information, stored in a vehicle unit, related to over speeding events (requirement 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                         EventFaultType,
   eventRecordPurpose                EventFaultRecordPurpose,
   eventBeginTime                    TimeReal,
   eventEndTime                      TimeReal,
   maxSpeedValue                     SpeedMax,
   averageSpeedValue                 SpeedAverage,
   cardNumberDriverSlotBegin         FullCardNumber,
   similarEventsNumber               SimilarEventsNumber
}
```

eventType is the type of the event.

eventRecordPurpose is the purpose for which this event has been recorded.

eventBeginTime is the date and time of beginning of event.

eventEndTime is the date and time of end of event.

maxSpeedValue is the maximum speed measured during the event.

averageSpeedValue is the arithmetic average speed measured during the event.

cardNumberDriverSlotBegin identifies the card inserted in the driver slot at the beginning of the event.

similarEventsNumber is the number of similar events that day.

2.142 VuPartNumber

Part number of the vehicle unit.

VuPartNumber ::= IA5String(SIZE(16))

Value assignment: VU manufacturer specific.

2.143 VuPlaceDailyWorkPeriodData

Information, stored in a vehicle unit, related to places where drivers begin or end a daily work periods (requirement 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                 INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords    SET SIZE(noOfPlaceRecords) OF
                                    VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords is the number of records listed in the vuPlaceDailyWorkPeriodRecords set.

vuPlaceDailyWorkPeriodRecords is a set of place related records.

2.144 VuPlaceDailyWorkPeriodRecord

Information, stored in a vehicle unit, related to a place where a driver begins or ends a daily work period (requirement 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                   FullCardNumber,
   placeRecord                      PlaceRecord
}
```

fullCardNumber is the driver's card type, card issuing Contracting Party and card number.

placeRecord contains the information related to the place entered.

2.145 VuPrivateKey

The private key of a vehicle unit.

VuPrivateKey ::= RSAKeyPrivateExponent

2.146 VuPublicKey

The public key of a vehicle unit.

VuPublicKey ::= PublicKey

2.147 VuSerialNumber

Serial number of the vehicle unit (requirement 075).

VuSerialNumber ::= ExtendedSerialNumber

2.148 VuSoftInstallationDate

Date of installation of the vehicle unit software version.

VuSoftInstallationDate ::= TimeReal

Value assignment: Unspecified.

2.149 VuSoftwareIdentification

Information, stored in a vehicle unit, related to the software installed.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                VuSoftwareVersion,
   vuSoftInstallationDate           VuSoftInstallationDate
}
```

vuSoftwareVersion is the software version number of the Vehicle Unit.

vuSoftInstallationDate is the software version installation date.

2.150 VuSoftwareVersion

Software version number of the vehicle unit.

VuSoftwareVersion ::= IA5String(SIZE(4))

Value assignment: Unspecified.

2.151 VuSpecificConditionData

Information, stored in a vehicle unit, related to specific conditions.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords     INTEGER(0..2^16-1)
   specificConditionRecords         SET SIZE (noOfSpecificConditionRecords) OF
                                    SpecificConditionRecord
}
```

noOfSpecificConditionRecords is the number of records listed in the specificConditionRecords set.

specificConditionRecords is a set of specific conditions related records.

2.152 VuTimeAdjustmentData

Information, stored in a vehicle unit, related to time adjustments performed outside the frame of a regular calibration (requirement 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords              INTEGER(0..6),
   vuTimeAdjustmentRecords           SET SIZE(noOfVuTimeAdjRecords) OF
                                     VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords is the number of records in vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords is a set of time adjustment records.

2.153 VuTimeAdjustmentRecord

Information, stored in a vehicle unit, related a time adjustment performed outside the frame of a regular calibration (requirement 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   newTimeValue                      TimeReal,
   workshopName                      Name,
   workshopAddress                   Address,
   workshopCardNumber                FullCardNumber
}
```

oldTimeValue, newTimeValue are the old and new values of date and time.

workshopName, workshopAddress are the workshop name and address.

workshopCardNumber identifies the workshop card used to perform the time adjustment.

2.154 W-VehicleCharacteristicConstant

Characteristic coefficient of the vehicle (definition k)).

W-VehicleCharacteristicConstant ::= INTEGER(0..2^{16}-1))

Value assignment: Impulses per kilometre in the operating range 0 to 64 255 pulses/km.

2.155 WorkshopCardApplicationIdentification

Information, stored in a workshop card related to the identification of the application of the card (requirement 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfCalibrationRecords              NoOfCalibrationRecords
}
```

typeOfTachographCardId is specifying the implemented type of card.

cardStructureVersion is specifying the the version of the structure that is implemented in the card.

noOfEventsPerType is the number of events per type of event the card can record.

noOfFaultsPerType is the number of faults per type of fault the card can record.

activityStructureLength indicates the number of bytes available for storing activity records..

noOfCardVehicleRecords is the number of vehicle records the card can contain.

noOfCardPlaceRecords is the number of places the card can record.

noOfCalibrationRecords is the number of calibration records the card can store.

2.156 WorkshopCardCalibrationData

Information, stored in a workshop card, related to workshop activity performed with the card (requirements 227 and 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber is the total number of calibrations performed with the card.

calibrationPointerNewestRecord is the index of the last updated calibration record.
Value assignment: Number corresponding to the numerator of the calibration record, beginning with '0' for the first occurrence of the calibration records in the structure.

calibrationRecords is the set of records containing calibration and/or time adjustment information.

2.157 WorkshopCardCalibrationRecord

Information, stored in a workshop card, related to a calibration performed with the card (requirement 227).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                CalibrationPurpose,
   vehicleIdentificationNumber       VehicleIdentificationNumber,
   vehicleRegistration               VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant    W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment     K-ConstantOfRecordingEquipment,
   lTyreCircumference                L-TyreCircumference,
   tyreSize                          TyreSize,
   authorisedSpeed                   SpeedAuthorised,
   oldOdometerValue                  OdometerShort,
   newOdometerValue                  OdometerShort,
   oldTimeValue                      TimeReal,
   newTimeValue                      TimeReal,
   nextCalibrationDate               TimeReal,
   vuPartNumber                      VuPartNumber,
   vuSerialNumber                    VuSerialNumber,
   sensorSerialNumber                SensorSerialNumber
}
```

calibrationPurpose is the purpose of the calibration.

vehicleIdentificationNumber is the VIN.

vehicleRegistration contains the VRN and registering Contracting Party .

wVehicleCharacteristicConstant is the characteristic coefficient of the vehicle.

kConstantOfRecordingEquipment is the constant of the control device.

lTyreCircumference is the effective circumference of the wheel tyres.

tyreSize is the designation of the dimensions of the tyres mounted on the vehicle.

authorisedSpeed is the maximum authorised speed of the vehicle.

oldOdometerValue, newOdometerValue are the old and new values of the odometer.

oldTimeValue, newTimeValue are the old and new values of date and time.

nextCalibrationDate is the date of the next calibration of the type specified in CalibrationPurpose to be carried out by the authorised inspection authority.

vuPartNumber, **vuSerialNumber** and **sensorSerialNumber** are the data elements for control device identification.

2.158 WorkshopCardHolderIdentification

Information, stored in a workshop card, related to the identification of the cardholder (requirement 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                    Name,
   workshopAddress                 Address,
   cardHolderName                  HolderName,
   cardHolderPreferredLanguage     Language
}
```

workshopName is name of the workshop of the card holder.

workshopAddress is the address of the workshop of the card holder.

cardHolderName is the name and first name(s) of the holder (e.g. the name of the mechanic).

cardHolderPreferredLanguage is the preferred language of the card holder.

2.159 WorkshopCardPIN

Personal identification number of the Workshop Card (requirement 213).

WorkshopCardPIN ::= IA5String(SIZE(8))

Value assignment: The PIN known to the cardholder, right padded with 'FF' bytes up to 8 bytes.

3. Value and size range definitions

Definition of variable values used for definitions in paragraph 2.

TimeRealRange ::= 2^{32}-1

3.1 Definitions for the Driver Card:

Name of the variable value	Min	Max
CardActivityLengthRange	5544 bytes (28 days 93 activity changes per day)	13776 bytes (28 days 240 activity changes per day)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 Definitions for the Workshop Card:

Name of the variable value	Min	Max
CardActivityLengthRange	198 bytes (1 day 93 activity changes)	492 bytes (1 day 240 activity changes)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 Definitions for the Control Card:

Name of the variable value	Min	Max
NoOfControlActivityRecords	230	520

3.4 Definitions for the Company Card:

Name of the variable value	Min	Max
NoOfCompanyActivityRecords	230	520

4. Character sets

IA5Strings use the ASCII characters as defined by ISO/IEC 8824-1. For readability and for easy referencing the value assignment is given below. The ISO/IEC 8824-1 supersedes this informative note in case of discrepancy.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Other character strings (Address, Name, VehicleRegistrationNumber) use, in addition, the characters defined by the codes 192 to 255 of ISO/IEC 8859-1 (Latin1 character set) or ISO/IEC 8859-7 (Greek character set):

5. Encoding

When encoded with ASN.1 encoding rules, all data types defined shall be encoded according to ISO/IEC 8825-2, aligned variant.

SUB-APPENDIX II

TACHOGRAPH CARDS SPECIFICATION

CONTENTS

CONTENTS (continued)

1. Introduction

1.1 Abbreviations

For the purpose of this sub-appendix, the following abbreviations apply.

AC	Access conditions
AID	Application Identifier
ALW	Always
APDU	Application Protocol Data Unit (structure of a command)
ATR	Answer To Reset
AUT	Authenticated.
C6, C7	Contacts N° 6 and 7 of the card as described in ISO/IEC 7816-2
cc	clock cycles
CHV	Card holder Verification Information
CLA	Class byte of an APDU command
DF	Dedicated File. A DF can contain other files (EF or DF)
EF	Elementary File
ENC	Encrypted: Access is possible only by encoding data.
etu	elementary time unit
IC	Integrated Circuit
ICC	Integrated Circuit Card
ID	Identifier
IFD	Interface Device
IFS	Information Field Size
IFSC	Information Field Size for the card
IFSD	Information Field Size Device (for the Terminal)
INS	Instruction byte of an APDU command
Lc	Length of the input data for a APDU command
Le	Length of the expected data (output data for a command)
MF	Master File (root DF)
P1-P2	Parameter bytes
NAD	Node Address used in T=1 protocol
NEV	Never
PIN	Personal Identification Number
PRO SM	Protected with secure messaging
PTS	Protocol Transmission Selection
RFU	Reserved for Future Use
RST	Reset (of the card)
SM	Secure Messaging
SW1-SW2	Status bytes
TS	Initial ATR character
VPP	Programming Voltage
XXh	Value XX in hexadecimal notation
||	Concatenation symbol 03||04=0304

1.2 References

The following references are used in this sub-appendix:

EN 726-3 Identification cards systems - Telecommunications integrated circuit(s) cards and terminals - Part 3 : Application independent card requirements. December 1994.

ISO/IEC 7816-2 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts. First edition: 1999.

ISO/IEC 7816-3 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocol. Edition 2: 1997.

ISO/IEC 7816-4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.

ISO/IEC 7816-6 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998.

ISO/IEC 7816-8 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands. First Edition: 1999.

ISO/IEC 9797 Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994.

2. Electrical and physical characteristics

TCS_200 All electronic signals shall be in accordance with ISO/IEC 7816-3 unless specified otherwise.

TCS_201 The location and dimensions of the card contacts shall comply with the ISO/IEC 7816-2.

2.1 Supply Voltage and Current Consumption

TCS_202 The card shall work according to specifications within the consumption limits specified in ISO/IEC 7816-3.

TCS_203 The card shall work with Vcc = 3V (± 0.3V) or with Vcc = 5V (± 0.5V).

Voltage selection shall be performed according to ISO/IEC 7816-3.

2.2 Programming Voltage V_{pp}

TCS_204 The card shall not require a programming voltage at pin C6. It is expected that pin C6 is not connected in an IFD. Contact C6 may be connected to V_{cc} in the card but shall not be connected to ground. This voltage should not be interpreted in any case.

2.3 Clock generation and Frequency

TCS_205 The card shall operate within a frequency range of 1 to 5 MHz. Within one card session the clock frequency may vary ± 2%. The clock frequency is generated by the Vehicle Unit and not the card itself. The duty cycle may vary between 40 and 60%.

TCS_206 Under conditions contained into the card file EF_{ICC}, the external clock can be stopped. The first byte of the EF_{ICC} file body codes the Clockstop mode conditions (see EN 726-3 for further details):

Low	High		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop allowed, no preferred level
0	1	1	Clockstop allowed, high level preferred
1	0	1	Clockstop allowed, low level preferred
0	0	0	Clockstop not allowed
0	1	0	Clockstop only allowed on high level
1	0	0	Clockstop only allowed on low level

Bits 4 to 8 are not used.

2.4 I/O Contact

TCS_207 The I/O contact C7 is used to receive data from and to transmit data to the IFD. During operation only either the card or the IFD shall be in transmit mode. Should both units be in transmit mode no damage shall occur to the card. Unless transmitting, the card shall enter the reception mode.

2.5 States of the Card

TCS_208 The card works in two states while the supply voltage is applied:

- Operation state while executing commands or interfacing with Digital Unit,
- Idle state at all other times; in this state all data shall be retained by the card.

3. Hardware and communication

3.1 Introduction

This paragraph describes the minimum functionality required by Tachograph cards and VUs to ensure correct operation and interoperability.

Tachograph cards are as compliant as possible with the available ISO/IEC applicable norms (especially ISO/IEC 7816). However, commands and protocols are fully described in order to specify some restricted usage or some differences if they exist. The commands specified are fully compliant with the referred norms except where indicated.

3.2 Transmission Protocol

TCS_300 The Transmission protocol shall be compliant with ISO/IEC 7816-3. In particular, the VU shall recognise waiting time extensions sent by the card.

3.2.1 Protocols

TCS_301 The card shall provide both protocol **T=0** and protocol **T=1**.

TCS_302 **T=0** is the default protocol, a **PTS** command is therefore necessary to change the protocol to **T=1**.

TCS_303 Devices shall support **direct convention** in both protocols : the direct convention is hence mandatory for the card.

TCS_304 The **Information Field Size Card** byte shall be presented at the ATR in character TA3. This value shall be at least 'F0h' (=240 bytes).

The following restrictions apply to the protocols:

TCS_305 **T=0**

- The interface device shall support an answer on I/O after the rising edge of the signal on RST from 400 cc.
- The interface device shall be able to read characters separated with 12 etu.
- The interface device shall read an erroneous character and its repetition if separated with 13 etu. If an erroneous character is detected, the Error signal on I/O can occur between 1 etu and 2 etu. The device shall support a 1 etu delay.
- The interface device shall accept a 33 bytes ATR (TS+32)
- If TC1 is present in the ATR, the Extra Guard Time shall be present for characters sent by the interface device although characters sent by the card can still be separated with 12 etu. This is also true for the ACK character sent by the card after a P3 character emitted by the interface device.
- The interface device shall take into account a NUL character emitted by the card.
- The interface device shall accept the complementary mode for ACK.
- The get-response command cannot be used in chaining mode to get a data which length could exceed 255 bytes.

TCS_306 **T=1**

- NAD byte : not used (NAD shall be set to '00').
- S-block ABORT : not used.
- S-block VPP state error : not used.
- The total chaining length for a data field will not exceed 255 bytes (to be ensured by the IFD).
- The Information Field Size Device (IFSD) shall be indicated by the IFD immediately after the ATR : the IFD shall transmit the S-Block IFS request after the ATR and the card shall send back S-Block IFS. The recommended value for IFSD is 254 bytes.
- The card will not ask for an IFS readjustment.

3.2.2 ATR

TCS_307 The device checks ATR bytes, according to ISO/IEC 7816-3. No verification shall be done on ATR Historical Characters.

Example of Basic Biprotocol ATR according to ISO/IEC 7816-3

Character	Value	Remarks
TS	'3Bh'	Indicates direct convention.
T0	'85h'	TD1 present; 5 historical bytes are presents.
TD1	'80h'	TD2 present; T=0 to be used
TD2	'11h'	TA3 present; T=1 to be used
TA3	'XXh' (at least 'F0h')	Information Field Size Card (IFSC)
TH1 to TH5	'XXh'	Historical characters
TCK	'XXh'	Check Character (exclusive OR)

TCS_308 After the Answer To Reset (ATR), the Master File (MF) is implicitly selected and becomes the Current Directory.

3.2.3 PTS

TCS_309 The default Protocol is T=0. To set the T=1 protocol, a PTS (also known as PPS) must be sent to the card by the device.

TCS_310 As both T=0 and T=1 protocols are mandatory for the card, the basic PTS for protocol switching is mandatory for the card.

The PTS can be used, as indicated in ISO/IEC 7816-3, to switch to higher baud rates than the default one proposed by the card in the ATR if any (TA(1) byte).

Higher baud rates are optional for the card.

TCS_311 If no other baud rate than the default one are supported (or if the selected baud rate is not supported), the card shall respond to the PTS correctly according to ISO/IEC 7816-3 by omitting the PPS1 byte.

Examples of basic PTS for protocol selection are the following :

Character	Value	Remarks
PPSS	'FFh'	The Initiate Character.
PPS0	'00h' or '01h'	PPS1 to PPS3 are not present; '00h' to select T0, '01h' to select T1.
PK	'XXh'	Check Character: 'XXh' = 'FFh' if PPS0 = '00h', 'XXh' = 'FEh' if PPS0 = '01h'.

3.3 Access Conditions (AC)

Access Conditions (AC) for the UPDATE_BINARY and READ_BINARY commands are defined for each Elementary File.

TCS_312 The AC of the current file must be met before accessing the file via these commands.

The definitions of the available access conditions are the following:

- **ALW** : The action is always possible and can be executed without any restriction.
- **NEV** : The action is never possible.
- **AUT** : The right corresponding a successful external authentication must be opened up (done by the EXTERNAL_AUTHENTICATE command).
- **PRO SM**: Command must be transmitted with a cryptographic checksum using secure messaging (See sub-appendix 11).
- **AUT** and **PRO SM** (combined)

On the processing commands (UPDATE_BINARY and READ_BINARY), the following access conditions can be set in the card:

	UPDATE_BINARY	READ_BINARY
ALW	Yes	Yes
NEV	Yes	Yes
AUT	Yes	Yes
PRO SM	Yes	No
AUT and PRO SM	Yes	No

The PRO SM access condition is not available for the READ_BINARY command. It means that the presence of a cryptographic checksum for a READ command is never mandatory. However, using the value 'OC' for the class, it is possible to use the READ_BINARY command with secure messaging, as described in paragraph 3.6.2.

3.4 Data encryption

When confidentiality of data to be read from a file needs to be protected, the file is marked as "Encrypted" . Encryption is performed using secure messaging (See sub-appendix 11).

3.5 Commands and error codes overview

Commands and file organisation are deduced from and complies with ISO/IEC 7816-4.

TCS_313 This section describes the following APDU command-response pairs:

Command	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION : VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT : SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 The status word SW1 SW2 are returned in any response message and denote the processing state of the command.

SW1	SW2	Meaning
90	00	Normal processing.
61	XX	Normal processing. XX = number of response bytes available.
62	81	Warning processing. Part of returned data may be corrupted
63	CX	Wrong CHV (PIN). Remaining attempts counter provided by 'X'.
64	00	Execution error - State of non-volatile memory unchanged. Integrity error.
65	00	Execution error - State of non-volatile memory changed
65	81	Execution error - State of non-volatile memory changed – Memory failure
66	88	Security error: wrong Cryptographic checksum (during Secure Messaging) or wrong certificate (during certificate verification) or wrong cryptogram (during external authentication) or wrong signature (during signature verification)
67	00	Wrong length (wrong Lc or Le)
69	00	Forbidden command (no response available in T=0)
69	82	Security status not satisfied.
69	83	Authentication method blocked.
69	85	Conditions of use not satisfied.
69	86	Command not allowed (no current EF).
69	87	Expected Secure Messaging Data Objects missing
69	88	Incorrect Secure Messaging Data Objects
6A	82	File not found.
6A	86	Wrong parameters P1-P2.
6A	88	Referenced data not found.
6B	00	Wrong parameters (offset outside the EF).
6C	XX	Wrong length, SW2 indicates the exact length. No data field is returned.
6D	00	Instruction code not supported or invalid.
6E	00	Class not supported.
6F	00	Other checking errors

3.6 Commands description

The mandatory commands for the Tachograph cards are described in this chapter.

Additional relevant details, related to cryptographic operations involved, are given in sub-appendix 11 Common security mechanisms.

All commands are described independently of the used protocol (T=0 or T=1). The APDU bytes CLA, INS, P1, P2, Lc and Le are always indicated. If Lc or Le is not needed for the described command, the associated length, value and description are empty.

TCS_315 If both length bytes (Lc and Le) are requested, the described command has to be split in two parts if the IFD is using protocol T=0 : the IFD sends the command as described with P3=Lc + data and then sends a GET_RESPONSE (see § 3.6.6) command with P3=Le.

TCS_316 If both length bytes are requested, and Le=0 (secure messaging):

- When using protocol T=1, the card shall answer to Le=0 by sending all available output data.
- When using protocol T=0, the IFD shall send the first command with P3=Lc + data, the card shall answer (to this implicit Le=0) by the Status bytes '**61La**', where La is the number of response bytes available. The IFD shall then generate a GET REPONSE command with P3 = La to read the data.

3.6.1 Select File

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The SELECT FILE command is used :
- to select an application DF (selection by name must be used)
- to select an elementary file corresponding to the submitted file ID

3.6.1.1 Selection by name (AID)

This command allows to select an application DF in the card.

TCS_317 This command can be performed from anywhere in the file structure (after the ATR or at anytime).

TCS_318 The selection of an application resets the current security environment. After performing the application selection, no current public key is selected anymore and the former session key is no longer available for secure messaging. The AUT access condition is also lost.

TCS_319 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selection by name (AID)
P2	1	'0Ch'	No response expected
Lc	1	'NNh'	Number of bytes sent to the card (length of the AID) : '06h' for the Tachograph application.
#6-#(5+NN)	NN	'XX..XXh'	AID : 'FF 54 41 43 48 4F' for the Tachograph application

No response to the SELECT FILE command is needed (Le absent in T=1, or no response asked in T=0).

TCS_320 **Response Message (no response asked)**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If the application corresponding with the AID is not found, the processing state returned is **'6A82'**.
- In T=1, if the byte Le is present, the state returned is **'6700'**.
- In T=0, if a response is asked after the SELECT FILE command, the state returned is **'6900'**.
- If the selected application is considered corrupted (integrity error is detected within the file attributes), the processing state returned is **'6400'** or **'6581'**.

3.6.1.2 Selection of an Elementary File using its File Identifier

TCS_321 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selection of an EF under the current DF
P2	1	'0Ch'	No response expected
Lc	1	'02h'	Number of bytes sent to the card
#6-#7	2	'XXXXh'	File Identifier

No response to the SELECT FILE command is needed (Le absent in T=1, or no response asked in T=0).

TCS_322 **Response Message (no response asked)**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If the file corresponding with the file identifier is not found, the processing state returned is **'6A82'**.
- In T=1, if the byte Le is present, the state returned is **'6700'**.
- In T=0, if a response is asked after the SELECT FILE command, the state returned is **'6900'**.
- If the selected file is considered corrupted (integrity error is detected within the file attributes), the processing state returned is **'6400'** or **'6581'**.

3.6.2 Read Binary

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The Read Binary command is used to read data from a transparent file.

The response of the card consists of returning the data read, optionally encapsulated in a secure messaging structure.

TCS_323 The command can be performed only if the security status satisfies the security attributes defined for the EF for the READ function.

3.6.2.1 Command without secure messaging

This command enables the IFD to read data from the EF currently selected, without secure messaging.

TCS_324 Reading data from a file marked as "Encrypted" shall not be possible through this command.

TCS_325 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	No Secure Messaging asked
INS	1	'B0h'	
P1	1	'XXh'	Offset in bytes from the beginning of the file : Most Significant Byte
P2	1	'XXh'	Offset in bytes from the beginning of the file : Least Significant Byte
Le	1	'XXh'	Length of data expected. Number of Bytes to be read.

Note: bit 8 of P1 must be set to 0.

TCS_326 **Response Message**

Byte	Length	Value	Description
#1-#X	X	'XX..XXh'	Data read
SW	2	'XXXXh'	Status Words (SW1,SW2)

- f the command is successful, the card returns **'9000'**.
- If no EF is selected , the processing state returned is **'6986'**.
- If the Access Control of the selected file are not satisfied, the command is interrupted with **'6982'**.
- If the Offset is not compatible with the size of the EF (Offset > EF size), the processing state returned is **'6B00'**.
- If the size of the data to be read is not compatible with the size of the EF (Offset + Le > EF size) the processing state returned is **'6700'** or **'6Cxx'** where 'xx' indicates the exact length.
- If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is **'6400'** or **'6581'.**
- If an integrity error is detected within the stored data, the card shall return the demanded data, and the processing state returned is **'6281'**.

3.6.2.2 Command with secure messaging

This command enables the IDF to read data from the EF currently selected with secure messaging, in order to verify the integrity of the data received and to protect the confidentiality of the data in the case the EF is marked as "Encrypted".

TCS_327 **Command Message**

Byte	Length	Value	Description
CLA	1	'0Ch'	Secure Messaging asked
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (offset in bytes from the beginning of the file) : Most Significant Byte
P2	1	'XXh'	P2 (offset in bytes from the beginning of the file) : Least Significant Byte
Lc	1	'09h'	Length of input data for secure messaging
#6	1	'97h'	T_{LE} : Tag for expected length specification.
#7	1	'01h'	L_{LE} : Length of expected length
#8	1	'NNh'	Expected length specification (original Le) : Number of Bytes to be read
#9	1	'8Eh'	T_{CC} : Tag for cryptographic checksum
#10	1	'04h'	L_{CC} : Length of following cryptographic checksum
#11-#14	4	'XX..XXh'	Cryptographic checksum (4 most significant bytes)
Le	1	'00h'	As specified in ISO/IEC 7816-4

TCS_328 **Response Message if EF is not marked as "Encrypted" and if Secure Messaging input format is correct:**

Byte	Length	Value	Description
#1	1	'81h'	T_{PV} : Tag for plain value data
#2	L	'NNh' or '81 NNh'	L_{PV} : length of returned data (=original Le). L is 2 bytes if L_{PV}>127 bytes.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Plain Data value
#(2+L+NN)	1	'8Eh'	T_{CC} : Tag for cryptographic checksum
#(3+L+NN)	1	'04h'	L_{CC} : Length of following cryptographic checksum
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Cryptographic checksum (4 most significant bytes)
SW	2	'XXXXh'	Status Words (SW1,SW2)

TCS_329 **Response Message if EF is marked as "Encrypted" and if Secure Messaging input format is correct:**

Byte	Length	Value	Description
#1	1	'87h'	$T_{PI\,CG}$: Tag for encrypted data (cryptogram)
#2	L	'MMh' or '81 MMh'	$L_{PI\,CG}$: length of returned encrypted data (different of original Le of the command due to padding). L is 2 bytes if $L_{PI\,CG}$ > 127 bytes.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Encrypted Data : Padding Indicator and cryptogram
#(2+L+MM)	1	'8Eh'	T_{CC} : Tag for cryptographic checksum
#(3+L+MM)	1	'04h'	L_{CC} : Length of following cryptographic checksum
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Cryptographic checksum (4 most significant bytes)
SW	2	'XXXXh'	Status Words (SW1,SW2)

The encrypted data returned contain a first byte indicating the used padding mode. For the tachograph application, the padding indicator always takes the value '01h', indicating that the used padding mode is the one specified in ISO/IEC 7816-4 (one byte with value '80h' followed by some null bytes: ISO/IEC 9797 method 2).

The "regular" processing states, described for the READ BINARY command with no secure messaging (see § 3.6.2.1), can be returned using the response message structures described above, under a '99h' Tag (as described in TCS 335).

Additionally, some errors specifically related to secure messaging can happen. In that case, the processing state is simply returned, with no secure messaging structure involved:

TCS_330 **Response Message if incorrect Secure Messaging input format**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If no current session key is available, the processing state **'6A88'** is returned. It happens either if the session key has not already been generated or if the session key validity has expired (in this case the IFD must re-run a mutual authentication process to set a new session key).
- If some expected data objects (as specified above) are missing in the secure messaging format, the processing state **'6987'** is returned : this error happens if an expected tag is missing or if the command body is not properly constructed.
- If some data objects are incorrect, the processing state returned is **'6988'** : this error happens if all the required tags are present but some lengths are different from the ones expected.
- If the verification of the cryptographic checksum fails, the processing state returned is **'6688'**.

3.6.3 Update Binary

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The UPDATE BINARY command message initiates the update (erase + write) of the bits already present in an EF binary with the bits given in the command APDU.

TCS_331 The command can be performed only if the security status satisfies the security attributes defined for the EF for the UPDATE function (If the Access Control of the UPDATE function includes PRO SM, a Secure Messaging must be added in the command).

3.6.3.1 Command without secure messaging

This command enables the IFD to write data into the EF currently selected, without the card verifying the integrity of data received. This plain mode is allowed only if the related file is not marked as "Encrypted".

TCS_332 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	No Secure Messaging asked
INS	1	'D6h'	
P1	1	'XXh'	Offset in bytes from the beginning of the file : Most Significant Byte
P2	1	'XXh'	Offset in bytes from the beginning of the file : Least Significant Byte
Lc	1	'NNh'	Lc Length of data to Update. Number of bytes to be written.
#6-#(5+NN)	NN	'XX..XXh'	Data to be written

Note: bit 8 of P1 must be set to 0.

TCS_333 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If no EF is selected , the processing state returned is **'6986'**.
- If the Access Control of the selected file are not satisfied, the command is interrupted with **'6982'**.
- If the Offset is not compatible with the size of the EF (Offset > EF size), the processing state returned is **'6B00'**.
- If the size of the data to be written is not compatible with the size of the EF (Offset + Lc > EF size) the processing state returned is **'6700'**.
- If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is **'6400'** or **'6500'**.
- If writing is unsuccessful, the processing state returned is **'6581'**.

3.6.3.2 Command with secure messaging

This command enables the IFD to write data into the EF currently selected, with the card verifying the integrity of data received. As no confidentiality is required, the data are not encrypted.

TCS_334 **Command Message**

Byte	Length	Value	Description
CLA	1	'0Ch'	Secure Messaging. Asked
INS	1	'D6h'	INS
P1	1	'XXh'	Offset in bytes from the beginning of the file : Most Significant Byte
P2	1	'XXh'	Offset in bytes from the beginning of the file : Least Significant Byte
Lc	1	'XXh'	Length of the secured data field
#6	1	'81h'	T_{PV} : Tag for plain value data
#7	L	'NNh' or '81 NNh'	L_{PV} : length of transmitted data. L is 2 bytes if L_{PV} > 127 bytes.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Plain Data value (Data to be written)
#(7+L+NN)	1	'8Eh'	T_{CC} : Tag for cryptographic checksum
#(8+L+NN)	1	'04h'	L_{CC} : Length of following cryptographic checksum
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Cryptographic checksum (4 most significant bytes)
Le	1	'00h'	As specified in ISO/IEC 7816-4

TCS_335 **Response message if correct Secure Messaging input format**

Byte	Length	Value	Description
#1	1	'99h'	T_{SW} : Tag for Status Words (to be protected by CC)
#2	1	'02h'	L_{SW} : length of returned Status Words
#3-#4	2	'XXXXh'	Status Words (SW1,SW2)
#5	1	'8Eh'	T_{CC} : Tag for cryptographic checksum
#6	1	'04h'	L_{CC} : Length of following cryptographic checksum
#7-#10	4	'XX..XXh'	Cryptographic checksum (4 most significant bytes)
SW	2	'XXXXh'	Status Words (SW1,SW2)

The "regular" processing states, described for the UPDATE BINARY command with no secure messaging (see § 3.6.3.1), can be returned using the response message structure described above.

Additionally, some errors specifically related to secure messaging can happen. In that case, the processing state is simply returned, with no secure messaging structure involved:

TCS_336 **Response Message if error in secure messaging**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If no current session key is available, the processing state **'6A88'** is returned.
- If some expected data objects (as specified above) are missing in the secure messaging format, the processing state **'6987'** is returned : this error happens if an expected tag is missing or if the command body is not properly constructed.
- If some data objects are incorrect, the processing state returned is **'6988'** : this error happens if all the required tags are present but some lengths are different from the ones expected.
- If the verification of the cryptographic checksum fails, the processing state returned is **'6688'**.

3.6.4 Get Challenge

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The GET CHALLENGE command asks the card to issue a challenge in order to use it in a security related procedure in which a cryptogram or some ciphered data are sent to the card.

TCS_337 The Challenge issued by the card is only valid for the next command, which uses a challenge, sent to the card.

TCS_338 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Length of Challenge expected).

TCS_339 **Response Message**

Byte	Length	Value	Description
#1-#8	8	'XX..XXh'	Challenge
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If Le is different from '08h', the processing state is **'6700'.**
- If parameters P1-P2 are incorrect, the processing state is **'6A86'.**

3.6.5 Verify

This command is compliant with ISO/IEC 7816-4, but has a restricted usage compared to the command defined in the norm.

The Verify command initiates the comparison in the card of the CHV (PIN) data sent from the command with the reference CHV stored in the card.

Note: The PIN entered by the user must be right padded with 'FFh' bytes up to a length of 8 bytes by the IFD.

TCS_340 If the command is successful, the rights corresponding to CHV presentation are opened and the remaining CHV attempt counter is reinitialised.

TCS_341 An unsuccessful comparison is recorded in the card in order to limit the number of further attempts of the use of the reference CHV.

TCS_342 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (the verified CHV is implicitly known)
Lc	1	'08h'	Length of CHV code transmitted
#6-#13	8	'XX..XXh'	CHV

TCS_343 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns '**9000**'.
- If the reference CHV is not found, the processing state returned is **'6A88'.**
- If the CHV is blocked, (the remaining attempt counter of the CHV is null), the processing state returned is **'6983'**. Once in that state, the CHV can never be successfully presented anymore.
- If the comparison is unsuccessful, the remaining attempt Counter is decreased and the status **'63CX'** is returned (X>0 and X equals the remaining CHV attempts counter. If X = 'F', the CHV attempts counter is greater than 'F').
- If the reference CHV is considered corrupted, the processing state returned is **'6400'** or **'6581'**.

3.6.6 Get Response

This command is compliant with ISO/IEC 7816-4.

This command (only necessary and available for T=0 Protocol) is used to transmit prepared data from the card to the interface device (case where a command had included both Lc and Le).

The GET_RESPONSE command has to be issued immediately after the command preparing the data, otherwise, the data are lost. After the execution of the GET_RESPONSE command (except if the error '61xx' or '6Cxx' occur, see below), the previously prepared data are no longer available.

TCS_344 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Number of bytes expected

TCS_345 **Response Message**

Byte	Length	Value	Description
#1-#X	X	'XX..XXh'	Data
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If no data have been prepared by the card, the processing state returned is **'6900'** or **'6F00'.**
- If Le exceeds the number of available bytes or if Le is null, the processing state returned is **'6Cxx'**, where xx denotes the exact number of available bytes. In that case, the prepared data are still available for a subsequent GET_RESPONSE command.
- If Le is not null and is smaller than the number of available bytes, the required data are sent normally by the card, and the processing state returned is **'61xx'**, where 'xx' indicates a number of extra bytes still available by a subsequent GET_RESPONSE command.
- If the command is not supported (protocol T=1), the card returns **'6D00'**.

3.6.7 PSO: Verify Certificate

This command is compliant with ISO/IEC 7816-8, but has a restricted usage compared to the command defined in the norm.

The VERIFY CERTIFICATE command is used by the card to obtain a Public Key from the outside and to check its validity.

TCS_346 When a VERIFY CERTIFICATE command is successful, the Public Key is stored for a future use in the Security environment. This key shall be explicitly set for the use in security related commands (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE or VERIFY CERTIFICATE) by the MSE command (see § 3.6.10) using its key identifier.

TCS_347 In any case, the VERIFY CERTIFICATE command uses the public key previously selected by the MSE command to open the certificate. This public key must be the one of a Contracting Party.

TCS_348 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	P1
P2	1	'AEh'	P2 : non BER-TLV coded data (concatenation of Data Elements)
Lc	1	'C2h'	Lc : Length of the certificate, 194 Bytes.
#6-#199	194	'XX..XXh'	Certificate : concatenation of data Elements (as described in sub-appendix 11)

TCS_349 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If the certificate verification fails, the processing state returned is **'6688'**. The verification and unwrapping process of the certificate is described in sub-appendix 11.
- If no Public Key is present in the Security Environment, **'6A88'** is returned.
- If the selected public key (used to unwrap the certificate) is considered corrupted, the processing state returned is **'6400'** or **'6581'**.
- If the selected public key (used to unwrap the certificate) has a CHA.LSB (CertificateHolderAuthorisation.equipmentType) different from '00' (i.e. is not the one of a Contracting Party) , the processing state returned is **'6985'**.

3.6.8 *Internal Authenticate*

This command is compliant with ISO/IEC 7816-4.

Using the INTERNAL AUTHENTICATE command, the IFD can authenticate the card.

The authentication process is described in sub-appendix 11. It includes the following statements :

TCS_350 The INTERNAL AUTHENTICATE command uses the card Private Key (implicitly selected) to sign authentication data including K1 (first element for session key agreement) and RND1, and uses the Public Key currently selected (through the last MSE command) to encrypt the signature and form the authentication token (more details in sub-appendix 11).

TCS_351 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Length of data sent to the card
#6 - #13	8	'XX..XXh'	Challenge used to authenticate the card
#14 -#21	8	'XX..XXh'	VU.CHR (see sub-appendix 11)
Le	1	'80h'	Length of the data expected from the card

TCS_352 **Response Message**

Byte	Length	Value	Description
#1-#128	128	'XX..XXh'	Card authentication token (see sub-appendix 11)
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If no Public Key is present in the Security Environment, the processing state returned is **'6A88'** .
- If no Private Key is present in the Security Environment, the processing state returned is **'6A88'** .
- If VU.CHR does not match the current public key identifier, the processing state returned is **'6A88'.**
- If the selected private key is considered corrupted, the processing state returned is **'6400'** or **'6581'**.

TCS_353 If the INTERNAL_AUTHENTICATE command is successful, the current session key, if existing, is erased and no longer available. In order to have a new session key available, the EXTERNAL_AUTHENTICATE command must be successfully performed.

3.6.9 *External Authenticate*

This command is compliant with ISO/IEC 7816-4.

Using the EXTERNAL AUTHENTICATE command, the card can authenticate the IFD.

The authentication process is described in sub-appendix 11. It includes the following statements :

TCS_354 A GET CHALLENGE command must precede the EXTERNAL_AUTHENTICATE command immediately. The card issues a challenge to the outside (RND3).

TCS_355 The verification of the cryptogram uses RND3 (challenge issued by the card), the card private key (implicitly selected) and the public key previously selected by the MSE command.

TCS_356 The card verifies the cryptogram, and if it is correct, the AUT access condition is opened.

TCS_357 The input cryptogram carries the second element for session key agreement K2.

TCS_358 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (the public Key to be used is implicitly known, and has been previously set by the MSE command)
Lc	1	'80h'	Lc (Length of the data sent to the card)
#6-#133	128	'XX..XXh'	Cryptogram (see sub-appendix 11)

TCS_359 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (Status Words (SW1,SW2))

- If the command is successful, the card returns '**9000**'.
- If no Public Key is present in the Security Environment, **'6A88'** is returned.
- If the CHA of the currently set public key is not the concatenation of the Tachograph application AID and of a VU equipment Type, the processing state returned is **'6F00'** (see sub-appendix 11).
- If no Private Key is present in the Security Environment, the processing state returned is **'6A88'** .
- If the verification of the cryptogram is wrong, the processing state returned is **'6688'** .
- If the command is not immediately preceded with a GET CHALLENGE command, the processing state returned is **'6985'**.
- If the selected private key is considered corrupted, the processing state returned is **'6400'** or **'6581'**.

TCS_360 If the EXTERNAL AUTHENTICATE command is successful, and if the first part of the session key is available from a successful INTERNAL AUTHENTICATE recently performed, the session key is set for future commands using secure messaging.

TCS_361 If the first session key part is not available from a previous INTERNAL AUTHENTICATE command, the second part of the session key, sent by the IFD, is not stored in the card. This mechanism ensures that the mutual authentication process is done in the order specified in sub-appendix 11.

3.6.10 *Manage Security Environment*

This command is used to set a public key for authentication purpose.

This command is compliant with ISO/IEC 7816-8. The use of this command is restricted regarding the related standard.

TCS_362 The key referenced in the MSE data field is valid for every file of the Tachograph DF.

TCS_363 The key referenced in the MSE data field remains the current public key until the next correct MSE command.

TCS_364 If the key referenced is not (already) present into the card, the security environment remains unchanged.

TCS_365 Command Message

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1 : referenced key valid for all cryptographic operations
P2	1	'B6h'	P2 (referenced data concerning Digital Signature)
Lc	1	'0Ah'	Lc : length of subsequent data field
#6	1	'83h'	Tag for referencing a public key in asymmetric cases
#7	1	'08h'	Length of the key reference (key identifier)
#8-#15	08h	'XX..XXh'	Key identifier as specified in sub-appendix 11

TCS_366 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If the referenced key is not present into the card, the processing state returned is **'6A88'** .
- If some expected data objects are missing in the secure messaging format, the processing state **'6987'** is returned. This can happen if the tag '83h' is missing.
- If some data objects are incorrect, the processing state returned is **'6988'**. This can happen if the length of the key identifier is not '08h'.
- If the selected key is considered corrupted, the processing state returned is **'6400'** or **'6581'**.

3.6.11 PSO: Hash

This command is used to transfer to the card the result of a hash calculation on some data. This command is used for the verification of digital signatures. The hash value is stored in EEPROM for the subsequent command verify digital signature.

This command is compliant with ISO/IEC 7816-8. The use of this command is restricted regarding the related standard.

TCS_367 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Return Hash code
P2	1	'A0h'	Tag : data field contains DOs relevant for hashing
Lc	1	'16h'	Length Lc of the subsequent data field
#6	1	'90h'	Tag for the hash code
#7	1	'14h'	Length of the hash code
#8-#27	20	'XX..XXh'	Hash code

TCS_368 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If some expected data objects (as specified above) are missing, the processing state **'6987'** is returned. This can happen if one of the tag '90h' is missing.
- If some data objects are incorrect, the processing state returned is **'6988'**. This error happens if the required tag is present but with a length different from '14h'.

3.6.12 Perform Hash of File

This command is not compliant with ISO/IEC 7816-8. Thus the CLA byte of this command indicates that there is a proprietary use of the PERFORM SECURITY OPERATION / HASH.

TCS_369 The perform hash file command is used to hash the data area of the currently selected transparent EF.

TCS_370 The result of the hash operation is stored in the card. It can then be used to get a digital signature of the file, using the PSO-COMPUTE_DIGITAL_SIGNATURE command. This result remains available for the COMPUTE DIGITAL SIGNATURE command until the next successful PERFORM HASH of FILE command.

TCS_371 **Command Message**

Byte	Length	Value	Description
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tag: Hash
P2	1	'00h'	P2: Hash the data of the currently selected transparent file

TCS_372 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If no application is selected, the processing state **'6985'** is returned
- If the selected EF is considered corrupted (file attributes or stored data integrity errors), the processing state returned is **'6400'** or **'6581'**.
- If the selected file is not a transparent file, the processing state returned is **'6986'**.

3.6.13 PSO: Compute Digital Signature

This command is used to compute the digital signature of previously computed hash code (see PERFORM HASH of FILE, § 3.6.12).

This command is compliant with ISO/IEC 7816-8. The use of this command is restricted regarding the related standard.

TCS_373 The card private key is used to compute the digital signature and is implicitly known by the card.

TCS_374 The card performs a digital signature using a padding method compliant with PKCS1 (see sub-appendix 11 for details).

TCS_375 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'9Eh'	Digital signature to be returned
P2	1	'9Ah'	Tag: data field contains data to be signed. As no data field is included, the data are supposed to be already present in the card (hash of file)
Le	1	'80h'	Length of the expected signature

TCS_376 **Response Message**

Byte	Length	Value	Description
#1-#128	128	'XX..XXh'	Signature of the previously computed hash
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns **'9000'**.
- If the implicitly selected private key is considered as corrupted, the processing state returned is **'6400'** or **'6581'**.

3.6.14 PSO: Verify Digital Signature

This command is used to verify the digital signature, provided as an input, in accordance with PKCS1 of a message, whose hash is known to the card. The signature algorithm is implicitly known by the card.

This command is compliant with ISO/IEC 7816-8. The use of this command is restricted regarding the related standard.

TCS_377 The Verify Digital Signature command always uses the public key selected by the previous Manage Security Environment command, and the previous hash code entered by a PSO: Hash command.

TCS_378 **Command Message**

Byte	Length	Value	Description
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	Tag : data field contains DOs relevant for verification
Lc	1	'83h'	Length Lc of the subsequent data field
#28	1	'9Eh'	Tag for Digital Signature
#29-#30	2	'8180h'	Length of digital signature (128 bytes, coded in accordance with ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Digital signature content

TCS_379 **Response Message**

Byte	Length	Value	Description
SW	2	'XXXXh'	Status Words (SW1,SW2)

- If the command is successful, the card returns '**9000**'.
- If the verification of the signature fails, the processing state returned is **'6688'**. The verification process is described in sub-appendix 11.
- If no public key is selected, the processing state returned is **'6A88'**.
- If some expected data objects (as specified above) are missing, the processing state **'6987'** is returned. This can happen if one of the required tag is missing.
- If no hash code is available to process the command (as a result of a previous PSO: Hash command), the processing state returned is **'6985'**.
- If some data objects are incorrect, the processing state returned is **'6988'**. This can happen if one of the required data objects length is incorrect.
- If the selected public key is considered corrupted, the processing state returned is **'6400'** or **'6581'**.

4. Tachograph cards structure

This paragraph specifies the file structures of the Tachograph cards for storage of accessible data.

It does not specify card manufacturer dependant internal structures, such as e.g. file headers, nor storage and handling of data elements needed for internal use only such as EuropeanPublicKey, CardPrivateKey, TDesSessionKey or WorkshopCardPin.

The useful storage capacity of Tachograph cards shall be of 11 Kbytes minimum. Greater capacities may be used. In such case, the structure of the card remains the same, but the number of records of some elements of the structure is increased. This paragraph specifies minimum and maximum values of these record numbers.

4.1 Driver card structure

TCS_400 After its personalisation, the driver card shall have the following permanent file structure and file access conditions:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application Identification	0501	ALW	NEV	No
├─EF Card Certificate	C100	ALW	NEV	No
├─EF CA Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card Download	050E	ALW	ALW	No
├─EF Driving Licence Info	0521	ALW	NEV	No
├─EF Events Data	0502	ALW	PRO SM /	No
├─EF Faults Data	0503	ALW	PRO SM /	No
├─EF Driver Activity Data	0504	ALW	PRO SM /	No
├─EF Vehicles Used	0505	ALW	PRO SM /	No
├─EF Places	0506	ALW	PRO SM /	No
├─EF Current Usage	0507	ALW	PRO SM /	No
├─EF Control Activity Data	0508	ALW	PRO SM /	No
└─EF Specific Conditions	0522	ALW	PRO SM /	No

TCS_401 All EFs structures shall be transparent.

TCS_402 Read with secure messaging shall be possible for all files under the DF Tachograph.

TCS_403 The driver card shall have the following data structure:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
├─ICC		*25*	*25*	
└─CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
└─CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
└─DF Tachograph		*1178*	*24926*	
├─EF Application Identification		*10*	*10*	
└─DriverCardApplicationIdentification		*10*	*10*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
└─noOfCardPlaceRecords		1	1	{00}
├─EF Card Certificate		*194*	*194*	
└─CardCertificate		194	194	{00..00}

EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
├CardIdentification		*65*	*65*	
├CardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└DriverCardHolderIdentification		*78*	*78*	
├cardHolderName		*72*	*72*	
├holderSurname		36	36	{00,
└holderFirstNames		36	36	{00,
├cardHolderBirthDate		4	4	{00..00}
└cardHolderPreferredLanguage		2	2	{20 20}
EF Card Download		*4*	*4*	
└LastCardDownload		4	4	
EF Driving Licence Info		*53*	*53*	
└CardDrivingLicenceInformation		*53*	*53*	
├drivingLicenceIssuingAuthority		36	36	{00,
├drivingLicenceIssuingNation		1	1	{00}
└drivingLicenceNumber		16	16	{20..20}
EF Events Data		*864*	*1728*	
└CardEventData		*864*	*1728*	
└cardEventRecords	6	*144*	*288*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00,
EF Faults Data		*576*	*1152*	
└CardFaultData		*576*	*1152*	
└cardFaultRecords	2	*288*	*576*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 0..20}
EF Driver Activity Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	5544	13776	{00..00}

EF Vehicles Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
EF Control Activity Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 The following values, used to provide sizes in the table above, are the minimum and maximum record number values the driver card data structure must use:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5544 bytes (28 days * 93 activity changes)	13776 Bytes (28 days * 240 activity changes)

4.2 Workshop card structure

TCS_405 After its personalisation, the workshop card shall have the following permanent file structure and file access conditions:

		Access conditions		
File	**File ID**	**Read**	**Update**	**Encrypted**
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application Identification	0501	ALW	NEV	No
├─EF Card Certificate	C100	ALW	NEV	No
├─EF CA Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM /	No
├─EF Sensor Installation Data	050B	ALW	NEV	**Yes**
├─EF Events Data	0502	ALW	PRO SM /	No
├─EF Faults Data	0503	ALW	PRO SM /	No
├─EF Driver Activity Data	0504	ALW	PRO SM /	No
├─EF Vehicles Used	0505	ALW	PRO SM /	No
├─EF Places	0506	ALW	PRO SM /	No
├─EF Current Usage	0507	ALW	PRO SM /	No
├─EF Control Activity Data	0508	ALW	PRO SM /	No
└─EF Specific Conditions	0522	ALW	PRO SM /	No

TCS_406 All EFs structures shall be transparent.

TCS_407 Read with secure messaging shall be possible for all files under the DF Tachograph.

TCS_408 The workshop card shall have the following data structure:

File / Data element	No of Records	Size (Bytes) Min	Max	Default Values
MF		*11055*	*29028*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00,
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00,
workshopAddress		36	36	{00,
cardHolderName				
holderSurname		36	36	{00,
holderFirstNames		36	36	{00,
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}

EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor Installation Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
EF Faults Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
EF Driver Activity Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}

EF Vehicles Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
EF Control Activity Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_409 The following values, used to provide sizes in the table above, are the minimum and maximum record number values the workshop card data structure must use:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 day * 93 activity changes)	492 bytes (1 day * 240 activity changes)

4.3 Control card structure

TCS_410 After its personalisation, the control card shall have the following permanent file structure and file access conditions:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├EF ICC	0002	ALW	NEV	No
├EF IC	0005	ALW	NEV	No
└DF Tachograph	0500			
├EF Application Identification	0501	ALW	NEV	No
├EF Card Certificate	C100	ALW	NEV	No
├EF CA Certificate	C108	ALW	NEV	No
├EF Identification	0520	AUT	NEV	No
└EF Controller Activity Data	050C	ALW	PRO SM /	No

TCS_411 All EFs structures shall be transparent.

TCS_412 Read with secure messaging shall be possible for files under the DF Tachograph.

TCS_413 The control card shall have the following data structure:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default values
├EF ICC		*25*	*25*	
└CardIccIdentification		*25*	*25*	
├clockStop		1	1	{00}
├cardExtendedSerialNumber		8	8	{00..00}
├cardApprovalNumber		8	8	{20..20}
├cardPersonaliserID		1	1	{00}
├embedderIcAssemblerId		5	5	{00..00}
└icIdentifier		2	2	{00 00}
├EF IC		*8*	*8*	
└CardChipIdentification		*8*	*8*	
├icSerialNumber		4	4	{00..00}
└icManufacturingReferences		4	4	{00..00}
└DF Tachograph		*11186*	*24526*	
├EF Application Identification		*5*	*5*	
└ControlCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfControlActivityRecords		2	2	{00 00}

EF Card Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00,
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00,
controlBodyAddress		36	36	{00,
cardHolderName				
holderSurname		36	36	{00,
holderFirstNames		36	36	{00,
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller Activity Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 The following values, used to provide sizes in the table above, are the minimum and maximum record number values the control card data structure must use:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4 Company card structure

TCS_415 After its personalisation, the company card shall have the following permanent file structure and file access conditions:

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├ EF ICC	0002	ALW	NEV	No
├ EF IC	0005	ALW	NEV	No
└ DF Tachograph	0500			
├ EF Application_Identification	0501	ALW	NEV	No
├ EF Card_Certificate	C100	ALW	NEV	No
├ EF CA_Certificate	C108	ALW	NEV	No
├ EF Identification	0520	ALW	NEV	No
└ EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 All EFs structures shall be transparent.

TCS_417 Read with secure messaging shall be possible for all files under the DF Tachograph.

TCS_418 The company card shall have the following data structure:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
EF ICC		*25*	*25*	
└ CardIccIdentification		*25*	*25*	
├ clockStop		1	1	{00}
├ cardExtendedSerialNumber		8	8	{00..00}
├ cardApprovalNumber		8	8	{20..20}
├ cardPersonaliserID		1	1	{00}
├ embedderIcAssemblerId		5	5	{00..00}
└ icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
└ CardChipIdentification		*8*	*8*	
├ icSerialNumber		4	4	{00..00}
└ icManufacturingReferences		4	4	{00..00}
DF Tachograph		*1114*	*24454*	
├ EF Application_Identification		*5*	*5*	
└ CompanyCardApplicationIdentification		*5*	*5*	
├ typeOfTachographCardId		1	1	{00}
├ cardStructureVersion		2	2	{00 00}
└ noOfCompanyActivityRecords		2	2	{00 00}
├ EF Card_Certificate		*194*	*194*	
└ CardCertificate		194	194	{00..00}
├ EF CA_Certificate		*194*	*194*	
└ MemberStateCertificate		194	194	{00..00}

+

EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00,
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00,
companyAddress		36	36	{00,
cardHolderPreferredLanguage		2	2	{20 20}
EF Company Activity Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_419 The following values, used to provide sizes in the table above, are the minimum and maximum record number values the company card data structure must use:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

SUB-APPENDIX III

PICTOGRAMS

PIC_001 The control device may use the following pictograms and pictograms combinations:

Basic pictograms

	People	Actions	Modes of operation
	Company		Company mode
	Controller	Control	Control mode
	Driver	Driving	Operational mode
	Workshop/test station	Inspection/calibration	Calibration mode
	Manufacturer		

	Activities	Duration
	Available	Current availability period
	Driving	Continuous driving time
	Rest	Current rest period
	Work	Current work period
	Break	Cumulative break time
?	Unknown	

	Equipment	Functions
1	Driver slot	
2	Co-driver slot	
	Card	
	Clock	
	Display	Displaying
	External storage	Downloading
	Power supply	
	Printer/printout	Printing
	Sensor	
	Tyre size	
	Vehicle/vehicle unit	

	Specific conditions
OUT	Out of scope
	Ferry/train crossing

Miscellaneous

!	Events	✕	Faults
⏵	Start of daily work period	⏯	End of daily work period
•	Location		
M	Manual entry of driver activities		
	Security		
>	Speed		
	Time		
Σ	Total/summary		

Qualifiers

24h	Daily
I	Weekly
II	Two weeks
+	From or to

Pictogram combinations

Miscellaneous

	Control place		
• ⏵	Location start of daily work period	⏯ •	Location end of daily work period
+	From time	+	To time
+	From vehicle		
OUT +	Out of scope begin	+ OUT	Out of scope end

Cards

	Driver card
	Company card
	Control card
	Workshop card
- - -	No card

Driving

	Crew driving
I	Driving time for one week
II	Driving time for two weeks

Printouts

24h Driver activities from card daily printout
24h Driver activities from VU daily printout
! × Events and faults from card printout
! × Events and faults from VU printout
Technical data printout
>> Over speeding printout

Events

! Insertion of a non valid card
! Card conflict
! Time overlap
! Driving without an appropriate card
! Card insertion while driving
! Last card session not correctly closed
>> Over speeding
! Power supply interruption
! Motion data error
! Security breach
! Time adjustment (by workshop)
> Over speeding control

Faults

× 1 Card fault (driver slot)
× 2 Card fault (co-driver slot)
× Display fault
× Downloading fault
× Printer fault
× Sensor fault
× VU internal fault

Manual entries procedure

? Still same daily work period ?
? End of previous work period ?
? Confirm or enter location of end of work period
? Enter start time
? Enter location of start of work period.

Note: Additional pictogram combinations to form printout block or record identifiers are defined in sub-appendix 4.

SUB-APPENDIX IV

PRINTOUTS

CONTENTS

1. Generalities

Each printout is built up by chaining various data blocks, possibly identified with a block identifier.

A data block contains one or more records, possibly identified with a record identifier.

PRT_001 When a block identifier immediately precedes a record identifier, the record identifier is not printed.

PRT_002 In the case where a data item is unknown, or must not be printed for data access rights reasons, spaces are printed instead.

PRT_003 If the content of a complete line is unknown, or need not to be printed, then the complete line is omitted.

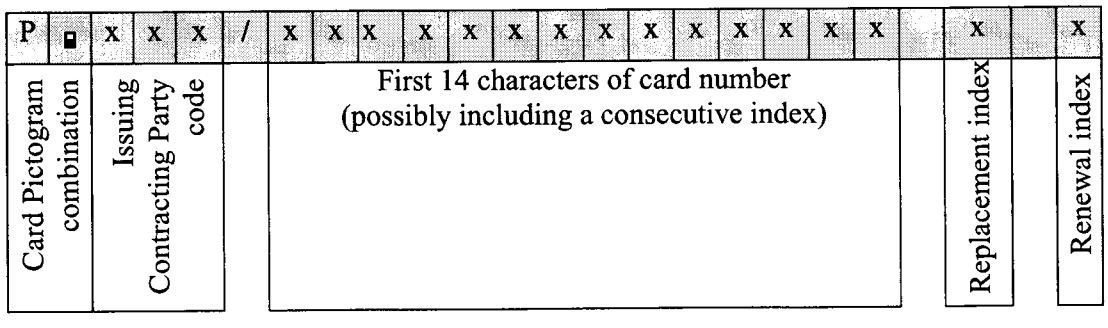
PRT_004 Numerical data fields are printed right aligned, with a space separator for thousands and millions, and without leading zeros.

PRT_005 String data fields are printed left aligned and filled up with spaces to data item length, or truncated to data item length when needed (names and addresses).

2. Data blocks specification

In this chapter the following format notation conventions have been used:

- Characters printed in **bold** denote plain text to be printed (printing remains in normal characters),
- Normal characters denote variables (pictograms or data) to be replaced by their values for printing,
- Variable names have been padded with underscores to show the data item length available for the variable,
- Dates are specified with a "dd/mm/yyyy" (day, month, year) format. A "dd.mm.yyyy" format may also be used,
- The term "card identification" denotes the composition of: the type of card through a card pictograms combination, the card issuing Contracting Party code, a forward slash character and the card number with the replacement index and the renewal index separated with a space:



PRT_006 Printouts shall use the following data blocks and/or data records, in accordance with the following meanings and formats:

Block or record number Meaning	Data Format
1. ***Date and time at which the document is printed.***	▼ dd/mm/yyyy hh:mm **(UTC)**
2. ***Type of printout.*** Block identifier Printout pictogram combination (see App. 3), Speed limiting device setting (Over speeding printout only)	----------▼---------- Picto xxx **km/h**
3. ***Card holder identification.*** Block identifier. P= people pictogram Card holder surname Card holder first name(s) (if any) Card identification Card expiry date (if any)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy

In the case where the card is a non-personal card, and holds no card holder surname, the company or workshop or control body name shall be printed instead.

4. ***Vehicle identification.*** Block identifier VIN Registering Contracting Party and VRN	----------🚙---------- 🚙 VIN_____ Nat/VRN_____
5. ***VU identification.*** Block identifier VU manufacturer's name VU part number	----------🖥---------- 🖥 VU_Manufacturer_____ VU_Part_Number__
6. ***Last calibration of the control device*** Block identifier Workshop name Workshop card identification Date of the calibration	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

7. ***Last control (by a control officer)***

Block identifier	----------▯----------
Controller's card identification	Card_Identification_____
Control date, time and type	▯ dd/mm/yyyy hh:mm pppp

Type of the control: Up to four pictograms. The type of control can be (a combination) of:
▮: Card downloading, ▼: VU downloading, ▼: printing, ▯: Displaying

8. ***Driver activities stored on a card in order of occurrence***

Block identifier	----------▣----------
Enquiry date (calendar day subject of the printout) + Daily card presence counter	dd/mm/yyyy xxx
8.1 *Period during which the card was not inserted*	
8.1a Record identifier (start of period)	----------
8.1b *Unknown period.* Start and end time, duration	hh:mm hh:mm hhhmm
8.1c *Activity manually entered.* Activity pictogram, start and end time (included), duration, rest periods of at least one hour are tagged with a star.	A hh:mm hh:mm hhhmm *
8.2 *Card insertion in slot S*	
Record identifier; S = Slot pictogram	---------S---------
Vehicle registering Contracting Party and VRN	▲ Nat/VRN_____
Vehicle odometer at card insertion	x xxx xxx km
8.3 *Activity (while card was inserted)*	
Activity pictogram, start and end time (included), duration, crew status (crew pictogram if CREW, blanks if SINGLE), rest periods of at least one hour are tagged with a star.	A hh:mm hh:mm hhhmm
8.3a *Specific condition.* Time of entry, specific condition pictogram (or pictogram combination).	hh:mm -----pppp-----
8.4 *Card withdrawal*	
Vehicle odometer and distance travelled since last insertion for which odometer is known	x xxx xxx km; x xxx km

9. ***Driver activities stored in a VU per slot in chronological order***

Block identifier	----------⊙----------
Enquiry date (calendar day subject of the printout)	dd/mm/yyyy
Vehicle odometer at 00:00 and 24:00	x xxx xxx - x xxx xxx **km**

10. ***Activities carried in slot S***

Block identifier	----------S----------

10.1 *Period where no card is inserted in slot S*

Record identifier.	----------
No Card inserted	⊙▪---
Vehicle odometer at beginning of period	x xxx xxx **km**

10.2 *Card insertion*

Card insertion Record identifier	----------
Driver's name	⊙ Last_Name_____
Driver's first name	First_Name_____
Driver's Card identification	Card_Identification_____
Driver's card expiry date	dd/mm/yyyy
Registering CP and VRN of previous vehicle used	**A**+Nat/VRN_____
Date and time of card withdrawal from previous vehicle	dd/mm/yyyy hh:mm
Blank line	
Vehicle odometer at card insertion, Manual entry of driver activities flag (M if yes, Blank if No).	x xxx xxx **km** **M**

10.3 *Activity*

Activity pictogram, start and end time (included), duration, crew Status (crew pictogram if CREW, blanks if SINGLE), rests of at least one hour are tagged with a star.	A hh:mm hh:mm hh**h**mm ⊙⊙ *

10.3a	*Specific condition.* Time of entry, specific condition pictogram (or pictogram combination).	hh:mm -----pppp-----
10.4	*Card withdrawal or End of 'No Card' period*	
	Vehicle odometer at card withdrawal or at end of 'no card' period and distance travelled since insertion, or since beginning of the 'No Card' period.	x xxx xxx **km**; x xxx **km**

11. ***Daily summary***

Block identifier	----------Σ----------

11.1	*VU summary of periods without card in driver slot*	
	Block identifier	1⊙▪---
11.2	*VU summary of periods without card in co-driver slot*	
	Block identifier	2⊙▪---
11.3	*VU daily summary per driver*	
	Record identifier	----------
	Driver's surname	Last_Name_____
	Driver's first name(s)	First_Name_____
	Driver's card identification	Card_Identification_____
11.4	*Entry of place where a daily work period begins and/or ends*	
	pi=location begin / end pictogram, time, country, region,	pihh:mm Cou Reg
	Odometer	x xxx xxx **km**

11.5	*Activity totals (from a card)*	
	Total driving duration, distance travelled	⊙ hh**h**mm x xxx **km**
	Total working and availability duration	* hh**h**mm ▫ hh**h**mm
	Total resting and unknown duration	⊢ hh**h**mm ? hh**h**mm
	Total duration of crew activities	⊙⊙ hh**h**mm

11.6	*Activity totals (periods without card driver slot)*	
	Total driving duration, distance travelled	⊙ hh**h**mm x xxx **km**
	Total working and availability duration	* hh**h**mm ▫ hh**h**mm
	Total resting duration	⊢ hh**h**mm

11.7 *Activity totals (periods without card co-driver slot)*

Total working and availability duration	* hh**h**mm ⧈ hh**h**mm
Total resting duration	⊢ hh**h**mm

11.8 *Activity totals (per driver both slots included)*

Total driving duration, distance travelled	• hh**h**mm x xxx **km**
Total working and availability duration	* hh**h**mm ⧈ hh**h**mm
Total resting duration	⊢ hh**h**mm
Total duration of crew activities	⊙⊙ hh**h**mm

When a daily printout is required for the current day, daily summary information is computed with available data at the time of the printout.

12. ***Events and/or faults stored on a card***

12.1 Block identifier last 5 'Events and Faults' from a card

---------- ! × ----------

12.2 Block identifier all recorded 'Events' on a card

---------- ! ----------

12.3 Block identifier all recorded 'Faults' on a card

---------- × ----------

12.4 *Event and/or Fault record*

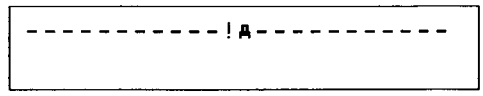
Record identifier	----------
Event/fault pictogram, record purpose, date time of start,	Pic dd/mm/yyyy hh:mm
Additional event/fault code (if any), duration	! xxx hh**h**mm
Registering Contracting Party & VRN of vehicle in which the event or fault occurred	Nat/VRN_____

13. ***Events and/or faults stored or on-going in a VU***

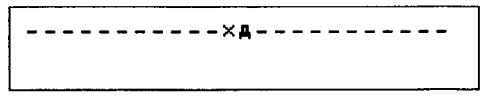
13.1 Block identifier last 5 'Events and Faults' from VU

---------- ! × ----------

13.2 Block identifier all recorded or on-going 'Events' in a VU



13.3 Block identifier all recorded or on-going 'Faults' in a VU



13.4 *Event and/or fault record*

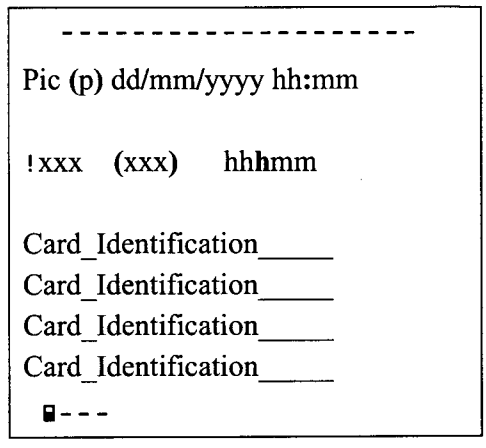
Record identifier

Event/fault pictogram, record purpose, date time of start,

Additional event/fault code (if any), No of similar events this day, duration

Identification of the cards inserted at start or end of the event or fault (up to 4 lines without repeating twice the same card numbers)

Case where no card was inserted



The record purpose (p) is a numerical code explaining why the event or fault was recorded, coded in accordance with the data element EventFaultRecordPurpose.

14. ***VU Identification***

Block identifier

VU manufacturer name

VU manufacturer address

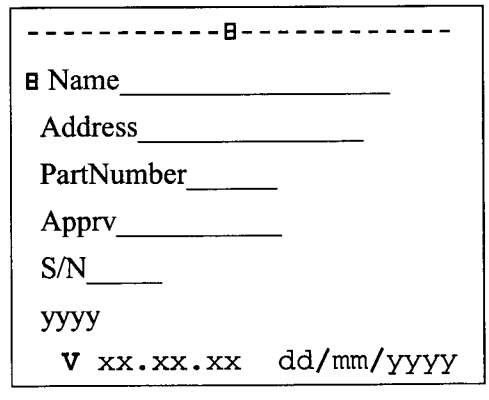
VU part number

VU approval number

VU serial number

VU year of manufacture

VU software version and installation date



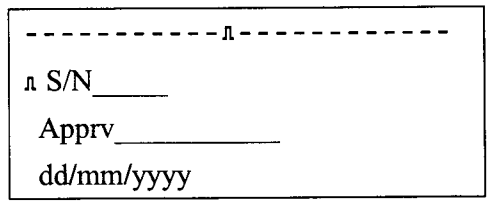
15. ***Sensor identification***

Block identifier

Sensor serial number

Sensor approval number

Sensor first installation date



16. ***Calibration data***

Block identifier	----------T----------

16.1 *Calibration record*

Record identifier	----------
Workshop having performed the calibration	T Workshop_name_____
Workshop address	Workshop_address_____
Workshop card identification	Card_Identification_____
Workshop card expiry date	dd/mm/yyyy
Blank line	
Calibration date + calibration purpose	T dd/mm/yyyy (p)
VIN	A VIN_____
Registering Contracting Party& VRN	Nat/VRN_____
Characteristic coefficient of vehicle	**w** xx xxx **Imp/km**
Constant of the control device	**k** xx xxx **Imp/km**
Effective circumference of wheel tyres	**l** xx xxx **mm**
Size of tyres mounted	• TyreSize_____
Speed limiting device setting	> xxx **km/h**
Old and new odometer values	x xxx xxx – x xxx xxx **km**

The calibration purpose (p) is a numerical code explaining why these calibration parameters were recorded, coded in accordance with the data element `CalibrationPurpose`.

17 ***Time adjustment***

Block identifier	----------@----------

17.1 *Time adjustment record*

Record identifier	----------
Old date and time	dd/mm/yyyy hh:mm
New date and time	dd/mm/yyyy hh:mm
Workshop having performed the time adjustment	Workshop_name_____
Workshop address	Workshop_address_____
Workshop card identification	Card_Identification_____
Workshop card expiry date	dd/mm/yyyy

18 ***Most recent event and Fault recorded in the VU***

Block identifier	----------!xA----------
Most recent event date time	dd/mm/yyyy hh:mm
Most recent fault date time	dd/mm/yyyy hh:mm

19	***Over speeding control information***	
	Block identifier	----------»»----------
	Date and time of last OVER SPEEDING CONTROL	»dd/mm/yyyy hh:mm
	Date/time of first over speeding and number of over speeding events since	»»dd/mm/yyyy hh:mm **(nnn)**
20	***Over speeding record***	
20.1	Block identifier 'First over speeding after the last calibration'	--------»»T---------
20.2	Block identifier 'The 5 most serious over the last 365 days'	-------»»(365)------
20.3	Block identifier 'The most serious for each of the last 10 days of occurrence'	-------»»(10)-------
20.4	Record identifier	----------
	Date time and duration	»»dd/mm/yyyy hh:mm hh**h**mm
	Max and average speeds, No. of similar events this day	xxx **km/h** xxx **km/h**(xxx)
	Driver's surname	Last_Name_____
	Driver's first name(s)	First_Name_____
	Driver card identification	Card_Identification_____
20.5	If no over speeding record exists in a block	»»---
21	***Hand-written information***	
	Block identifier	----------
21.1	Control Place	.....
21.2	Controller's signature	.....
21.3	From time	.....
21.4	To time	.....
21.5	Driver's signature	.....

'Hand-written information'; Insert enough blank lines above a hand-written item, to be able to actually write the required information or to put a signature.

3. Printout specifications

In this chapter the following notation conventions have been used:

N	Print block or record number N
N	Print block or record number N repeated as many times as necessary
X / Y	Print blocks or records X and/or Y as needed, and repeating as many times as necessary.

3.1 Driver Activities from Card Daily Printout

PRT_007 The driver activities from card daily printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Controller identification (if a control card is inserted in the VU)
3	Driver identification (from card subject of the printout)
4	Vehicle identification (vehicle from which printout is taken)
5	VU identification (VU from which printout is taken)
6	Last calibration of this VU
7	Last control the inspected driver has been subject to
8	Driver activities delimiter
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activities of the driver in order of occurrence
11	Daily summary delimiter
11.4	Places entered in chronological order
11.5	Activity totals
12.1	Events or faults from card delimiter
12.4	Event/Fault records (Last 5 events or faults stored in the card)
13.1	Events or faults from VU delimiter
13.4	Event/Fault records (Last 5 events or faults stored or on-going in the VU)
21.1	Control place
21.2	Controller's signature
21.5	Driver's signature

3.2 Driver Activities from VU Daily Printout

PRT_008 The driver activities from VU daily printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Card holder identification (for all cards inserted in VU)
4	Vehicle identification (vehicle from which printout is taken)
5	VU identification (VU from which printout is taken)
6	Last calibration of this VU
7	Last control on this control device
9	Driver activities delimiter
10	Driver slot delimiter (slot 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activities in chronological order (driver slot)
10	Co-driver slot delimiter (slot 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activities in chronological order (co-driver slot)
11	Daily summary delimiter
11.1	Summary of periods without card in driver slot
11.4	Places entered in chronological order
11.6	Activity totals
11.2	Summary of periods without card in co-driver slot
11.4	Places entered in chronological order
11.7	Activity totals
11.3	Summary of activities for a driver both slots included
11.4	Places entered by this driver in chronological order
11.7	Activity totals for this driver
13.1	Events faults delimiter
13.4	Event/Fault records (Last 5 events or faults stored or on-going in the VU)
21.1	Control place
21.2	Controller's signature
21.3	From time(space available for a driver without a card to indicate
21.4	To time which periods are relevant to himself)
21.5	Driver's signature

3.3 Events and Faults from Card Printout

PRT_009 The events and faults from card printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Controller identification (if a control card is inserted in the VU)
3	Driver identification (from card subject of the printout)
4	Vehicle identification (vehicle from which printout is taken)
12.2	Events delimiter
12.4	Event records (all events stored on the card)
12.3	Faults delimiter
12.4	Fault records (all faults stored on the card)
21.1	Control place
21.2	Controller's signature
21.5	Driver's signature

3.4 Events and Faults from VU Printout

PRT_010 The events and faults from VU printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Card holder identification (for all cards inserted in VU)
4	Vehicle identification (vehicle from which printout is taken)
13.2	Events delimiter
13.4	Event records (All Events stored or on-going in the VU)
13.3	Faults delimiter
13.4	Fault records (All Faults stored or on-going in the VU)
21.1	Control place
21.2	Controller's signature
21.5	Driver's signature

3.5 Technical data Printout

PRT_011 The technical data printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Card holder identification (for all cards inserted in VU)
4	Vehicle identification (vehicle from which printout is taken)
14	VU identification
15	Sensor identification

16	Calibration data delimiter
16.1	Calibration records (all records available in chronological order)
17	Time adjustment delimiter
17.1	Time adjustment records (all records available from time adjustment and from calibration data records)
18	Most recent event and Fault recorded in the VU

3.6 Over speeding Printout

PRT_012 The over speeding printout shall be in accordance with the following format:

1	Date and time at which the document is printed
2	Type of printout
3	Card holder identification (for all cards inserted in VU)
4	Vehicle identification (vehicle from which printout is taken)
19	Over speeding control information
20.1	Over speeding data identifier
20.4 / 20.5	First over speeding after the last calibration
20.2	Over speeding data identifier
20.4 / 20.5	The 5 most serious over speeding events over the last 365 days
20.3	Over speeding data identifier
20.4 / 20.5	The most serious over speeding for each of the last 10 days of occurrence
21.1	Control place
21.2	Controller's signature
21.5	Driver's signature

SUB-APPENDIX V

DISPLAY

In this sub appendix the following format notation conventions have been used:

- characters printed in **bold** denote plain text to be displayed (display remains in normal character),
- normal characters denote variables (pictograms or data) to be replaced by their values for displaying:
- dd mm yyyy: day, month, year,
- hh: hours,
- mm: minutes,
- D: duration pictogram,
- EF: event or fault pictograms combination,
- O: mode of operation pictogram.

DIS_001 The control device shall display data using the following formats:

Data	Format
Default display	
Local time	hh:mm
Mode of operation	O
Information related to the driver	1Dhh**h**mm ▪hh**h**mm
Information related to the co-driver	2Dhh**h**mm
Out of scope condition opened	OUT
Warning display	
Exceeding continuous driving time	1⊙hh**h**mm ▪hh**h**mm
Event or fault	EF
Other displays	
UTC date time	**UTC**⊙dd/mm/yyyy or **UTC**⊙dd.mm.yyyy hh:mm
Driver's continuous driving time and cumulative break time	1⊙hh**h**mm ▪hh**h**mm
Co-driver's continuous driving time and cumulative break time	2⊙hh**h**mm ▪hh**h**mm
Driver's cumulated driving time for the previous and the current week	1⊙‖ hhh**h**mm
Co-driver's cumulated driving time for the previous and the current week	2⊙‖ hhh**h**mm

SUB- APPENDIX VI

EXTERNAL INTERFACES

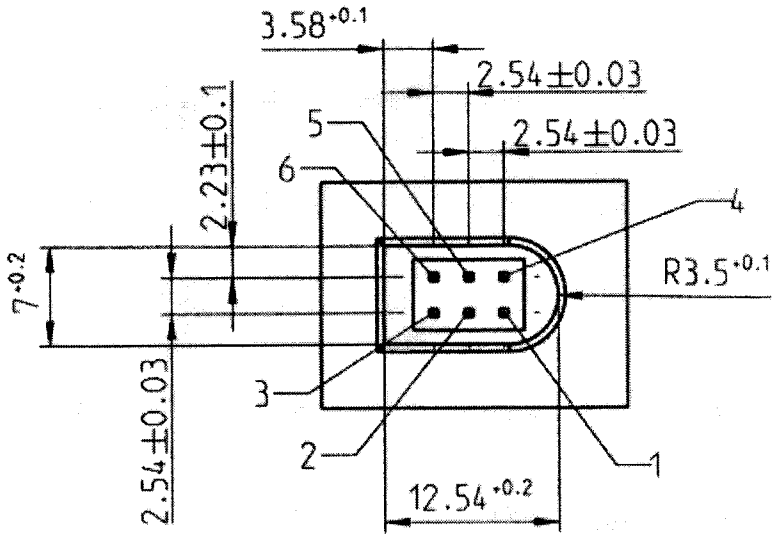
CONTENTS

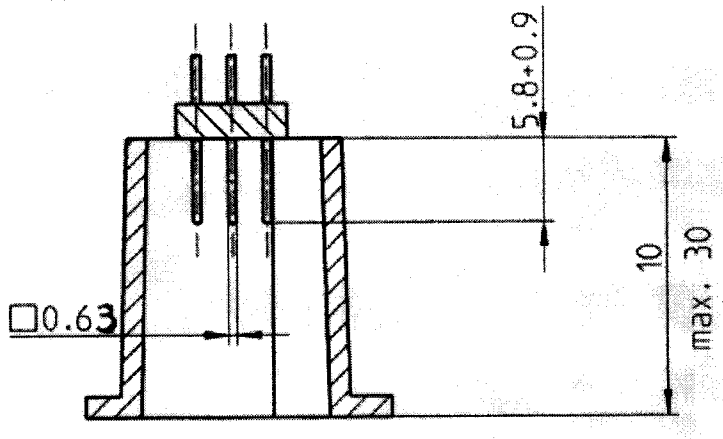
PAGE

1. Hardware

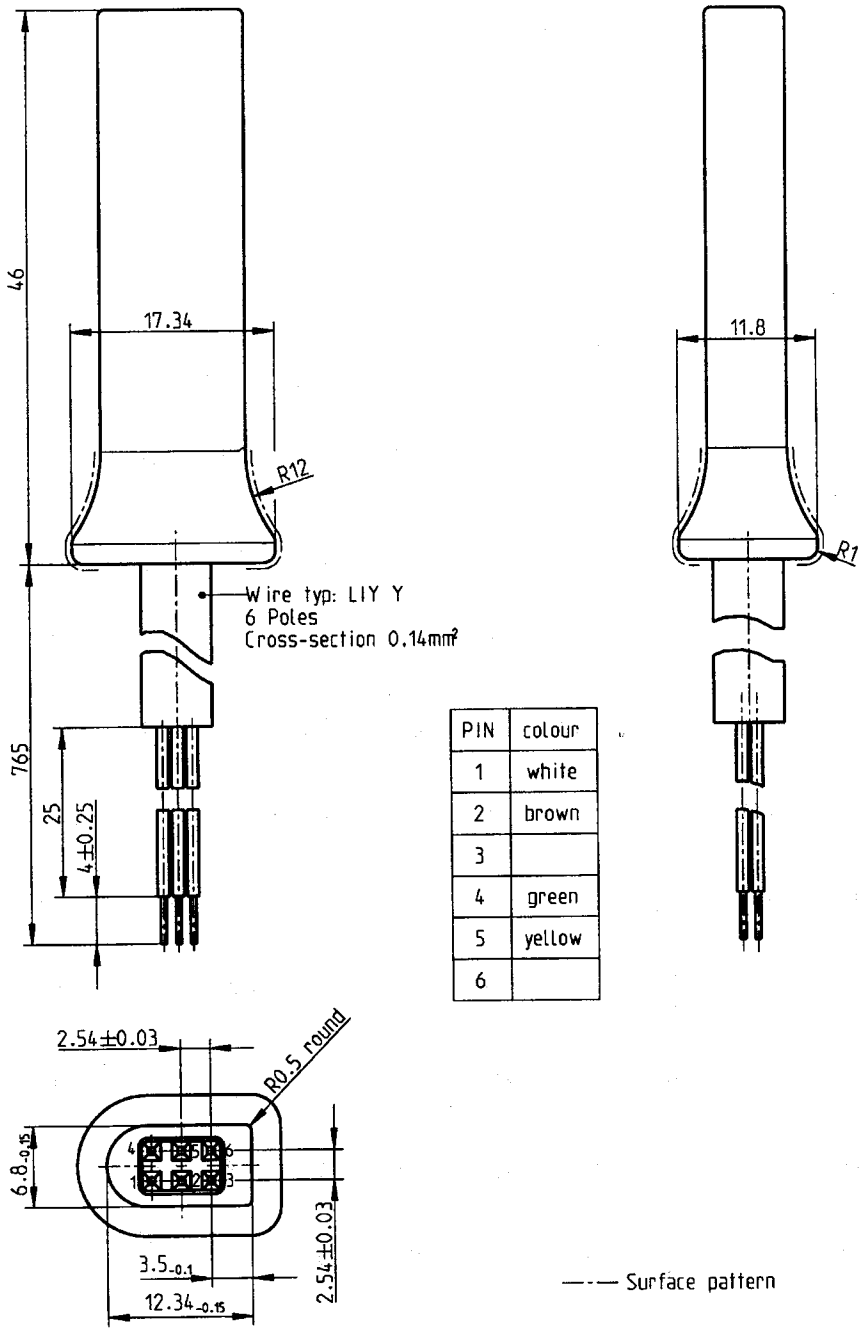
1.1 Connector

INT_001 The downloading/calibration connector shall be a 6 pin connector, accessible on the front panel without the need to disconnect any part of the control deviceand shall comply with the following drawing (all dimensions in millimetres):





The following diagram shows a typical 6 pin mating plug:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

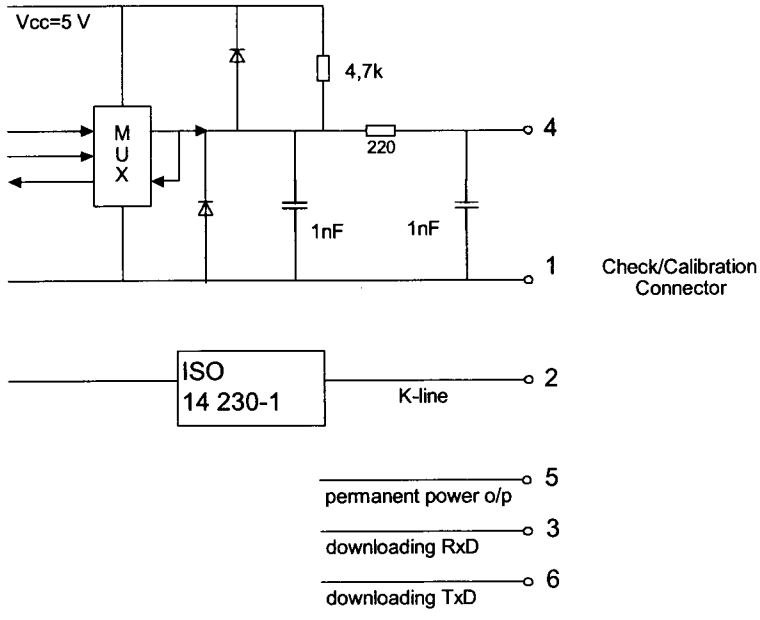
1.2 Contact allocation

INT_002 Contacts shall be allocated in accordance with the following table:

Pin	Description	Remark
1	Battery minus	Connected to the battery minus of the vehicle
2	Data communication	K-line (ISO 14230-1)
3	RxD – Downloading	Data input to control device
4	Input/output signal	Calibration
5	Permanent power output	The voltage range is specified to be that of the vehicle power minus 3V to allow for the voltage drop across the protective circuitry Output 40 mA
6	TxD – Downloading	Data output from control device

1.3 Block diagram

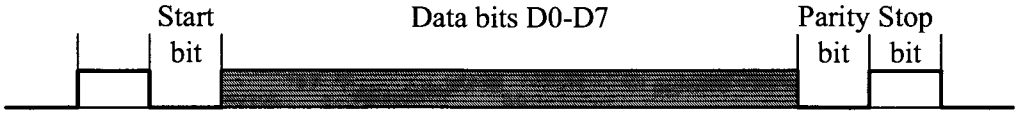
INT_003 The block diagram shall comply with the following:



2. Downloading interface

INT_004 The downloading interface shall comply to RS232 specifications.

INT_005 The downloading interface shall use one start bit, 8 data bits LSB first, one even parity bit and 1 stop bit.



Data byte organisation

Start bit: one bit with logic level 0;
Data bits: transmitted with LSB first;
Parity bit: even parity
Stop bit: one bit with logic level 1

When numerical data composed by more than one byte are transmitted, the most significant byte is transmitted first and the least significant byte last.

INT_006 Transmission baud rates shall be adjustable from 9 600 bps to 115 200 bps. Transmission shall be achieved at the highest possible transmission speed, the initial baud rate after a start of communication being set at 9 600 bps.

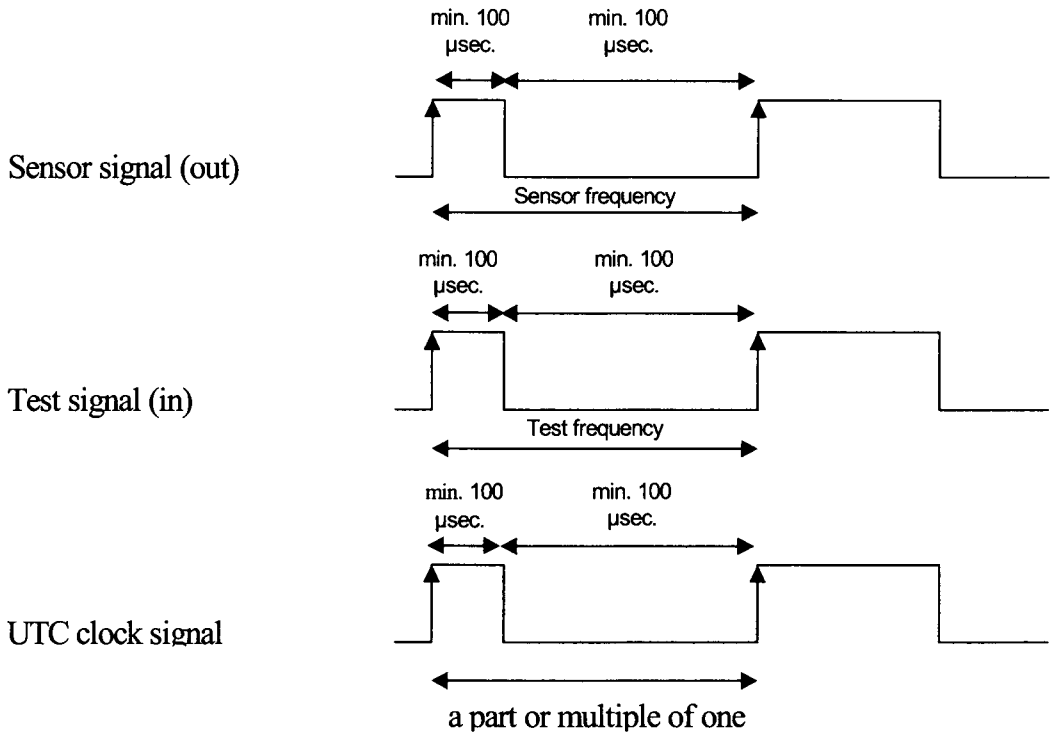
3. Calibration interface

INT_007 The data communication shall comply to ISO 14230-1 Road vehicles - Diagnostic systems - Keyword protocol 2000 - Part 1: Physical layer, First edition: 1999.

INT_008 The input/output signal shall comply with the following electrical specification:

Parameter	Minimum	Typical	Maximum	Remark
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frequency			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 The input/output signal shall comply with the following timing diagrams:


min. 100 µsec.
min. 100 µsec.
Sensor signal (out)
Sensor frequency
min. 100 µsec.
min. 100 µsec.
Test signal (in)
Test frequency
min. 100 µsec.
min. 100 µsec.
UTC clock signal
a part or multiple of one

SUB-APPENDIX VII

DATA DOWNLOADING PROTOCOLS

CONTENTS

CONTENTS (continued)

1. Introduction

This sub-appendix specifies the procedures to follow in order to perform the different types of data download to an External Storage Medium, together with the protocols that must be implemented to assure the correct data transfer and the full compatibility of the downloaded data format to allow any controller to inspect these data and be able to control their authenticity and their integrity before analysing them.

1.1 Scope

Data may be downloaded to an ESM:

- from a Vehicle Unit by an Intelligent Dedicated Equipment (IDE) connected to the VU,
- from a tachograph card by an IDE fitted with a card interface device (IFD),
- from a tachograph card via a vehicle unit by an IDE connected to the VU.

To give the possibility to verify the authenticity and integrity of downloaded data stored on an ESM, data is downloaded with a signature appended in accordance with sub-appendix 11 Common Security Mechanisms. The source equipment (VU or card) identification and its security certificates (Contracting Party and equipment) are also downloaded. The verifier of the data must possess independently a trusted European public key.

DDP_001 Data downloaded during one download session must be stored in the ESM within one file.

1.2 Acronyms and notations

The following acronyms are used in this sub-appendix:

AID Application Identifier
ATR Answer To Reset
CS Checksum byte
DF Dedicated File
DS_ Diagnostic Session
EF Elementary File
ESM External Storage Medium
FID File Identifier (File ID)
FMT Format Byte (first byte of message header)
ICC Integrated Circuit Card
IDE Intelligent Dedicated Equipment: The equipment used to perform data downloading to the ESM (e.g. Personal Computer)
IFD Interface Device
KWP Keyword Protocol 2000
LEN Length Byte (last byte of message header)
PPS Protocol Parameter Selection
PSO Perform Security Operation
SID Service Identifier
SRC Source byte
TGT Target Byte
TLV Tag Length Value
TREP Transfer Response Parameter
TRTP Transfer Request Parameter
VU Vehicle Unit

2. V.U. data downloading

2.1 Download procedure

In order to carry on a VU data download, the operator must perform the following operations:

- Insert his tachograph card inside a card slot of the VU(*);
- Connect the IDE to the VU download connector;
- Establish the connection between the IDE and the VU;
- Select on the IDE the data to download and send the request to the VU;
- Close the download session.

(*) The card inserted will trigger the appropriate access rights to the downloading function and to the data.

2.2 Data download protocol

The protocol is structured on a master-slave basis, with the IDE playing the master role and the VU playing the slave role.

The message structure, types and flow are principally based on the Keyword Protocol 2000 (KWP) (ISO 14230-2 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part2 : Data link layer).

The application layer is principally based on the current draft to date of ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1 : Diagnostic services, version 6 of 22 February 2001).

2.2.1 Message structure

DDP_002 All the messages exchanged between the IDE and the VU are formatted with a structure consisting of three parts:

- Header composed by a Format byte (FMT), a Target byte (TGT), a Source byte (SRC) and possibly a Length byte (LEN),
- Data field composed by a Service Identifier byte (SID) and a variable number of data bytes, which can include an optional diagnostic session byte (DS_) or an optional transfer parameter byte (TRTP or TREP).
- Checksum composed by a Checksum byte (CS).

Header				Data field					Checksum
FMT	TGT	SRC	LEN	SID	DATA	.....	.....	.....	CS
4 bytes				Max 255 bytes					1 byte

The TGT and SRC byte represent the physical address of the recipient and originator of the message. Values are F0 Hex for the IDE and EE Hex for the VU.

The LEN byte is the length of the Data field part.

The Checksum byte is the 8 bit sum series modulo 256 of all the bytes of the message excluding the CS itself.

FMT, SID, DS_, TRTP and TREP bytes are defined later in this document.

DDP_003 In the case where the data to be carried by the message is longer than the space available in the data field part, the message is actually sent in several sub messages. Each sub message bears a header, the same SID, TREP and a 2-byte sub message counter indicating the sub message number within the total message. To enable error checking and abort the IDE acknowledges every sub message. The IDE can accept the sub message, ask for it to be re-transmitted, request the VU to start again or abort the transmission.

DDP_004 If the last sub message contains exactly 255 bytes in the data field, a final sub message with an empty (except SID TREP and sub message counter) data field must be appended to show the end of the message.

Example:

Header	SID	TREP	Message	CS
4 Bytes	Longer than 255 Bytes			

Will be transmitted as:

Header	SID	TREP	00	01	Sub message 1	CS
4 Bytes	255 Bytes					

Header	SID	TREP	00	02	Sub message 2	CS
4 Bytes	255 Bytes					

...

Header	SID	TREP	xx	yy	Sub message n	CS
4 Bytes	Less than 255 Bytes					

or as:

Header	SID	TREP	00	01	Sub message 1	CS
4 Bytes	255 Bytes					

Header	SID	TREP	00	02	Sub message 2	CS
4 Bytes	255 Bytes					

...

Header	SID	TREP	xx	yy	Sub message n	CS
4 Bytes	255 Bytes					

Header	SID	TREP	xx	yy+1	CS
4 Bytes	4 bytes				

2.2.2 Message types

The communication protocol for data download between the VU and the IDE requires the exchange of 8 different message types.

The following table summarises these messages.

Message Structure	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte CheckSum
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS / TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		'EA' '8F'	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00 ,00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Notes:

- Sid Req = the Sid of the corresponding request.
- TREP = the TRTP of the corresponding request.
- Dark cells denotes that nothing is transmitted.
- The term upload (as seen from the IDE) is used for compatibility with ISO 14229. It means the same as download (as seen from the VU).
- Potential 2-byte sub message counters are not shown in this table.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 This message is issued by the IDE to establish the communication link with the VU. Initial communications are always performed at 9600 baud (until baud rate is eventually changed using the appropriate Link control services).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 This message is issued by the VU to answer positively to a start communication request. It includes the 2 key bytes 'EA' '8F' indicating that the unit supports protocol with header including target source and length information.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 The Start Diagnostic Session request message is issued by the IDE in order to request a new diagnostic session with the VU. The sub function 'default session' (81 Hex) indicates a standard diagnostic session is to be opened.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 The Positive Response Start Diagnostic message is sent by the VU to answer positively to Diagnostic Session Request.

2.2.2.5 Link Control Service (SID 87)

DDP_052 The Link Control Service is used by the IDE to initiate a change in baud rate. This takes place in two steps. In step one the IDE proposes the baud rate change, indicating the new rate. On receipt of a positive message from the VU the IDE sends out confirmation of the baud rate change to the VU (step two). The IDE then changes to the new baud rate. After receipt of the confirmation the VU changes to the new baud rate

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 The Link Control Positive response is issued by the VU to answer positively to Link Control Service request (step one). Note that no response is given to the confirmation request (step two).

2.2.2.7 Request Upload (SID 35)

DDP_009 The Request Upload message is issued by the IDE to specify to the VU that a download operation is requested. To meet the requirements of ISO14229 data is included covering address, the size and format details for the data requested. As these are not known to the IDE prior to a download, the memory address is set to 0, format is unencrypted and uncompressed and the memory size is set to the maximum.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 The Positive Response Request Upload message is sent by the VU to indicate to the IDE that the VU is ready to download data. To meet the requirements of ISO 14229 data is included in this positive response message, indicating to the IDE that further Positive Response Transfer Data messages will include 00FF hex bytes maximum.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 The Transfer Data Request is sent by the IDE to specify to the VU the type of data that are to be downloaded. A one byte Transfer Request Parameter (TRTP) indicates the type of transfer.

There are six types of data transfer:
- Overview (TRTP 01),
- Activities of a specified date (TRTP 02),
- Events and faults (TRTP 03),
- Detailed speed (TRTP 04),
- Technical data (TRTP 05),
- Card download (TRTP 06).

DDP_054 It is mandatory for the IDE to request the overview data transfer (TRTP 01) during a download session as this only will ensure that the VU certificates are recorded within the downloaded file (and allow for verification of digital signature).

In the second case (TRTP 02) the Transfer Data Request message includes the indication of the calendar day (`TimeReal` format) to be downloaded.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 The Positive Response Transfer Data is sent by the VU in response to the Transfer Data Request. The message contains the requested data, with a Transfer Response Parameter (TREP) corresponding to the TRTP of the request.

DDP055 In the first case (TREP 01), the VU will send data helping the IDE operator to choose the data he wants to download further. The information contained within this message is:
- Security certificates,
- Vehicle identification,
- VU current date and time,
- Min and Max downloadable date (VU data),
- Indication of cards presence in the VU,
- Previous download to a company,
- Company locks,
- Previous controls.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 The Request Transfer Exit message is sent by the IDE to inform the VU that the download session is terminated.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 The Positive Response Request Transfer Exit message is sent by the VU to acknowledge the Request Transfer Exit.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 The Stop Communication Request message is sent by the IDE to disconnect the communication link with the VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 The Positive Response Stop Communication message is sent by the VU to acknowledge the Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 The Acknowledge Sub Message is sent by the IDE to confirm receipt of each part of a message that is being transmitted as several sub messages. The data field contains the SID received from the VU and a 2-byte code as follows:

- MsgC +1 Acknowledges correct receipt of sub message number MsgC.
  Request from the IDE to the VU to send next sub message
- MsgC indicates a problem with the receipt of sub message number MsgC.
  Request from the IDE to the VU to send the sub message again.
- FFFF requests termination of the message.
  This can be used by the IDE to end the transmission of the VU message for any reason.

The last sub message of a message (LEN byte < 255) may be acknowledged using any of these codes or not acknowledged.

The VU responses that will consist of several sub messages are:

- Positive Response Transfer Data (SID 76)

2.2.2.16 Negative Response (SID 7F)

DDP_018 The Negative Response message is sent by the VU in response to the above request messages when the VU cannot satisfy the request. The data fields of the message contains the SID of the response (7F), the SID of the request, and a code specifying the reason of the negative response. The following codes are available:

- 10 general reject
  The action cannot be performed for a reason not covered below.
- 11 service not supported
  The SID of the request is not understood.
- 12 sub function not supported
  The DS_ or TRTP of the request is not understood, or there are no further sub messages to be transmitted.
- 13 incorrect message length
  The length of the received message is wrong.
- 22 conditions not correct or request sequence error
  The required service is not active or the sequence of request messages is not correct.
- 31 Request out of range
  The request parameter record (data field) is not valid.
- 50 upload not accepted
  The request cannot be performed (VU in a non appropriate mode of operation or internal fault of the VU).

- 78 response pending
  The action requested cannot be completed in time and the VU is not ready to accept another request.
- FA data not available
  The data object of a data transfer request are not available in the VU (e.g. no card is inserted, ...).

2.2.3 Message flow

A typical message flow during a normal data download procedure is the following:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
...		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 Timing

DDP_019 During normal operation the timing parameters shown in the following figure are relevant:

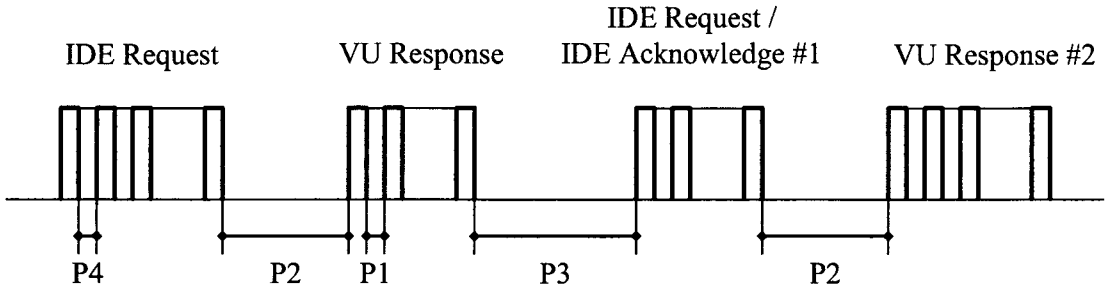


Figure 1

Message flow, timing

Where:

P1 = Inter byte time for VU response.

P2 = Time between end of IDE request and start of VU response, or between end of IDE acknowledge and start of next VU response.

P3 = Time between end of VU response and start of new IDE request, or between end of VU response and start of IDE acknowledge, or between end of IDE request and start of new IDE request if VU fails to respond.

P4 = Inter byte time for IDE request.

P5 = Extended value of P3 for card downloading.

The allowed values for the timing parameters are showed in the following table (KWP extended timing parameters set, used in case of physical addressing for faster communication).

Timing Parameter	Lower limit Value (ms)	Upper limit value (ms)
P1	0	20
P2	20	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 minutes

(*) if the VU responds with a Negative Response containing a code meaning "request correctly received, response pending", this value is extended to the same upper limit value of P3.

2.2.5 Error handling

If an error occurs during the message exchange, the message flow scheme is modified depending on which equipment has detected the error and on the message generating the error.

In figure 2 and figure 3 the error handling procedures for the VU and the IDE are respectively shown.

2.2.5.1 Start Communication phase

DDP_020 If the IDE detects an error during the Start Communication phase, either by timing or by the bit stream, then it will wait for a period P3min before issuing again the request.

DDP_021 If the VU detects an error in the sequence coming from the IDE, it shall send no response and wait for another Start Communication Request message within a period P3 max.

2.2.5.2 Communication phase

Two different error handling areas can be defined:

1. The VU detects an IDE transmission error.

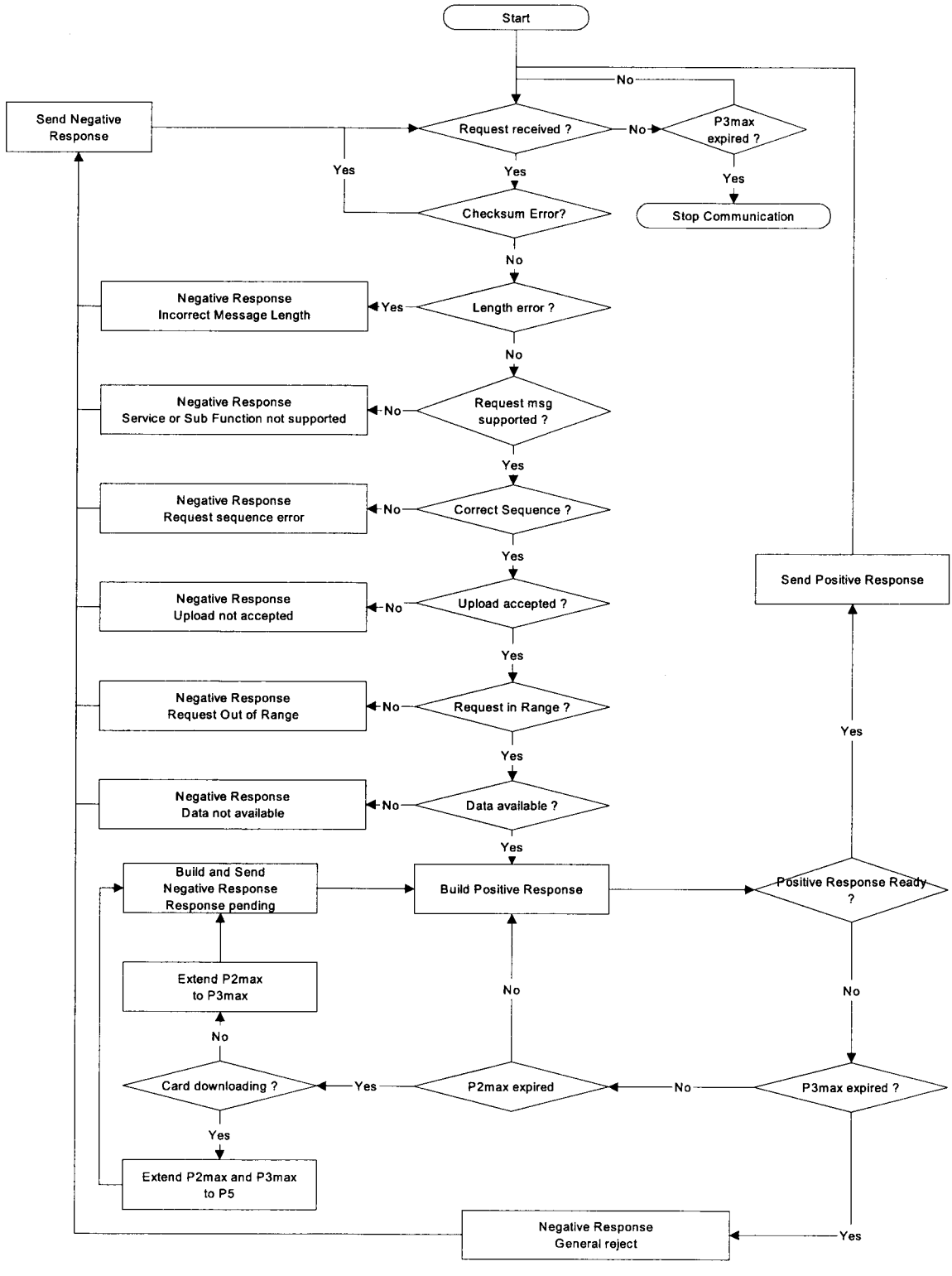
DDP_022 For every received message the VU shall detect timing errors, byte format errors (e.g. start and stop bit violations) and frame errors (wrong number of bytes received, wrong checksum byte).

DDP_023 If the VU detects one of the above errors, then it sends no response and ignores the message received.

DDP_024 The VU may detect other errors in the format or content of the received message (e.g. message not supported) even if the message satisfies the length and checksum requirements; in such a case, the VU shall respond to the IDE with a Negative Response message specifying the nature of the error.

Figure 2

VU error handling



2. The IDE detects a VU transmission error.

DDP_025 For every received message the IDE shall detect timing errors, byte format errors (e.g. start and stop bit violations) and frame errors (wrong number of bytes received, wrong checksum byte).

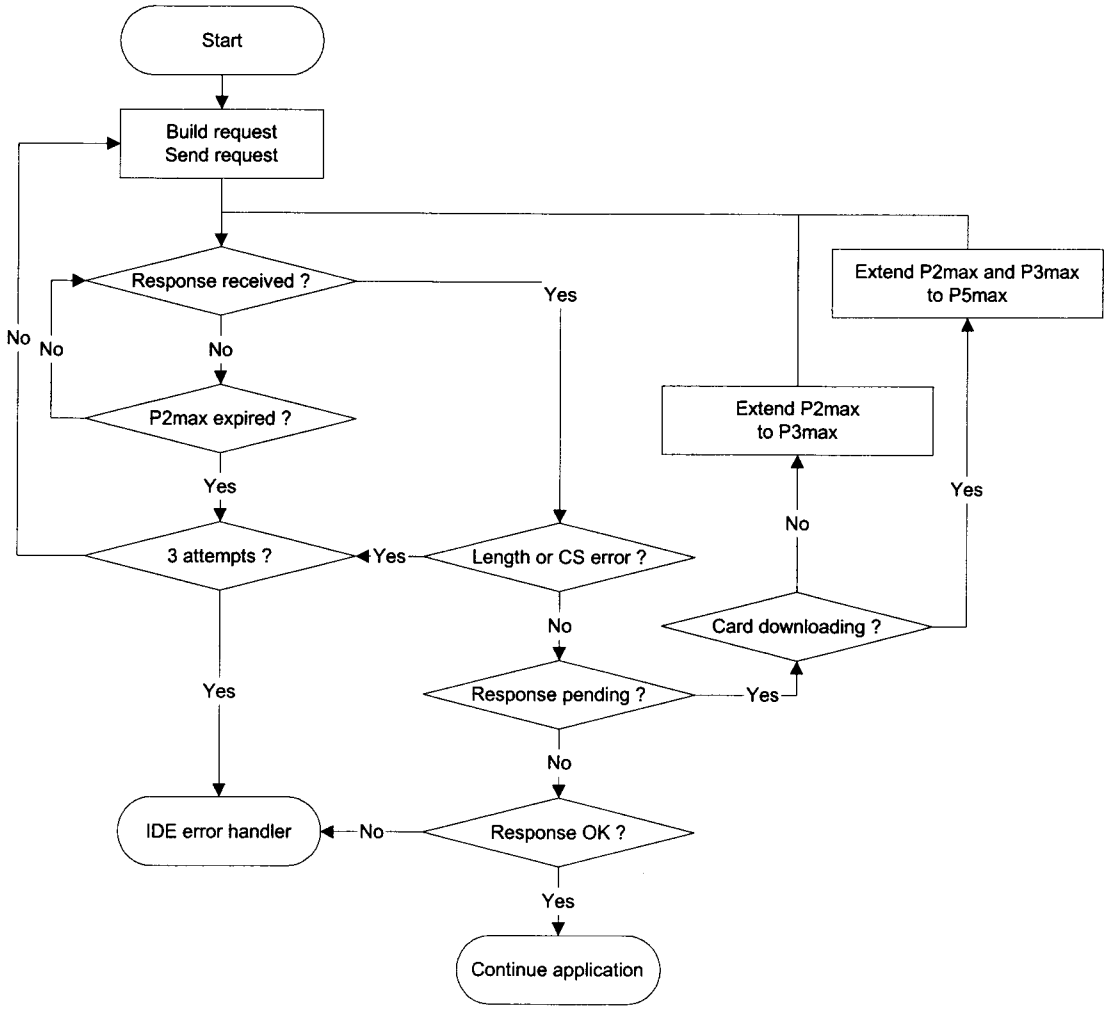
DDP_026 The IDE shall detect sequence errors, e.g. incorrect sub message counter increments in successive received messages.

DDP_027 If the IDE detects an error or there was no response from the VU within a P2max period, the request message will be sent again for a maximum of three transmissions in total. For the purposes of this error detection a sub message acknowledge will be considered as a request to the VU.

DDP_028 The IDE shall wait at least for a period of P3min before beginning each transmission; the wait period shall be measured from the last calculated occurrence of a stop bit after the error was detected.

Figure 3

IDE error handling



2.2.6 Response Message content

This paragraph specifies the content of the data fields of the various positive response messages.

Data elements are defined in sub-appendix 1 data dictionary.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 The data field of the "Positive Response Transfer Data Overview" message shall provide the following data in the following order under the SID 76 Hex, the TREP 01 Hex and appropriate sub message splitting and counting:

Data element	Length (Bytes)	Comment
MemberStateCertificate	194	VU Security certificates
VUCertificate	194	
VehicleIdentificationNumber	17	Vehicle identification
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	VU current date and time
VuDownloadablePeriod		Downloadable period
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Type of cards inserted in the VU
VuDownloadActivityData		Previous VU download
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		All company locks stored. If the section is empty, only noOfLocks = 0 is sent.
noOfLocks	1	
...	(98)	
Vu Company Locks Record: lockInTime	4	
Vu Company Locks Record: lockOutTime	4	
Vu Company Locks Record: companyName	36	
Vu Company Locks Record: companyAddress	36	
Vu Company Locks Record: companyCardNumber	18	
...		
VuControlActivityData		All control records stored in the VU. If the section is empty, only noOfControls = 0 is sent.
noOfControls	1	
...	(31)	
Vu Control Activity Record: controlType	1	
Vu Control Activity Record: controlTime	4	
Vu Control Activity Record: controlCardNumber	18	
Vu Control Activity Record: downloadPeriodBeginTime	4	
Vu Control Activity Record: downloadPeriodEndTime	4	
...		
Signature	128	RSA signature of all data (except certificates) starting from VehicleIdentificationNumber down to last byte of last VuControlActivityRecord.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 The data field of the "Positive Response Transfer Data Activities" message shall provide the following data in the following order under the SID 76 Hex, the TREP 02 Hex and appropriate sub message splitting and counting:

Data element	Length (Bytes)	Comment
TimeReal	4	Date of day downloaded
OdometerValueMidnight	3	Odometer at end of downloaded day
VuCardIWData		Cards insertion withdrawal cycles data. – If this section contains no available data, only noOfVuCardIWRecords = 0 is sent. – When a VuCardIWRecord lies across 00:00 (card insertion on previous day) or across 24:00 (card withdrawal the following day) it shall appear in full within the two days involved.
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord: cardHolderName		
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Slots status at 00:00 and activity changes recorded for the day downloaded.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Places related data recorded for the day downloaded. If the section is empty, only noOfPlaceRecords = 0 is sent.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		

VuSpecificConditionData		Specific conditions data recorded for the day downloaded. If the section is empty, only noOfSpecificConditionRecords =0 is sent
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
entryTime	4	
specificConditionType	1	
...		
Signature	128	RSA signature of all data starting from TimeReal down to last byte of last specific condition record.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 The data field of the "Positive Response Transfer Data Events and Faults" message shall provide the following data in the following order under the SID 76 Hex, the TREP 03 Hex and appropriate sub message splitting and counting:

Data element	Length (Bytes)	Comment
VuFaultData		All faults stored or on-going in the VU. If the section is empty, only noOfVuFaults = 0 is sent.
noOfVuFaults	1	
...	(82)	
VuFaultRecord: faultType	1	
VuFaultRecord: faultRecordPurpose	1	
VuFaultRecord: faultBeginTime	4	
VuFaultRecord: faultEndTime	4	
VuFaultRecord: cardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: cardNumberDriverSlotEnd	18	
VuFaultRecord: cardNumberCodriverSlotEnd	18	
...		
VuEventData		All events (except over speeding) stored or on-going in the VU. If the section is empty, only noOfVuEvents = 0 is sent.
noOfVuEvents	1	
...	(83)	
VuEventRecord: eventType	1	
VuEventRecord: eventRecordPurpose	1	
VuEventRecord: eventBeginTime	4	
VuEventRecord: eventEndTime	4	
VuEventRecord: cardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: cardNumberDriverSlotEnd	18	
VuEventRecord: cardNumberCodriverSlotEnd	18	
VuEventRecord: similarEventsNumber	1	
...		

VuOverSpeedingControlData		Data related to last over speeding control (default value if no data).
lastOverspeedControlTime	4	
firstOverspeedSince	4	
numberOfOverspeedSince	1	
VuOverSpeedingEventData		All over speeding events stored in the VU. If the section is empty, only noOfVuOverSpeedingEvents = 0 is sent.
noOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord		
eventType	1	
eventRecordPurpose	1	
eventBeginTime	4	
eventEndTime	4	
maxSpeedValue	1	
averageSpeedValue	1	
CardNumberDriverSlotBegin	18	
similarEventsNumber	1	
...		
VuTimeAdjustmentData		All time adjustment events stored in the VU (outside the frame of a full calibration). If the section is empty, only noOfVuTimeAdjRecords = 0 is sent.
noOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord		
oldTimeValue	4	
newTimeValue	4	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
...		
Signature	128	RSA signature of all data starting from noOfVuFaults down to last byte of last time adjustment record

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 The data field of the "Positive Response Transfer Data Detailed Speed" message shall provide the following data in the following order under the SID 76 Hex, the TREP 04 Hex and appropriate sub message splitting and countering:

Data element	Length (Bytes)	Comment
VuDetailedSpeedData		All detailed speed stored in the VU (one speed block per minute during which the vehicle has been moving)
noOfSpeedBlocks	2	
...		
VuDeatailed SpeedBlock: speedBlockBeginDate	4	
VuDeatailed SpeedBlock: speedsPerSecond	60	60 speed values per minute (one per second).
...		
Signature	128	RSA signature of all data starting from noOfSpeedBlocks down to last byte of last speed block.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 The data field of the "Positive Response Transfer Data Technical Data" message shall provide the following data in the following order under the SID 76 Hex, the TREP 05 Hex and appropriate sub message splitting and counting:

Data element	Length (Bytes)	Comment
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		All calibration records stored in the VU.
noOfVuCalibrationRecords	1	
...	(167)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA signature of all data starting from vuManufacturerName down to last byte of last VuCalibrationRecord.

2.3 ESM File storage

DDP_034 When a download session has included a VU data transfer, the IDE shall store within one physical file all data received from the VU during the download session within Positive Response Transfer Data messages. Data stored excludes message headers, sub-message counters, empty sub-messages and checksums but include the SID and TREP (of the first sub-message only if several sub-messages).

3. Tachograph cards downloading protocol

3.1 Scope

This paragraph describes the direct card data downloading of a tachograph card to an IDE. The IDE is not part of the secure environment; therefore no authentication between the card and the IDE is performed.

3.2 Definitions

Download session: Each time a download of the ICC data is performed. The session covers the complete procedure from the reset of the ICC by an IFD until the deactivation of the ICC (withdraw of the card or next reset).

Signed Data File: A file from the ICC. The file is transferred to the IFD in plain text. On the ICC the file is hashed and signed and the signature is transferred to the IFD.

3.4 Card Downloading

DDP_035 The download of a tachograph card includes the following steps:

- Download the common information of the card in the EFs ICC and IC. This information is optional and is not secured with a digital signature.
- Download the EFs Card_Certificate and CA_Certificate. This information is not secured with a digital signature.
  It is mandatory to download these files for each download session.
- Download the other application data EFs (within Tachograph DF) except EF Card_Download. This information is secured with a digital signature.
- It is mandatory to download at least the EFs Application_Identification and ID for each download session.
  - When downloading a driver card it is also mandatory to download the following EFs:
    - Events_Data,
    - Faults_Data,
    - Driver_Activity_Data,
    - Vehicles_Used,
    - Places,
    - Control_Activity_Data,
    - Specific_Conditions.
- When downloading a driver card, update the LastCardDownload date in EF Card_Download,
- When downloading a workshop card, reset the calibration counter in EF Card_Download.

3.3.1 Initialisation sequence

DDP_036 The IDE shall initiate the sequence as follows:

Card	Direction	IDE / IFD	Meaning / Remarks
	⇦	Hardware reset	
ATR	⇨		

It is optional to use PPS to switch to a higher baudrate as long as the ICC supports it.

3.3.2 Sequence for un-signed data files

DDP_037 The sequence to download the EFs ICC, IC, Card_Certificate and CA_Certificate is as follows:

Card	Direction	IDE / IFD	Meaning / Remarks
	⇦	Select File	Select by File identifiers
OK	⇨		
	⇦	Read Binary	If the file contains more data than the buffer size of the reader or the card the command has to be repeated until the complete file is read.
File Data OK	⇨	Store data to ESM	according to 3.4, (3.4 Data storage format)

Note: Before selecting the Card_Certificate EF, the Tachograph Application must be selected (selection by AID).

3.3.3 Sequence for Signed data files

DDP_038 The following sequence shall be used for each of the following files that has to be downloaded with their signature:

Card	Dir	IDE / IFD	Meaning / Remarks
	⇦	Select File	
OK	⇨		
	⇦	Perform Hash of File	Calculates the hash value over the data content of the selected file using the prescribed hash algorithm in accordance with sub-appendix 11. This command is not an ISO-Command.
Calculate Hash of File and store Hash value temporarily			
OK	⇨		
	⇦	Read Binary	If the file contains more data than the buffer of the reader or the card can hold, the command has to be repeated until the complete file is read.
File Data OK	⇨	Store received data to ESM	according to 3.4 (3.4 Data storage format)
	⇦	PSO: Compute Digital Signature	
Perform Security Operation „Compute Digital Signature“ using the temporarily stored Hash value			
Signature OK	⇨	Append data to the previous stored data on the ESM	according to 3.4 Data storage format)

3.3.4 Sequence for resetting the calibration counter.

DDP_039 The sequence to reset the NoOfCalibrationsSinceDownload counter in the EF Card_Download in a workshop card is the following:

Card	Dir	IDE / IFD	Meaning / Remarks
	⇦	Select File EF Card_Download	Select by File identifiers
OK	⇨		
	⇦	Update Binary NoOfCalibrationsSinceDownload = '00 00'	
resets card download number			
OK	⇨		

3.4 Data storage format

3.4.1 Introduction

DDP_040 The downloaded data has to be stored according to the following conditions:

- The data shall be stored transparent. This means that the order of the bytes as well as the order of the bits inside the byte that are transferred from the card has to be preserved during storage.
- All files of the card downloaded within a download session are stored in one file on the ESM.

3.4.2 File format

DDP_041 The file format is a concatenation of several TLV objects.

DDP_042 The tag for an EF shall be the FID plus the appendix „00".

DDP_043 The tag of an EF's signature shall be the FID of the file plus the appendix „01".

DDP_044 The length is a two byte value. The value defines the number of bytes in the value field. The value „FF FF" in the length field is reserved for future use.

DDP_045 When a file is not downloaded nothing related to the file shall be stored (no tag and no zero length).

DDP_046 A signature shall be stored as the next TLV object directly after the TLV object that contains the data of the file.

Definition	Meaning	Length
FID (2 Bytes) || „00"	Tag for EF (FID)	3 Bytes
FID (2 Bytes) || „01"	Tag for Signature of EF(FID)	3 Bytes
Xx xx	Length of Value field	2 Bytes

Example of data in a download file on an ESM:

Tag	Length	Value
00 02 00	00 11	Data of EF ICC
C1 00 00	00 C2	Data of EF Card_Certificate
		...
05 05 00	0A 2E	Data of EF Vehicles_Used
05 05 01	00 80	Signature of EF Vehicles_Used

4. Downloading a tachograph card via a vehicle unit.

DDP_047 The VU must allow for downloading the content of a driver card inserted to a connected IDE.

DDP_048 The IDE shall send a "Transfer Data Request Card Download" message to the VU to initiate this mode (see 2.2.2.9).

DDP_049 The VU shall then download the whole card, file by file, in accordance with the card downloading protocol defined in paragraph 0, and forward all data received from the card to the IDE within the appropriate TLV file format (see 3.4.2) and encapsulated within a "Positive Response Transfer Data" message.

DDP_050 The IDE shall retrieve card data from the "Positive Response Transfer Data" message (striping all headers, SIDs, TREPs, sub message counters, and checksums) and store them within one physical file as described in paragraph 2.3.

DDP_051 The VU shall then, as applicable, update the Control_Activity_Data or the Card_Download file of the driver card.

SUB-APPENDIX VIII

CALIBRATION PROTOCOL

CONTENTS

CONTENTS (continued)

PAGE

1. Introduction

This sub-appendix describes how data is exchanged between a vehicle unit and a tester via the K-line which forms part of the calibration interface described in sub-appendix 6. It also describes control of the input / output signal line on the calibration connector.

Establishing K-line communications is described in Section 4 "Communication Services".

This sub-appendix uses the idea of diagnostic "sessions" to determine the scope of K-line control under different conditions. The default session is the "StandardDiagnosticSession" where all data can be read from a vehicle unit but no data can be written to a vehicle unit.

Selection of the diagnostic session is described in Section 5 "Management Services"

CPR_001 The "ECUProgrammingSession" allows data entry into the vehicle unit. In the case of entry of calibration data (requirements 097 and 098), the vehicle unit must, in addition be in the CALIBRATION mode of operation.

Data transfer via K-line is described in Section 6 "Data Transmission Services". Formats of data transferred are detailed in Section 8 "dataRecords formats"

CPR_002 The "ECUAdjustmentSession" allows the selection of the I/O mode of the calibration I/O signal line via the K-line interface. Control of the calibration I/O signal line is described in section 7 "Control of Test Pulses – Input/Output Control functional unit".

CPR_003 Throughout this document the address of the tester is referred to as 'tt'. Although there may be preferred addresses for testers, the VU shall respond correctly to any tester address. The physical address of the VU is 0xEE.

2. Terms, Definitions and References

The protocols, messages and error codes are principally based on the current draft to date of ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1 : Diagnostic services, version 6 of 22 February 2001).

Byte encoding and hexadecimal values are used for the service identifiers, the service requests and responses, and the standard parameters.

The term 'tester' refers to the equipment used to enter programming/calibration data into the VU.

The terms 'client' and 'server' refer to the tester and the VU respectively.

The term ECU means "Electronic Control Unit" and refers to the VU.

References :

ISO 14230-2 Road Vehicles -Diagnostic Systems - Keyword Protocol 2000- Part 2 : Data Link Layer. First edition: 1999. Vehicles – Diagnostic Systems.

3. Overview of services

3.1 Services available

The following table provides an overview of the services that will be available in the control device and are defined in this document.

CPR_004 The table indicates the services that are available in an enabled diagnostic session.

- The **1st column** lists the services that are available.
- The **2nd column** includes the section number in this sub-appendix where of service is further defined.
- The **3rd column** assigns the assigns the service identifier values for request messages.
- The **4th column** specifies the services of the **"StandardDiagnosticSession" (SD)** which must be implemented in each VU.
- The **5th column** specifies the services of the **"ECUAdjustmentSession" (ECUAS)** which must be implemented to allow control of the I/O signal line in the front panel calibration connector of the VU.
- The **6th column** specifies the services of the **"ECUProgrammingSession" (ECUPS)** which must be implemented to allow for programming of parameters in the VU.

Table 1

Service Identifier value summary table

			Diagnostic Sessions		
Diagnostic Service Name	**Paragraphs No.**	**SId Req.Value**	**SD**	**ECUAS**	**ECUPS**
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ This symbol indicates that the service is mandatory in this diagnostic session.
No symbol indicates that this service is not allowed in this diagnostic session.

3.2 Response codes

Response codes are defined for each service.

4. Communication Services

Some services are necessary to establish and maintain communication. They do not appear on the application layer. The services available are detailed in the following table:

Table 2

Communication Services

Service name	Description
StartCommunication	The client requests to start a communication session with a server(s).
StopCommunication	The client requests to stop the current communication session.
TesterPresent	The client indicates to the server that it is still present.

CPR_005 The StartCommunication Service is used for starting a communication. In order to perform any service, communication must be initialised and the communication parameters need to be appropriate for the desired mode.

4.1 StartCommunication Service

CPR_006 Upon receiving a StartCommunication indication primitive, the VU shall check if the requested communication link can be initialised under the present conditions. Valid conditions for the initialisation of a communication link are described in document ISO 14230-2.

CPR_007 Then the VU shall perform all actions necessary to initialise the communication link and send a StartCommunication response primitive with the Positive Response parameters selected.

CPR_008 If a VU that is already initialised (and has entered any diagnostic session) receives a new StartCommunication Request (e.g. due to error recovery in the tester) the request shall be accepted and the VU shall be reinitialised.

CPR_009 If the communication link cannot be initialised for any reason, the VU shall continue operating as it was immediately prior to the attempt to initialise the communication link..

CPR_010 The StartCommunication Request message must be physically addressed.

CPR_011 Initialising the VU for services is performed through a 'fast initialisation' method,

- There is a bus-idle time prior to any activity.
- The tester then sends an initialisation pattern.
- All information which is necessary to establish communication is contained in the response of the VU.

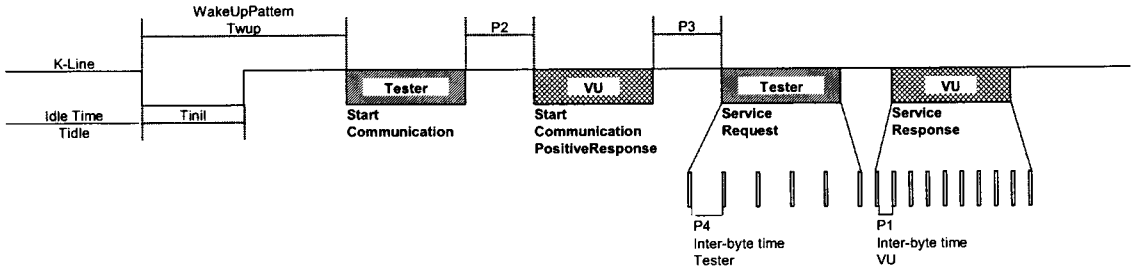
CPR_012 After completion of the initialisation,

All communication parameters are set to values defined in

- according to the key bytes.
- The VU is waiting for the first request of the tester.
- The VU is in the default diagnostic mode, i.e. StandardDiagnosticSession.
- The calibration I/O signal line is in the default state, i.e. disabled state.

CPR_014 The data rate on the K-line shall be 10 400 Baud.

CPR_016 The fast initialisation is started by the tester transmitting a Wake up pattern (Wup) on the K-line. The pattern begins after the idle time on K-line with a low time of Tinil. The tester transmits the first bit of the StartCommunication Service after a time of Twup following the first falling edge.



CPR_017 The timing values for the fast initialisation and communications in general are detailed in the tables below. There are different possibilities for the idle time :

- First transmission after power on, Tidle = 300ms.
- After completion of a StopCommunication Service, T_{idle} = P3 min.
- After stopping communication by time-out P3 max, T_{idle} = 0.

Table 3

Timing values for fast initialisation

Parameter		min value	max value
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Table 4

Communication timing values

Timing Parameter	Parameter Description	lower limit values [ms]	upper limit values [ms]
		min.	max.
P1	Inter byte time for VU response	0	20
P2	Time between tester request and VU response or two VU responses	25	250
P3	Time between end of VU responses and start of new tester request	55	5000
P4	Inter byte time for tester request	5	20

CPR_018 The message format for fast initialisation is detailed in the following tables.

Table 5

StartCommunication Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	81	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Checksum	00-FF	CS

Table 6

StartCommunication Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Key byte 1	EA	KB1
#7	Key byte 2	8F	KB2
#8	Checksum	00-FF	CS

CPR_019 There is no negative response to the StartCommunication Request message, if there is no positive response message to be transmitted then the VU is not initialised, nothing is transmitted and it remains in its normal operation.

4.2 StopCommunication Service

4.2.1 Message description

The purpose of this communication layer service is to terminate a communication session.

CPR_020 Upon receiving a StopCommunication indication primitive, the VU shall check if the current conditions allow to terminate this communication. In this case the VU shall perform all actions necessary to terminate this communication.

CPR_021 If it is possible to terminate the communication, the VU shall issue a StopCommunication response primitive with the Positive Response parameters selected, before the communication is terminated.

CPR_022 If the communication cannot be terminated by any reason, the VU shall issue a StopCommunication response primitive with the Negative Response parameter selected.

CPR_023 If time-out of P3max is detected by the VU, the communication shall be terminated without any response primitive being issued.

4.2.2 Message format

CPR_024 The message formats for the StopCommunication primitives are detailed in the following tables.

Table 7

StopCommunication Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Checksum	00-FF	CS

Table 8

StopCommunication Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Checksum	00-FF	CS

Table 9

StopCommunication Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Checksum	00-FF	CS

4.2.3 Parameter Definition

This service does not require any parameter definition.

4.3 TesterPresent Service

4.3.1 Message description

The TesterPresent service is used by the tester to indicate to the server that it is still present, in order to prevent the server from automatically returning to normal operation and possibly stopping the communication. This service, sent periodically, keeps the diagnostic session / communication active by resetting the P3 timer each time a request for this service is received.

4.3.2 Message format

CPR_079 The message formats for the TesterPresent primitives are detailed in the following tables.

Table 10

TesterPresent Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**
#6	Sub Function = responseRequired = [yes no]	01 02	RESPREQ_Y RESPREQ_NO
#7	Checksum	00-FF	CS

CPR_080 If the responseRequired parameter is set to 'yes', then the server shall respond with the following positive response message. If set to 'no', then no response is sent by the server.

Table 11

TesterPresent Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Checksum	00-FF	CS

CPR_081 The service shall support the following negative responses codes:

Table 12

TesterPresent Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP
#7	ResponseCode = [SubFunctionNotSupported- InvalidFormat incorrectMessageLength]	 12 13	 RC_SFNS_IF RC_IML
#8	Checksum	00-FF	CS

5. Management Services

The services available are detailed in the following table:

Table 13

Management Services

Service name	Description
StartDiagnosticSession	The client requests to start a diagnostic session with a VU.
SecurityAccess	The client requests access to functions restricted to authorised users.

5.1 StartDiagnosticSession service

5.1.1 Message description

CPR_025 The service StartDiagnosticSession is used to enable different diagnostic sessions in the server. A diagnostic session enables a specific set of services according to Table 17. A session can enable vehicle manufacturer specific services which are not part of this document. Implementation rules shall conform to the following requirements:

- There shall be always exactly one diagnostic session active in the VU,
- The VU shall always start the StandardDiagnosticSession when powered up. If no other diagnostic session is started, then the StandardDiagnosticSession shall be running as long as the VU is powered,
- If a diagnostic session which is already running has been requested by the tester, then the VU shall send a positive response message,

- Whenever the tester requests a new diagnostic session, the VU shall first send a StartDiagnosticSession positive response message before the new session becomes active in the VU. If the VU is not able to start the requested new diagnostic session, then it shall respond with a StartDiagnosticSession negative response message, and the current session shall continue.

CPR_026 A diagnostic session shall only be started if communication has been established between the client and the VU.

CPR_027 The timing parameters defined in

shall be active after a successful StartDiagnosticSession with the diagnosticSession parameter set to "StandardDiagnosticSession" in the request message if another diagnostic session was previously active.

5.1.2 Message format

CPR_028 The message formats for the StartDiagnosticSession primitives are detailed in the following tables.

Table 14
Management Services

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	02	LEN
#5	**StartDiagnosticSession Request Service Id**	10	STDS
#6	DiagnosticSession = [one value from Table 17]	xx	DS_...
#7	Checksum	00-FF	CS

Table 15
StartDiagnosticSession Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	DiagnosticSession = [same value as in byte #6 Table 14]	xx	DS_...
#7	Checksum	00-FF	CS

Table 16

StartDiagnosticSession Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	StartDiagnosticSession Request Service Id	10	STDS
#7	ResponseCode = [subFunctionNotSupported [a] incorrectMessageLength [b] conditionsNotCorrect [c]	12 13 22	RC_SFNS RC_IML RC_CNC
#8	Checksum	00-FF	CS

[a] – the value inserted in byte #6 of the request message is not supported, i.e. not in Table 17.
[b] – the length of the message is wrong,
[c] – the criteria for the request StartDiagnosticSession are not met.

5.1.3 Parameter definition

CPR_029 The parameter ***diagnosticSession (DS_)*** is used by the StartDiagnosticSession service to select the specific behaviour of the server(s). The following diagnostic sessions are specified in this document:

Table 17

Definition of diagnosticSession Values

Hex	Description	Mnemonic
81	StandardDiagnosticSession This diagnostic session enables all services specified in **Table 1, column 4 "SD"**. These services allow reading of data from a server (VU). This diagnostic Session is active after the initialisation has been successfully completed between client (tester) and server (VU). This diagnostic session may be overwritten by other diagnostic sessions specified in this section.	SD
85	ECUProgrammingSession This diagnostic session enables all services specified in **Table 1, column 6"ECUPS"**. These services support the memory programming of a server (VU) This diagnostic session may be overwritten by other diagnostic sessions specified in this section..	ECUPS
87	ECUAdjustmentSession This diagnostic session enables all services specified in **Table 1, column 5 "ECUAS"**. These services support the input/output control of a server (VU). This diagnostic session may be overwritten by other diagnostic sessions specified in this section.	ECUAS

5.2 SecurityAccess service

Writing of calibration data or access to the calibration input/output line is not possible unless the VU is in CALIBRATION mode. In addition to insertion of a valid workshop card into the VU, it is necessary to enter the appropriate PIN into the VU before access to the CALIBRATION mode is granted.

The SecurityAccess service provides a means to enter the PIN and to indicate to the tester whether or not the VU is in CALIBRATION mode.

It is acceptable that the PIN may be entered through alternative methods.

5.2.1 Message Description

The SecurityAccess service consists of a SecurityAccess "requestSeed" message, eventually followed by a SecurityAccess "sendKey" message. The SecurityAccess service must be carried out after the StartDiagnosticSession service.

CPR_033 The tester shall use the SecurityAccess "requestSeed" message to check if the vehicle unit is ready to accept a PIN.

CPR_034 If the vehicle unit is already in CALIBRATION mode, it shall answer the request by sending a "seed" of 0x0000 using the service SecurityAccess Positive Response.

CPR_035 If the vehicle unit is ready to accept a PIN for verification by a workshop card, it shall answer the request by sending a "seed" greater than 0x0000 using the service SecurityAccess Positive Response.

CPR_036 If the vehicle unit is not ready to accept a PIN from the tester, either because the workshop card inserted is not valid, or because no workshop card has been inserted, or because the vehicle unit expects the PIN from another method, it shall answer the request with a Negative Response with a response code set to conditionsNotCorrectOrRequestSequenceError.

CPR_037 The tester shall then, eventually, use the SecurityAccess "sendKey" message to forward a PIN to the Vehicle Unit. To allow time for the card authentication process to take place, the VU shall use the negative response code requestCorrectlyReceived-ResponsePending to extend the time to respond. However, the maximum time to respond shall not exceed 5 minutes. As soon as the requested service has been completed, the VU shall send a positive response message or negative response message with a response code different from this one. The negative response code requestCorrectlyReceived-ResponsePending may be repeated by the VU until the requested service is completed and the final response message is sent.

CPR_038 The vehicle unit shall answer to this request using the service SecurityAccess Positive Response only when in CALIBRATION mode.

CPR_039 In the following cases, the vehicle unit shall answer to this request with a Negative Response with a response code set to:

- subFunctionNot supported: Invalid format for the subfunction parameter (accessType),
- conditionsNotCorrectOrRequestSequenceError: Vehicle unit not ready to accept a PIN entry,
- invalidKey: PIN not valid and number of PIN checks attempts not exceeded,
- exceededNumberOfAttempts:PIN not valid and number of PIN checks attempts exceeded,
- generalReject: Correct PIN but mutual authentication with workshop card failed.

5.2.2 Message format - SecurityAccess - requestSeed

CPR_040 The message formats for the SecurityAccess "requestSeed" primitives are detailed in the following tables.

Table 18

SecurityAccess Request- requestSeed Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Checksum	00-FF	CS

Table 19

SecurityAccess - requestSeed Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Checksum	00-FF	CS

Table 20

SecurityAccess Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Checksum	00-FF	CS

5.2.3 Message format - SecurityAccess - sendKey

CPR_041 The message formats for the SecurityAccess "sendKey" primitives are detailed in the following tables.

Table 21

SecurityAccess Request - sendKey Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 to #m+6	Key #1 (High) … Key #m (low, m must be a minimum of 4, and a maximum of 8)	xx … xx	KEY
#m+7	Checksum	00-FF	CS

Table 22

SecurityAccess - sendKey Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Checksum	00-FF	CS

Table 23

SecurityAccess Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	ResponseCode = [generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequestSequenceError invalidKey exceededNumberOfAttempts requestCorrectlyReceived-ResponsePending]	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Checksum	00-FF	CS

6. Data Transmission Services

The services available are detailed in the following table:

Table 24

Data Transmission Services

Service name	Description
ReadDataByIdentifier	The client requests the transmission of the current value of a record with access by recordDataIdentifier.
WriteDataByIdentifier	The client requests to write a record accessed by recordDataIdentifier.

6.1 ReadDataByIdentifier service

6.1.1 Message description

CPR_050 The ReadDataByIdentifier service is used by the client to request data record values from a server. The data are identified by a recordDataIdentifier. It is the VU manufacturer's responsibility that the server conditions are met when performing this service.

6.1.2 Message format

CPR_051 The message formats for the ReadDataByIdentifier primitives are detailed in the following tables.

Table 25

ReadDataByIdentifier Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 to #7	recordDataIdentifier = [a value from Table 28]	xxxx	RDI_...
#8	Checksum	00-FF	CS

Table 26

ReadDataByIdentifier Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 and #7	recordDataIdentifier = [the same value as bytes #6 and #7 Table 25]	xxxx	RDI_...
#8 to #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Checksum	00-FF	CS

Table 27

ReadDataByIdentifier Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id	22	RDBI
#7	ResponseCode= [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Checksum	00-FF	CS

6.1.3 Parameter Definition

CPR_052 The parameter *recordDataIdentifier (RDI_)* in the ReadDataByIdentifier request message identifies a data record.

CPR_053 recordDataIdentifier values defined by this document are shown in the table below.

The recordDataIdentifier table consists of four columns and multiple lines.

- The 1st column (Hex) includes the "Hex Value" assigned to the recordDataIdentifier specified in the 3rd column.
- The 2nd column (Data element) specifies the data element of sub-appendix 1 on which the recordDataIdentifier is based (transcoding is sometimes necessary).
- The 3rd column (Description) specifies the corresponding recordDataIdentifier name.
- The 4th column (Mnemonic) specifies the mnemonic of this recordDataIdentifier.
-

Table 28

Definition of recordDataIdentifier values

Hex	Data element	recordDataIdentifier Name (see format in Section 8.2)	Mnemonic
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 The parameter ***dataRecord (DREC_)*** is used by the ReadDataByIdentifier positive response message to provide the data record value identified by the recordDataIdentifier to the client (tester). Data formats are specified in section 8. Additional user optional dataRecords including VU specific input, internal and output data may be implemented, but are not defined in this document.

6.2 WriteDataByIdentifier service

6.2.1 Message description

CPR_056 The WriteDataByIdentifier service is used by the client to write data record values to a server. The data are identified by a recordDataIdentifier. It is the VU manufacturer's responsibility that the server conditions are met when performing this service. To update the parameters listed in Table 28, the VU must be in CALIBRATION mode.

6.2.2 Message format

CPR_057 The message formats for the WriteDataByIdentifier primitives are detailed in the following tables.

Table 29

WriteDataByIdentifier Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 to #7	recordDataIdentifier = [a value from Table 28]	xxxx	RDI_...
#8 to m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Checksum	00-FF	CS

Table 30

WriteDataByIdentifier Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 to #7	recordDataIdentifier = [the same value as bytes #6 and #7 Table 29]	xxxx	RDI_...
#8	Checksum	00-FF	CS

Table 31

WriteDataByIdentifier Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI
#7	ResponseCode=[requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Checksum	00-FF	CS

6.2.3 Parameter definition

The parameter *recordDataIdentifier (RDI_)* is defined in Table 28.

The parameter *dataRecord (DREC_)* is used by the WriteDataByIdentifier request message to provide the data record values identified by the recordDataIdentifier to the server (VU). Data formats are specified in section 8.

7. Control of Test Pulses – Input/Output Control functional unit

The services available are detailed in the following table:

Table 32

InputOutputControlByIdentifier service

Service name	Description
InputOutputControlByIdentifier	The client requests the control of an input/output specific to the server.

7.1 InputOutputControlByIdentifier service

7.1.1 Message description

There is a connection via the front connector which allows test pulses to be controlled or monitored using a suitable tester.

CPR_058 This calibration I/O signal line can be configured by K-line command using the InputOutputControlByIdentifier service to select the required input or output function for the line. The available states of the line are:

- disabled,
- speedSignalInput, where the calibration I/O signal line is used to input a speed signal (test signal) replacing the motion sensor speed signal,
- realTimeSpeedSignalOutputSensor, where the calibration I/O signal line is used to output the speed signal of the motion sensor,
- RTCOutput, where the calibration I/O signal line is used to output the UTC clock signal.

CPR_059 The vehicle unit must have entered an adjustment session and must be in CALIBRATION mode to configure the state of the line. On exit of the adjustment session or of the CALIBRATION mode the vehicle unit must ensure the calibration I/O signal line is returned to the 'disabled' (default) state.

CPR_060 If speed pulses are received at the real time speed signal input line of the VU while the calibration I/O signal line is set to input then the calibration I/O signal line shall be set to output or returned to the disabled state.

CPR_061 The sequence shall be:

- Establish communications by StartCommunication Service
- Enter an adjustment session by StartDiagnosticSession Service and be in CALIBRATION mode of operation (the order of these two operation is not important).
- Change the state of the output by InputOutputControlByIdentifier Service.

7.1.2 Message format

CPR_062 The message formats for the InputOutputControlByIdentifier primitives are detailed in the following tables.

Table 33

InputOutputControlByIdentifier Request Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte - physical addressing	80	FMT
#2	Target address byte	EE	TGT
#3	Source address byte	tt	SRC
#4	Additional length byte	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 and #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 or #8 to #9	ControlOptionRecord = [inputOutputControlParameter - one value from Table 36 controlState – one value from Table 37 (see note below)]	 xx xx	COR_... IOCP_... CS_...
#9 or #10	Checksum	00-FF	CS

Note: The controlState parameter is present only in some cases (see 7.1.3).

Table 34

InputOutputControlByIdentifier Positive Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 and #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 or #8 to #9	controlStatusRecord = [inputOutputControlParameter (same value as byte #8 Table 33) controlState (same value as byte #9 Table 33)] (if applicable)	 xx xx	CSR_ IOCP_... CS_...
#9 or #10	Checksum	00-FF	CS

Table 35

InputOutputControlByIdentifier Negative Response Message

Byte #	Parameter Name	Hex Value	Mnemonic
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	 13 22 31 7A	 RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Checksum	00-FF	CS

7.1.3 Parameter definition

CPR_064 The parameter ***inputOutputControlParameter (IOCP_)*** is defined in the following table.

Table 36

Definition of inputOutputControlParameter values

Hex	Description	Mnemonic
00	**ReturnControlToECU** This value shall indicate to the server (VU) that the tester does no longer have control about the calibration I/O signal line.	RCTECU
01	**ResetToDefault** This value shall indicate to the server (VU) that it is requested to reset the calibration I/O signal line to its default state.	RTD
03	**ShortTermAdjustment** This value shall indicate to the server (VU) that it is requested to adjust the calibration I/O signal line to the value included in the controlState parameter.	STA

CPR_065 The parameter ***controlState*** is present only when the inputOutputControlParameter is set to ShortTermAdjustment and is defined in the following table:

Table 37

Definition of controlState values

Mode	Hex Value	Description
Disable	00	I/O line is disabled (default state)
Enable	01	Enable calibration I/O line as speedSignalInput
Enable	02	Enable calibration I/O line as realTimeSpeedSignalOutputSensor
Enable	03	Enable calibration I/O line as RTCOutput

8. dataRecords formats

This section details:

- general rules that shall be applied to ranges of parameters transmitted by the vehicle unit to the tester,
- formats that shall be used for data transferred via the Data Transmission Services described in section 6.

CPR_067 All parameters identified shall be supported by the VU.

CPR_068 Data transmitted by the VU to the tester in response to a request message shall be of the measured type (i.e. current value of the requested parameter as measured or observed by the VU).

8.1 Transmitted parameter ranges

CPR_069 Table 38 defines the ranges used to determine the validity of a transmitted parameter.

CPR_070 The values in the range «error indicator» provide a means for the vehicle unit to immediately indicate that valid parametric data is not currently available due to some type of error in the control device.

CPR_071 The values in the range «not available» provide a means for the vehicle unit to transmit a message which contains a parameter that is not available or not supported in that module. The values in the range «not requested» provide a means for a device to transmit a command message and identify those parameters where no response is expected from the receiving device.

CPR_072 If a component failure prevents the transmission of valid data for a parameter, the error indicator as described in Table 38 should be used in place of that parameter's data. However, if the measured or calculated data has yielded a value that is valid yet exceeds the defined parameter range, the error indicator should not be used. The data should be transmitted using the appropriate minimum or maximum parameter value.

Table 38

dataRecords ranges

Range Name	1 byte (Hex value)	2 bytes (Hex value)	4 bytes (Hex Value)	ASCII
Valid signal	00 to FA	0000 to FAFF	00000000 to FAFFFFFF	1 to 254
Parameter specific indicator	FB	FB00 to FBFF	FB000000 to FBFFFFFF	none
Reserved range for future indicator bits	FC to FD	FC00 to FDFF	FC000000 to FDFFFFFF	none
Error indicator	FE	FE00 to FEFF	FE000000 to FEFFFFFF	0
Not available or not requested	FF	FF00 to FFFF	FF000000 to FFFFFFFF	FF

CPR_073 For parameters coded in ASCII, the ASCII character "*" is reserved as a delimiter.

8.2 dataRecords formats

Tables 39 to 42 below detail the formats that shall be used via the ReadDataByIdentifier and WriteDataByIdentifier Services.

CPR_074 Table 39 provides the length, resolution and operating range for each parameter identified by its recordDataIdentifier:

Table 39

Format of dataRecords

Parameter Name	Data length (bytes)	Resolution	Operating range
TimeDate	8	*See details in Table 40*	
HighResolutionTotalVehicleDistance	4	5 m/bit gain, 0 m offset	0 to +21 055 406 km
Kfactor	2	0.001 pulse/m/bit gain, 0 offset	0 to 64.255 pulse/m
LfactorTyreCircumference	2	0.125 10^{-3} m /bit gain, 0 offset	0 to 8,031 m
WvehicleCharacteristicFactor	2	0.001 pulse/m/bit gain, 0 offset	0 to 64.255 pulse/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	*See details in Table 41*	
SpeedAuthorised	2	1/256 km/h/bit gain, 0 offset	0 to 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	*See details in Table 42*	
VIN	17	ASCII	ASCII

CPR_075 Table 40 details the formats of the different bytes of the TimeDate parameter :

Table 40

Detailed format of TimeDate (recordDataIdentifier value # F90B)

Byte	Parameter definition	Resolution	Operating range
1	Seconds	0.25 s/bit gain, 0 s offset	0 to 59.75s
2	Minutes	1 min/bit gain, 0 min offset	0 to 59 min
3	Hours	1 h/bit gain, 0 h offset	0 to 23 h
4	Month	1 month/bit gain, 0 month offset	1 to 12 month
5	Day	0.25 day/bit gain, 0 day offset (see NOTE below Table 41)	0.25 to 31.75 day
6	Year	1 year/bit gain, +1985 year offset (see NOTE below Table 41)	1985 to 2235 year
7	Local Minute Offset	1 min/bit gain, -125 min offset	-59 to +59 min
8	Local Hour Offset	1 h/bit gain, -125 h offset	- 23 to +23 h

CPR_076 Table 41 details the formats of the different bytes of the NextCalibrationDate parameter.

Table 41

Detailed format of NextCalibrationDate (recordDataIdentifier value # F922)

Byte	Parameter definition	Resolution	Operating range
1	Month	1 month/bit gain, 0 month offset	1 to 12 month
2	Day	0.25 day/bit gain, 0 day offset (see NOTE below)	0.25 to 31.75 day
3	Year	1 year/bit gain, +1985 year offset (see NOTE below)	1985 to 2235 year

NOTE concerning the use of the "Day" parameter:

A value of 0 for the date is null. The values 1, 2, 3, and 4 are used to identify the first day of the month; 5, 6, 7, and 8 identify the second day of the month; etc.

This parameter does not influence or change the hours parameter above.

NOTE concerning the use of byte "Year" parameter:
A value of 0 for the year identifies the year 1985; a value of 1 identifies 1986; etc.

CPR_078 Table 42 details the formats of the different bytes of the VehicleRegistrationNumber parameter:

Table 42

Detailed format of VehicleRegistrationNumber (recordDataIdentifier value # F97E)

Byte	Parameter definition	Resolution	Operating range
1	Code Page (as defined in sub-appendix 1)	ASCII	01 to 0A
2 – 14	Vehicle Registration Number (as defined in sub-appendix 1)	ASCII	ASCII

SUB-APPENDIX IX

TYPE APPROVAL

LIST OF MINIMUM REQUIRED TESTS

CONTENTS

1. Introduction

1.1 Type approval

The type approval procedure for the recording equipment (or component) or tachograph card is based on:

- a security certification, performed by an ITSEC authority, against a security target fully compliant with sub-appendix 10 to this appendix,

- a functional certification performed by a Contracting Party authority certifying that the item tested fulfils the requirements of this appendix in terms of functions performed, measurement accuracy and environmental characteristics,
- an interoperability certification performed by the competent body certifying that the control device(or tachograph card) is fully interoperable with the necessary tachograph card (or control device) models (see Chapter VIII of this appendix).

This sub-appendix specifies which tests, as a minimum, must be performed by a Contracting Party authority during the functional tests, and which tests, as a minimum, must be performed by the competent body during the interoperability tests. Procedures to follow to carry out the tests or the type of tests are not specified further.

The security certification aspects are not covered by this sub-appendix. If some tests requested for type approval are performed during the security evaluation and certification process, then these tests do not need to be performed again. In this case, only the results of these security tests may be inspected. For information, the requirements expected to be tested (or closely related to tests expected to be performed) during the security certification, are marked with a "*" in this sub-appendix.

This sub-appendix considers separately the type approval of the motion sensor and of the vehicle unit, as components of the control device. Interoperability between every model of motion sensor and every model of vehicle unit is not required, therefore the type approval for a motion sensor can be granted only in combination with the type approval of a vehicle unit and vice versa.

1.2 References

The following references are used in this sub-appendix:

IEC 68-2-1	Environmental testing - Part 2: Tests - Tests A: Cold. 1990 + Amendment 2: 1994.
IEC 68-2-2	Environmental testing - Part 2: Tests - Tests B: Dry heat. 1974 + Amendment 2: 1994.
IEC 68-2-6	Basic environmental testing procedures - Test methods - Test Fc and guidance: Vibration (sinusoidal). 6th edition: 1985.
IEC 68-2-14	Basic environmental testing procedures - Test methods - Test N: Change of temperature. Modification 1: 1986.
IEC 68-2-27	Basic environmental testing procedures - Test methods - Test Ea and guidance:Shock. Edition 3: 1987.

IEC 68-2-30 Basic environmental testing procedures - Test methods - Test Db and guidance: Damp heat, cyclic (12 + 12 - hour cycle). Modification 1: 1985.

IEC 68-2-35 Basic environmental testing procedure - Test methods - Test Fda: Random vibration wide band - Reproductibility High. Modification 1: 1983.

IEC 529 Degrees of protection provided by enclosures (IP code). Edition 2: 1989.

IEC 61000-4-2 Electromagnetic Compatibility (EMC) - Testing and measurement techniques - Electrostatic discharge immunity test: 1995 / Amendment 1: 1998

ISO 7637-1 Road vehicles - Electrical disturbance by conduction and coupling - Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage - Electrical transient conduction along supply lines only. Edition 2: 1990.

ISO 7637-2 Road vehicles - Electrical disturbance by conduction and coupling - Part 2: Commercial vehicles with nominal 24 V supply voltage - Electrical transient conduction along supply lines only. First edition: 1990.

ISO 7637-3 Road vehicles - Electrical disturbance by conduction and coupling - Part 3: Vehicles with 12 V or 24 V supply voltage - Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995.

ISO/IEC 7816-1 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics. First edition: 1998.

ISO/IEC 7816-2 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts. First edition: 1999.

ISO/IEC 7816-3 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocol. Edition 2: 1997.

ISO/IEC 10373 Identification cards - Test methods. First edition: 1993.

2. Vehicle unit functional tests

No	Test	Description	Related requirements
1	**Administrative examination**		
1.1	Documentation	Correctness of documentation	
1.2	Manufacturer test results	Results of manufacturer test performed during integration. Paper demonstrations.	070, 071, 073
2	**Visual inspection**		
2.1	Compliance with documentation		
2.2	Identification / markings		168, 169
2.3	Materials		163 to 167
2.4	Sealing		251

No	Test	Description	Related requirements
2.5	External interfaces		
3	**Functional tests**		
3.1	Functions provided		002, 004, 244
3.2	Modes of operation		006*, 007*, 008*, 009*, 106, 107
3.3	Functions and data access rights		010*, 011*, 240, 246, 247
3.4	Monitoring cards insertion and withdrawal		013, 014, 015*, 016*, 106
3.5	Speed and distance measurement		017 to 026
3.6	Time measurement (test performed at 20°C)		027 to 032
3.7	Monitoring driver activities		033 to 043, 106
3.8	Monitoring driving status		044, 045, 106
3.9	Manual entries		046 to 050b
3.10	Company locks management		051 to 055
3.11	Monitoring control activities		056, 057
3.12	Detection of events and/or faults		059 to 069, 106
3.13	Equipment identification data		075*, 076*, 079
3.14	Driver card insertion and withdrawal data		081* to 083*
3.15	Driver activity data		084* to 086*
3.16	Places data		087* to 089*
3.17	Odometer data		090* to 092*
3.18	Detailed speed data		093*
3.19	Events data		094*, 095
3.20	Faults data		096*
3.21	Calibration data		097*, 098*
3.22	Time adjustment data		100*, 101*
3.23	Control activity data		102*, 103*
3.24	Company locks data		104*
3.25	Download activity data		105*
3.26	Specific conditions data		105a*, 105b*
3.27	Recording and storing on tachographs cards		108, 109*, 109a*, 110*, 111, 112
3.28	Displaying		072, 106, 113 to 128, PIC_001, DIS_001

No	Test	Description	Related requirements
3.29	Printing		072, 106, 129 to 138, PIC_001, PRT_001 to PRT_012
3.30	Warning		106, 139 to 148, PIC_001
3.31	Data downloading to external media		072, 106, 149 to 151
3.32	Output data to additional external devices		152, 153
3.33	Calibration		154*, 155*, 156*, 245
3.34	Time adjustment		157*, 158*
3.35	Non-interference of additional functions		003, 269
4	**Environmental tests**		
4.1	Temperature	Verify functionality through: - IEC 68-2-1, test Ad, with a test duration of 72 hours at the lower temperature (-20°C), 1 hour operating, 1 hour non operating, - IEC 68-2-2, test Bd, with a test duration of 72 hours at the higher temperature (+70°C), 1 hour operating, 1 hour non operating Temperature cycles: verify that the vehicle unit can withstand rapid changes in the environment temperature through IEC 68-2-14 test Na, 20 cycles, each with temperature varying from the lower temperature (-20°C) to the higher temperature (+70°C) and a 2 hours stay at both the lower and the higher temperature A reduced set of tests (among those defined in section 3 of this table) can be carried out at the lower temperature, the higher temperature and during the temperature cycles	159
4.2	Humidity	Verify that the vehicle unit can withstand a cyclic damp (heat test) through IEC 68-2-30, test Db, six 24 hours cycles, each temperature varying from +25°C to + 55°C and a relative humidity of 97% at + 25°C and equal to 93% at +55°C	160

No	Test	Description	Related requirements
4.3	Vibration	1. Sinusoidal vibrations. verify that the vehicle unit can withstand sinusoidal vibrations with the following characteristics: constant displacement between 5 and 11 Hz: 10mm peak constant acceleration between 11 and 300 Hz: 5g This requirement is verified through IEC 68-2-6, test Fc, with a minimum test duration of 3x12 hours (12 hours per axis) 2. Random vibrations: verify that the vehicle unit can withstand random vibrations with the following characteristics: frequency 5-150 Hz, level $0.02g^2/Hz$ This requirement is verified through IEC 68-2-35, test Ffda, with a minimum test duration of 3x12 hours (12 hours per axis), 1hour operating, 1 hour non operating The two tests described above are performed on two different samples of the equipment type being tested.	163
4.4	Protection against water and foreign bodies	Verify that the vehicle unit protection index according to IEC 529 is at least IP 40, when mounted in operating conditions in a vehicle	164, 165
4.5	Over-voltage protection	Verify that the vehicle unit can withstand a power supply of: 24 V versions: 34V at +40°C 1 hour 12 V versions: 17V at +40°C 1 hour	161
4.6	Reverse polarity protection	Verify that the vehicle unit can withstand an inversion of its power supply	161
4.7	Short-circuit protection	Verify that input output signals are protected against short circuits to power supply and ground	161
5	**EMC tests**		
5.1	Radiated emissions and susceptibility	Compliance with ECE Regulation N°10.	162

No	Test	Description	Related requirements
5.2	Electrostatic discharge	Compliance with IEC 61000-4-2, ±2kV (level 1)	162
5.3	Conducted transient susceptibility on power supply	For 24V versions: compliance with ISO 7637-2: pulse 1a: Vs=-100V, Ri=10 ohms pulse 2: Vs=+100V, Ri=10 ohms pulse 3a: Vs=-100V, Ri=50 ohms pulse 3b: Vs=+100V, Ri=50 ohms pulse 4: Vs= - 16V Va=-12V, t6=100ms pulse 5: Vs=+120V, Ri=2,2 ohms, td=250ms For 12V versions: compliance with ISO 7637-1: pulse 1: Vs=-100V, Ri=10 ohms pulse 2: Vs=+100V, Ri=10 ohms pulse 3a: Vs=-100V, Ri=50 ohms pulse 3b: Vs=+100V, Ri=50 ohms pulse 4: Vs=-6V Va=-5V, t6=15ms pulse 5: Vs=+65V, Ri=3 ohms, td=100ms Pulse 5 shall be tested only for vehicle units designed to be installed in vehicles for which no external common protection against load dump is implemented	162

3 Motion sensor functional tests

No	Test	Description	Related requirements
1.	**Administrative examination**		
1.1	Documentation	Correctness of documentation	
2.	**Visual inspection**		
2.1.	Compliance with documentation		
2.2.	Identification / markings		169, 170
2.3	Materials		163 to 167
2.4.	Sealing		251
3.	**Functional tests**		
3.1	Sensor identification data		077*
3.2	Motion sensor – vehicle unit pairing		099*, 155
3.3	Motion detection Motion measurement accuracy		022 to 026
4.	**Environmental tests**		
4.1	Operating temperature	Verify functionality (as defined in test No 3.3) in temperature range [–40°C; +135°C] through: - IEC 68-2-1 test Ad, with a test duration of 96 hours at the lowest temperature To_{min}, - IEC 68-2-2 test Bd, with a test duration of 96 hours at the highest temperature To_{max}	159
4.2	Temperature cycles	Verify functionality (as defined in test No 3.3) through IEC 68-2-14 test Na, 20 cycles, each with temperature varying from the lower temperature (-40°C) to the higher temperature (+135°C) and a 2 hours stay at both the lower and the higher temperature. A reduced set of tests (among those defined in test 3.3) can be carried out at the lower temperature, the higher temperature and during the temperature cycles	159

4.3	Humidity cycles	Verify functionality (as defined in test No. 3.3) through IEC 68-2-30, test Db, six 24 hours cycles, each temperature varying from +25°C to + 55°C and a relative humidity of 97% at + 25°C and equal to 93% at +55°C	160
4.4	Vibration	Verify functionality (as defined in test No. 3.3) through IEC 68-2-6, test Fc, with a test duration of 100 frequency cycles: constant displacement between 10 and 57 Hz: 1,5 mm peak constant accelaration between 57 and 500 Hz: 20g	163
4.5	Mechanical shock	Verify functionality (as defined in test No. 3.3) through IEC 68-2-27, test Ea, 3 shocks in both directions of the 3 perpendicular axes	163
4.6	Protection against water and foreign bodies	Verify that the motion sensor protection index according to IEC 529 is at least IP 64, when mounted in operating conditions in a vehicle	165
4.7	Reverse polarity protection	Verify that the motion sensor can withstand an inversion of its power supply	161
4.8	Short circuit protection	Verify that input output signals are protected against short circuits to power supply and ground	161
5.	**EMC**		
5.1	radiated emissions and susceptibility	Verify compliance with ECE Regulation N°10.	162
5.2	Electrostatic discharge	Compliance with IEC 61000-4-2, ±2kV (level 1)	162
5.3	Conducted transient susceptibility on data lines)	Compliance with ISO7637-3 (level III)	162

4. Tachograph cards functional tests

No	Test	Description	Related requirements
1.	**Administrative examination**		
1.1	Documentation	Correctness of documentation	
2	**Visual inspection**		
2.1		Make sure that all features for protection and visible data are correctly printed on the card and compliant	171 to 181
3	**Physical tests**		
3.1		Check dimension of the card and location of the contacts	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4	**Protocol tests**		
4.1	ATR	Check that the ATR is compliant	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Check that T=0 protocol is compliant	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS	Check that the PTS command is compliant by setting T=1 from T=0.	ISO/IEC 7816-3 TCS 309 to 311
4.4	T=1	Check that T=1 protocol is compliant	ISO/IEC 7816-3 TCS 303, / 306
5	**Card structure**		
5.1		Test that the file structure of the card is compliant by checking the presence of the mandatory files in the card and their access conditions	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419

6	**Functional tests**		
6.1	Normal processing	Test at least once each allowed usage of each command (ex: test the UPDATE BINARY command with CLA = '00', CLA = '0C' and with different P1,P2 and Lc parameters) Check that the operations have actually been performed in the card (ex: by reading the file the command has been performed on)	TCS 313 to TCS 379
6.2	Error messages	Test at least once each error message (as specified in sub-appendix 2) for each command Test at least once every generic error (except '**6400**' integrity errors checked during security certification)	
7	**Environmental tests**		
7.1		Make sure that the cards work within the limit conditions defined in accordance with ISO/IEC 10373.	185 to 188 ISO/IEC 7816-1

5. Interoperability tests

No	Test	Description
1	Mutual authentication	Check that the mutual authentication between the vehicle unit and the tachograph card runs normally
2	Write/read tests	Execute a typical activity scenario on the vehicle unit. The scenario shall be adapted to the type of card being tested and involve writings in as many EFs as possible in the card Verify through a card downloading that all corresponding recordings have been properly made Verify through a card daily printout that all corresponding recordings can be properly read

SUB-APPENDIX X

GENERIC SECURITY TARGETS

CONTENTS

CONTENTS (continued)

PAGE

CONTENTS (continued)

PAGE

CONTENTS (continued)

Note concerning this sub-appendix

This sub-appendix specifies the minimum required content of motion sensor, vehicle unit and tachograph card security targets.

In order to form the security targets against which they may seek security certification, manufacturers shall refine and complete the documents as necessary, without amending nor deleting existing threats, objectives, procedural means and security enforcing functions specifications.

MOTION SENSOR GENERIC SECURITY TARGET

1. Introduction

This document contains a description of the motion sensor, of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

Requirements referred to in the document, are those of the body of Appendix 1B. For clarity of reading, duplication sometimes arises between Appendix 1B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Appendix 1B body requirement referred by this security target requirement, the Appendix 1B body requirement shall prevail.

Appendix 1B body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

2. Abbreviations, definitions and references

2.1 Abbreviations

ROM Read Only Memory

SEF Security Enforcing Function

TBD To Be Defined

TOE Target Of Evaluation

VU Vehicle Unit

2.2 Definitions

Digital Tachograph	Control device
Entity	A device connected to the motion sensor.
Motion data	The data exchanged with the VU, representative of speed and distance travelled.
Physically separated parts.	Physical components of the motion sensor that are distributed in the vehicle as opposed to physical components gathered into the motion sensor casing.

Security data	The specific data needed to support security enforcing functions (e.g. crypto keys).
System	Equipment, people or organisations, involved in any way with the control device.
User	A human user of the motion sensor (when not used in the expression "user data").
User data	Any data, other than motion or security data, recorded or stored by the motion sensor.

2.3 References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.

3. Product rationale

3.1 Motion sensor description and method of use

The motion sensor is intended to be installed in road transport vehicles. Its purpose is to provide a VU with secured motion data representative of vehicle's speed and distance travelled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement can be representative of vehicle's speed or distance travelled. It may be located in the vehicle's gear box or in any other part of the vehicle.

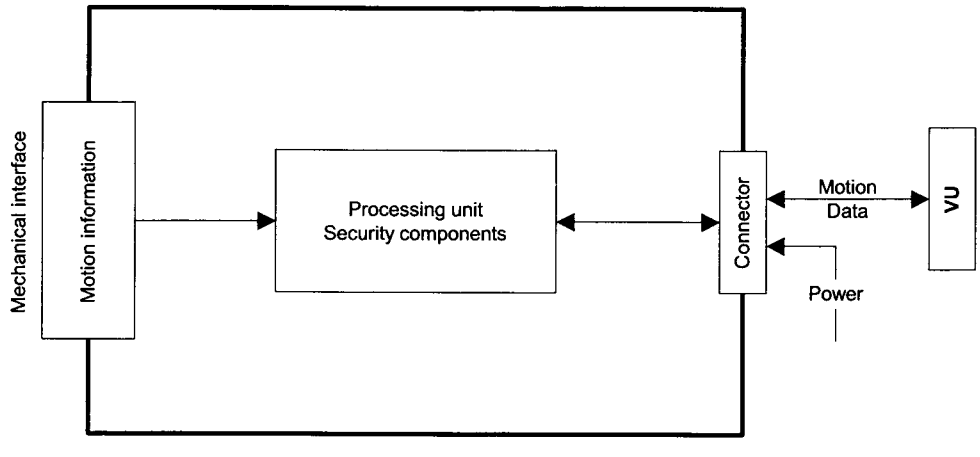
In its operational mode, the motion sensor is connected to a VU.

It may also be connected to specific equipment for management purposes (*TBD by manufacturer*)

The typical motion sensor is described in the following figure:

Figure 1

Typical motion sensor

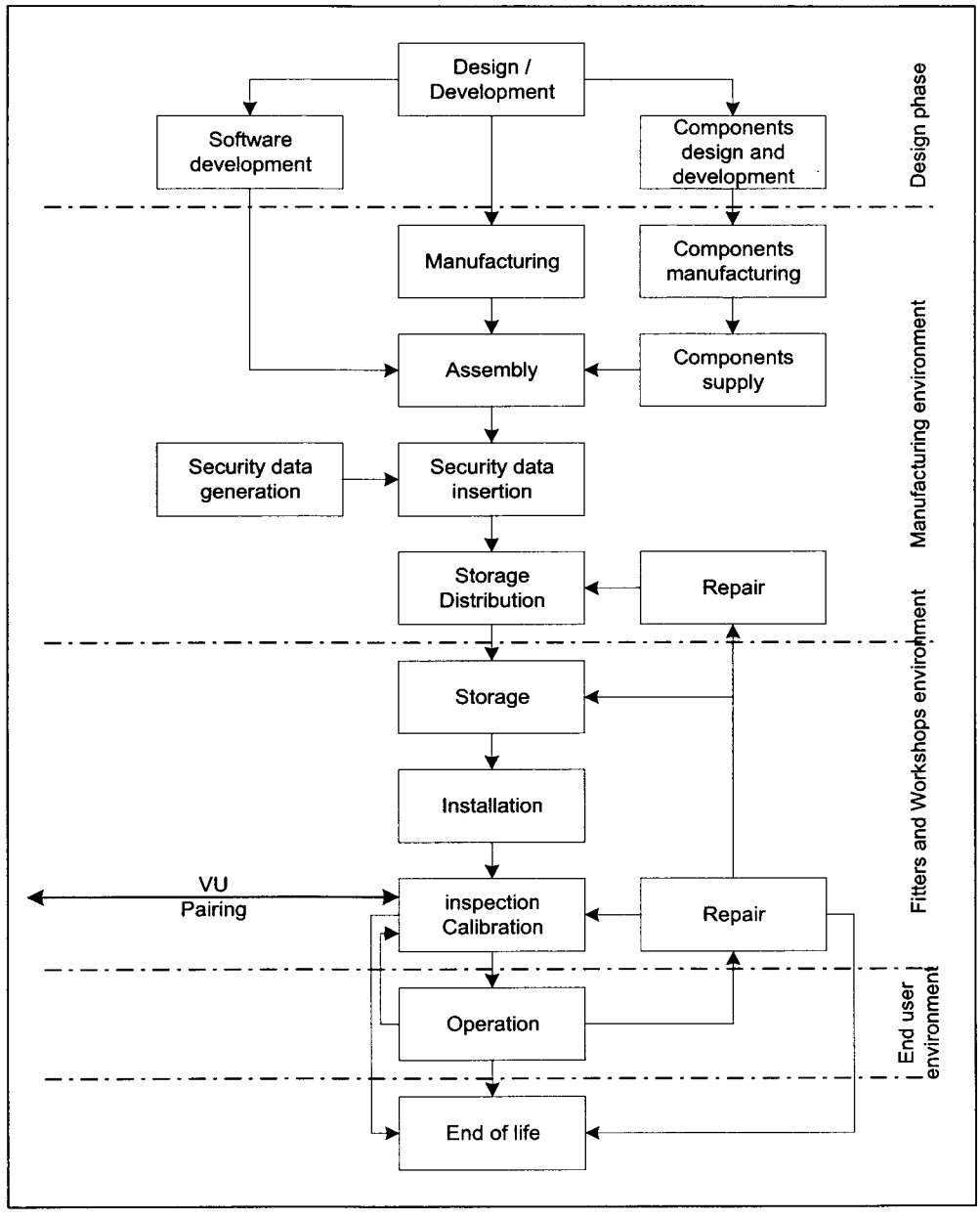


3.2 Motion sensor life cycle

The typical life cycle of the motion sensor is described in the following figure:

Figure 2

Motion sensor typical life cycle



3.3 Threats

This paragraph describes the threats the motion sensor may face.

3.3.1 Threats to access control policies

T.Access	Users could try to access functions not allowed to them.

3.3.2 Design related threats

T.Faults	Faults in hardware, software, communication procedures could place the motion sensor in unforeseen conditions compromising its security.
T.Tests	The use of non invalidated test modes or of existing back doors could compromise the motion sensor security.
T.Design	Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, ...) or from reverse engineering.

3.3.3 Operation oriented threats

T.Environment	Users could compromise the motion sensor security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,...).
T.Hardware	Users could try to modify motion sensor hardware.
T.Mechanical_Origin	Users could try to manipulate the motion sensor input (e.g. unscrewing from gearbox, ...).
T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).
T.Power_Supply	Users could try to defeat the motion sensor security objectives by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify motion sensor software.
T.Stored_Data	Users could try to modify stored data (security or user data).

3.4 Security objectives

The main security objective of the digital tachograph system is the following:

O.Main	The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

Therefore the security objective of the motion sensor, contributing to the global security objective, is:

O.Sensor_Main	The data transmitted by the motion sensor must be available to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance travelled.

3.5 Information Technology Security Objectives

The specific IT security objectives of the motion sensor contributing to its main security objective, are the following:

O.Access	The motion sensor must control connected entities' access to functions and data.
O.Audit	The motion sensor must audit attempts to undermine its security and should trace them to associated entities.
O.Authentication	The motion sensor must authenticate connected entities.
O.Processing	The motion sensor must ensure that processing of input to derive motion data is accurate.
O.Reliability	The motion sensor must provide a reliable service.
O.Secured_Data_Exchange	The motion sensor must secure data exchanges with the VU.

3.6 Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the motion sensor.

3.6.1 Equipment design

M.Development	Motion sensor developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
M.Manufacturing	Motion sensor manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the motion sensor is protected from physical attacks which might compromise IT security.

3.6.2 Equipment delivery

M.Delivery	Motion sensor manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor is done in a manner which maintains IT security.

3.6.3 Security data generation and delivery

M.Sec_Data_Generation	Security data generation algorithms must be accessible to authorised and trusted persons only.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the motion sensor, in such a way to preserve its appropriate confidentiality and integrity.

3.6.4 Control device installation, calibration, and inspection

M.Approved_Workshops Installation, calibration and repair of control device must be carried by trusted and approved fitters or workshops.

M.Mechanical_Interface Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)

M.Regular_Inpections Control device must be periodically inspected and calibrated.

3.6.5 Law enforcement control

M.Controls Law enforcement controls must be performed regularly and randomly, and must include security audits.

3.6.6 Software upgrades

M.Software_Upgrade Software revisions must be granted security certification before they can be implemented in a motion sensor.

4. Security enforcing functions

4.1 Identification and authentication

UIA_101 The motion sensor shall be able to establish, for every interaction, the identity of any entity it is connected to.

UIA_102 The identity of a connected entity shall consist of:

- an entity group:
  - VU,
  - Management device,
  - Other,
- an entity ID (VU only).

UIA_103 The entity ID of a connected VU shall consist of the VU approval number and the VU serial number.

UIA_104 The motion sensor shall be able to authenticate any VU or management device it is connected to:

- at entity connection,
- at power supply recovery

UIA_105 The motion sensor shall be able to periodically re-authenticate the VU it is connected to.

UIA_106 The motion sensor shall detect and prevent use of authentication data that has been copied and replayed.

UIA_107 After (*TBD by manufacturer and not more than 20*) consecutive unsuccessful authentication attempts have been detected, the SEF shall:

- generate an audit record of the event,
- warn the entity,
- continue to export motion data in a non secured mode.

4.2 Access control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

4.2.1 Access control policy

ACC_101 The motion sensor shall control access rights to function and data.

4.2.2 Data access rights

ACC_102 The motion sensor shall ensure that motion sensor identification data can be written once only (requirement 078).

ACC_103 The motion sensor shall accept and/or store user data from authenticated entities only.

ACC_104 The motion sensor shall enforce appropriate read and write access rights to security data.

4.2.3 File structure and access conditions

ACC_105 Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

4.3 Accountability

ACT_101 The motion sensor shall hold in its memory motion sensor identification data (requirement 077).

ACT_102 The motion sensor shall store in its memory installation data (requirement 099).

ACT_103 The motion sensor shall have a capability to output accountability data to authenticated entities at their request.

4.4 Audit

AUD_101 The motion sensor shall, for events impairing its security, generate audit records of the events.

AUD_102 The events affecting the security of the motion sensor are the following:

- security breach attempts:
  - authentication failure,
  - stored data integrity error,
  - internal data transfer error,
  - unauthorised case opening,
  - hardware sabotage.
- Sensor fault,

AUD_103 Audit records shall include the following data:

- date and time of the event,
- type of event,
- connected entity identity.

when required data is not available, an appropriate default indication shall be given (*TBD by manufacturer*).

AUD_104 The motion sensor shall send the generated audit records to the VU at the moment of their generation, and may also store them in its memory.

AUD_105 In the case where the motion sensor stores audit records, it shall ensure that 20 audit records will be maintained independent of audit storage exhaustion, and shall have a capability to output stored audit records to authenticated entities at their request.

4.5 Accuracy

4.5.1 Information flow control policy

ACR_101 The motion sensor shall ensure that motion data may only been processed and derived from sensor mechanical input.

4.5.2 Internal data transfers

The requirements of this paragraph apply only if the motion sensor makes use of physically separated parts.

ACR_102 If data are transferred between physically separated parts of the motion sensor, the data shall be protected from modification.

ACR_103 Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

4.5.3 Stored data integrity

ACR_104 The motion sensor shall check user data stored in its memory for integrity errors.

ACR_105 Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

4.6 Reliability of service

4.6.1 Tests

RLB_101 All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase. It shall not be possible to restore them for later use.

RLB_102 The motion sensor shall run self-tests, during initial start-up, and during normal operation to verify its correct operation. The motion sensor self-tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).

RLB_103 Upon detection of an internal fault during self-test, the SEF shall generate an audit record (sensor fault).

4.6.2 Software

RLB_104 There shall be no way to analyse or debug the motion sensor software in the field.

RLB_105 Inputs from external sources shall not be accepted as executable code.

4.6.3 Physical protection

RLB_106 If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of 6 months. In such a case, the SEF shall generate an audit record of the event (It is acceptable that the audit record is generated and stored after power supply reconnection).

If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).

RLB_107 The motion sensor shall detect specified (*TBD by manufacturer*) hardware sabotage.

RLB_108 In the case described above, the SEF shall generate an audit record and the motion sensor shall: (*TBD by manufacturer*).

4.6.4 Power supply interruptions

RLB_109 The motion sensor shall preserve a secure state during power supply cut-off or variations.

4.6.5 Reset conditions

RLB_110 In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the motion sensor shall be reset cleanly.

4.6.6 Data availability

RLB_111 The motion sensor shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

4.6.7 Multiple applications

RLB_112 If the motion sensor provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.

4.7 Data exchange

DEX_101 The motion sensor shall export motion data to the VU with associated security attributes, such that the VU will be able to verify its integrity and authenticity.

4.8 Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions.

CSP_101 Any cryptographic operation performed by the motion sensor shall be in accordance with a specified algorithm and a specified key size.

CSP_102 If the motion sensor generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes.

CSP_103 If the motion sensor distributes cryptographic keys, it shall be in accordance with specified key distribution methods.

CSP_104 If the motion sensor accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.

CSP_105 If the motion sensor destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.

5. Definition of security mechanisms

The security mechanisms, fulfilling the motion sensor security enforcing functions, are defined by the motion sensor manufacturers.

6. Minimum strength of security mechanisms

The minimum strength of the motion sensor security mechanisms is **High,** as defined in [ITSEC].

7. Level of assurance

The target level of assurance for the motion sensor is ITSEC level **E3**, as defined in [ITSEC].

8. Rationale

The following matrixes give a rationale for the SEFs by showing:
- which SEFs or means counteract which threats,
- which SEFs fulfil which IT security objectives.

	Threats												IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
Physical Personnel Procedural means																		
Development		x	x	x														
Manufacturing			x	x														
Delivery						x					x	x						
Security Data Generation										x								
Security Data Transport										x								
Approved Workshops							x											
Mechanical interface							x											
Regular Inspection						x	x		x		x							
Law enforcement controls					x	x	x		x	x	x							
Software Upgrades											x							
Security Enforcing Functions																		
Identification and authentication																		
UIA_101 Entities identification	x							x					x		x			x
UIA_102 Entities identity	x												x		x			
UIA_103 VU identity														x				

	Threats												IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
UIA_104 Entities authentication	x							x					x		x			x
UIA_105 re-authentication	x							x					x		x			x
UIA_106 Unforgeable authentication	x							x					x		x			
UIA_107 Authentication failure								x						x			x	
Access control																		
ACC_101 Access control policy	x									x		x	x					
ACC_102 Motion sensor ID												x	x					
ACC_103 User data												x	x					
ACC_104 Security Data										x		x	x					
ACC_105 File structure and access conditions	x									x		x	x					
Accountability																		
ACT_101 Motion sensor ID data														x				
ACT_102 Pairing data														x				
ACT_103 Accountability data														x				
Audit																		
AUD_101 Audit records														x				
AUD_102 Audit events list	x				x	x						x		x				
AUD_103 Audit data														x				
AUD_104 Audit tools														x				
AUD_105 Audit records storage														x				

	Threats												IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
Accuracy																		
ACR_101 Information flow control policy								x								x	x	
ACR_102 Internal transfers																x	x	
ACR_103 Internal transfers														x				
ACR_104 Stored data integrity												x					x	
ACR_105 Stored data integrity												x		x				
Reliability																		
RLB_101 Manufacturing tests			x	x													x	
RLB_102 Self tests		x				x			x		x						x	
RLB_103 Self tests						x			x		x			x				
RLB_104 Software analysis				x							x						x	
RLB_105 Software input											x					x	x	
RLB_106 Case opening				x	x	x				x	x	x					x	
RLB_107 Hardware sabotage						x											x	
RLB_108 Hardware sabotage						x								x				
RLB_109 Power supply interruptions									x								x	
RLB_110 Reset		x															x	
RLB_111 Data Availability																x	x	
RLB_112 Multiple Applications																	x	
Data exchange																		
DEX_101 Secured motion data export								x										x

	Threats												IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
Cryptographic support																		
CSP_101 Algorithms																	x	x
CSP_102 key generation																	x	x
CSP_103 key distribution																	x	x
CSP_104 key access																	x	x
CSP_105 key destruction																	x	x

VEHICLE UNIT GENERIC SECURITY TARGET

1. Introduction

This document contains a description of the vehicle unit, of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

Requirements referred to in the document, are those of the body of Appendix 1B. For clarity of reading, duplication sometimes arises between Appendix 1B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Appendix 1B body requirement referred by this security target requirement, the Appendix 1B body requirement shall prevail.

Appendix 1B body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

2. Abbreviations, definitions and references

2.1 Abbreviations

PIN Personal Identification Number

ROM Read Only Memory

SEF Security Enforcing Function

TBD To Be Defined

TOE Target Of Evaluation

VU Vehicle Unit

2.2 Definitions

Digital tachograph	Control device.
Motion data	The data exchanged with the motion sensor, representative of speed and distance travelled.
Physically separated parts.	Physical components of the VU that are distributed in the vehicle as opposed to physical components gathered into the VU casing.
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys).
System	Equipment, people or organisations, involved in any way with the control device.
User	Users are to be understood as human user of the equipment. Normal users of the VU comprise drivers, controllers, workshops and companies.
User data	Any data, other than security data, recorded or stored by the VU, required by Chapter III.12.

2.3 References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.

3. Product rationale

3.1 Vehicle Unit description and method of use

The VU is intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities.

It is connected to a motion sensor with which it exchanges vehicle's motion data.

Users identify themselves to the VU using tachograph cards.

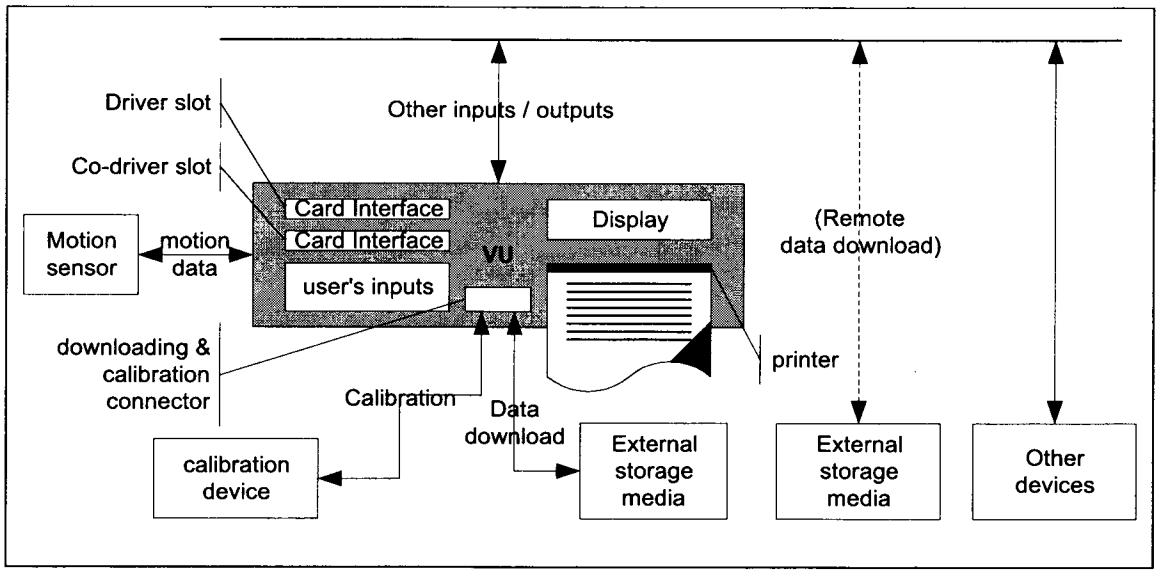
The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards.

The VU outputs data to display, printer and external devices.

The vehicle unit's operational environment while installed in a vehicle is described in the following figure:

Figure 1

VU operational environment



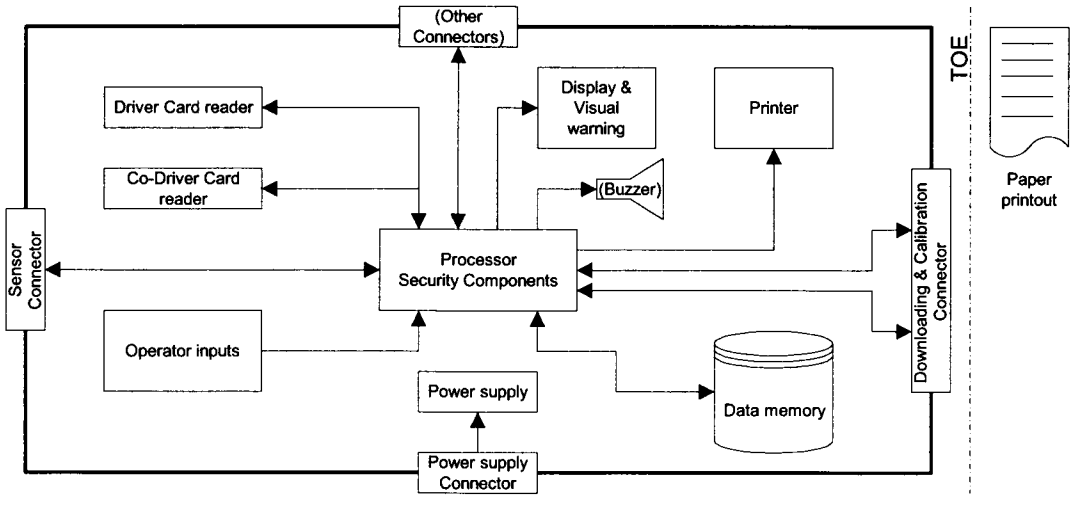
The VU general characteristics, functions and mode of operations are described in Chapter II of Appendix 1B.

The VU functional requirements are specified in Chapter III of Appendix 1B.

The typical VU is described in the following figure:

Figure 2

Typical VU (...) optional



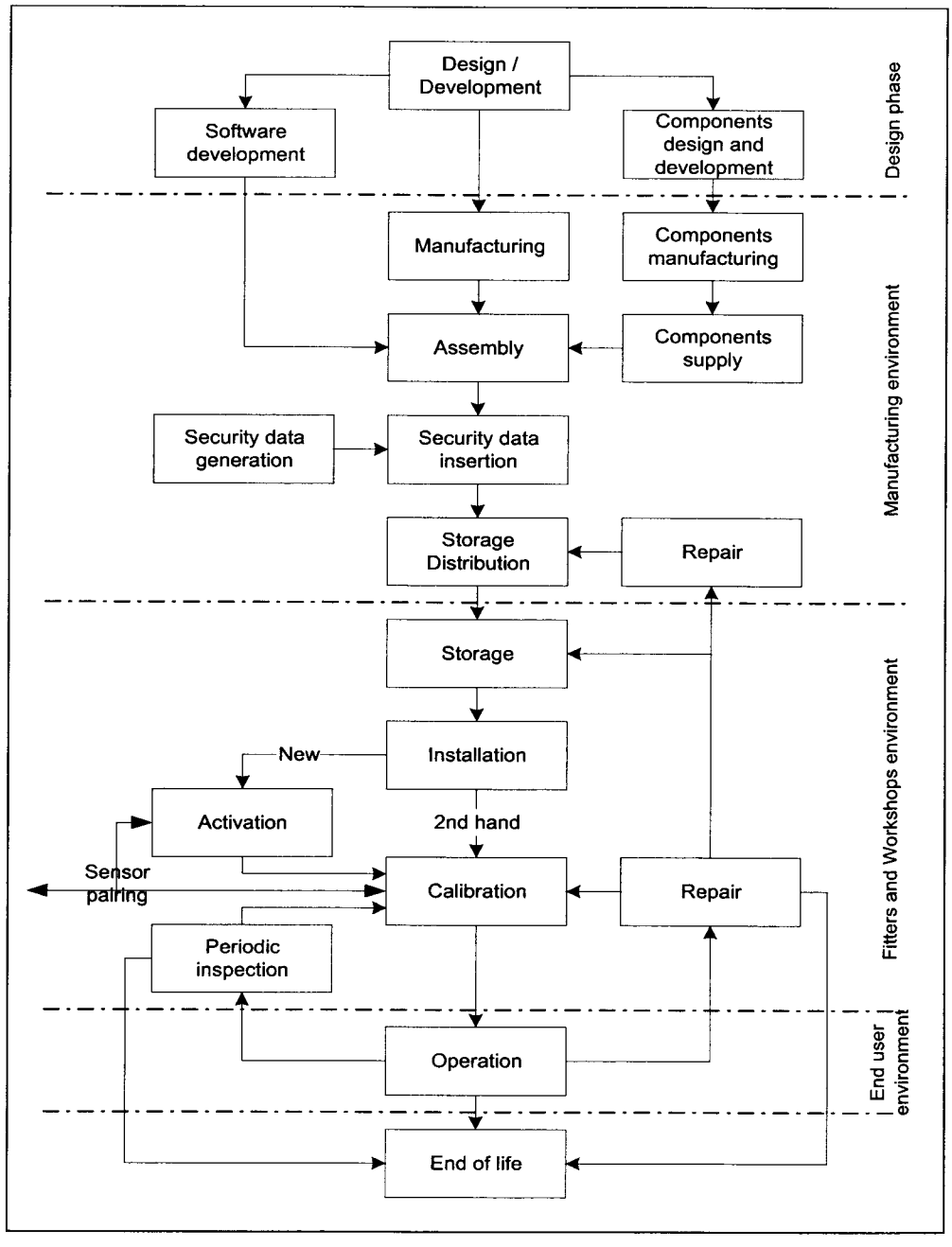
It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

3.2 Vehicle Unit life cycle

The typical life cycle of the VU is described in the following figure:

Figure 3

VU typical life cycle



3.3 Threats

This paragraph describes the threats the VU may face.

3.3.1 Threats to identification and access control policies

T.Access	Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function).
T.Identification	Users could try to use several identifications or no identification.

3.3.2 Design related threats

T.Faults	Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.
T.Tests	The use of non invalidated test modes or of existing back doors could compromise the VU security.
T.Design	Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, ...) or from reverse engineering.

3.3.3 Operation oriented threats

T.Calibration_Parameters	Users could try to use mis-calibrated equipment (through calibration data modification, or through organisational weaknesses).
T.Card_Data_Exchange	Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).
T.Clock	Users could try to modify internal clock.
T.Environment	Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,...).
T.Fake_Devices	Users could try to connect fake devices (motion sensor, smart cards) to the VU.
T.Hardware	Users could try to modify VU hardware.
T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).
T.Non_Activated	Users could use non activated equipment.
T.Output_Data	Users could try to modify data output (print, display or download).
T.Power_Supply	Users could try to defeat the VU security objectives by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify VU software.
T.Stored_Data	Users could try to modify stored data (security or user data).

3.4 Security objectives

The main security objective of the digital tachograph system is the following:

O.Main	The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

Therefore the security objectives of the VU, contributing to the global security objective, are the following:

O.VU_Main	The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.
O.VU_Export	The VU must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity.

3.5 Information Technology Security Objectives

The specific IT security objectives of the VU contributing to its main security objectives, are the following:

O.Access	The VU must control user access to functions and data.
O.Accountability	The VU must collect accurate accountability data.
O.Audit	The VU must audit attempts to undermine system security and should trace them to associated users.
O.Authentication	The VU should authenticate users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The VU must maintain stored data integrity.
O.Ouput	The VU must ensure that data output reflects accurately data measured or stored.
O.Processing	The VU must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The VU must provide a reliable service.
O.Secured_Data_Exchange	The VU must secure data exchanges with the motion sensor and with tachograph cards.

3.6 Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the VU.

3.6.1 Equipment design

M.Development	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
M.Manufacturing	VU manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which

maintains IT security, and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

3.6.2 Equipment delivery and activation

M.Delivery VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of non activated VUs is done in a manner which maintains VU security.

M.Activation Vehicle manufacturers and fitters or workshops must activate the VU after its installation before the vehicle leaves the premises where installation took place.

3.6.3 Security data generation and delivery

M.Sec_Data_Generation Security data generation algorithms must be accessible to authorised and trusted persons only.

M.Sec_Data_Transport Security data must be generated, transported, and inserted into the VU, in such a way to preserve its appropriate confidentiality and integrity.

3.6.4 Cards delivery

M.Card_Availability Tachograph cards must be available and delivered to authorised persons only.

M.Driver_Card_Uniqueness Drivers must possess, at one time, one valid driver card only.

M.Card_Traceability Card delivery must be traceable (white lists, black lists) , and black lists must be used during security audits.

3.6.5 Control device installation, calibration, and inspection

M.Approved_Workshops Installation, calibration and repair of control device must be carried by trusted and approved fitters or workshops.

M.Regular_Inpections Control device must be periodically inspected and calibrated.

M.Faithful_Calibration Approved fitters and workshops must enter proper vehicle parameters in control device during calibration.

3.6.6 Equipment operation

M.Faithful_Drivers Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, ...).

3.6.7 Law enforcement control

M.Controls Law enforcement controls must be performed regularly and randomly, and must include security audits.

3.6.8 Software upgrades

M.Software_Upgrade Software revisions must be granted security certification before they can be implemented in a VU.

4. Security enforcing functions

4.1 Identification and authentication

4.1.1 Motion sensor identification and authentication

UIA_201 The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.

UIA_202 The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.

UIA_203 The VU shall authenticate the motion sensor it is connected to:
- at motion sensor connection,
- at each calibration of the control device,
- at power supply recovery.

Authentication shall be mutual and triggered by the VU.

UIA_204 The VU shall periodically (*period TBD by manufacturer and more frequently than once per hour*) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the control device has not been changed.

UIA_205 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_206 After (*TBD by manufacturer and not more than 20)* consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the control device), the SEF shall:
- generate an audit record of the event,
- warn the user,
- continue to accept and use non secured motion data sent by the motion sensor.

4.1.2 User identification and authentication

UIA_207 The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.

UIA_208 The user identity shall consist of:
- a user group:
  - DRIVER (driver card),
  - CONTROLLER (control card),
  - WORKSHOP (workshop card),
  - COMPANY (company card),
  - UNKNOWN (no card inserted),
- a user ID, composed of :
  - the card issuing Contracting Party code and of the card number,
  - UNKNOWN if user group is UNKNOWN.

UNKNOWN identities may be implicitly or explicitly known.

UIA_209 The VU shall authenticate its users at card insertion.

UIA_210 The VU shall re-authenticate its users:
- at power supply recovery,
- periodically or after occurrence of specific events (*TBD by manufacturers and more frequently than once per day*).

UIA_211 Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.

UIA_212 In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long.
Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.

UIA_213 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_214 After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall:
- generate an audit record of the event,
- warn the user,
- assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007).

4.1.3 Remotely connected company identification and authentication

Company remote connection capability is optional. This paragraph therefore applies only if this feature is implemented.

UIA_215 For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.

UIA_216 The remotely connected company's identity shall consist of its company card issuing Contracting Party code and of its company card number.

UIA_217 The VU shall successfully authenticate the remotely connected company before allowing any data export to it.

UIA_218 Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.

UIA_219 The VU shall detect and prevent use of authentication data that has been copied and replayed.

UIA_220 After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:
- warn the remotely connected company.

4.1.4 Management device identification and authentication

VU manufacturers may foresee dedicated devices for additional VU management functions (e.g. Software upgrading, security data reloading, ...). This paragraph therefore applies only if this feature is implemented.

UIA_221 For every interaction with a management device, the VU shall be able to establish the device identity.

UIA_222 Before allowing any further interaction, the VU shall successfully authenticate the management device.

UIA_223 The VU shall detect and prevent use of authentication data that has been copied and replayed.

4.2 Access control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

It must be noted that the user data recorded by the VU, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011) is not the subject of a security enforcing function.

4.2.1 Access control policy

ACC_201 The VU shall manage and check access control rights to functions and to data.

4.2.2 Access rights to functions

ACC_202 The VU shall enforce the mode of operation selection rules (requirements 006 to 009).

ACC_203 The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).

4.2.3 Access rights to data

ACC_204 The VU shall enforce the VU identification data write access rules (requirement 076)

ACC_205 The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)

ACC_206 After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).

ACC_207 After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).

ACC_208 After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).

ACC_209 After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).

ACC_210 The VU shall enforce appropriate read and write access rights to security data (requirement 080).

4.2.4 File structure and access conditions

ACC_211 Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

4.3 Accountability

ACT_201 The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).

ACT_202 The VU shall hold permanent identification data (requirement 075).

ACT_203 The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).

ACT_204 The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).

ACT_205 The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).

ACT_206 The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.

ACT_207 The VU shall ensure that it does not modify data already stored in a tachograph card (requirements 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in sub-appendix 1, Paragraph 2.1.Note.

4.4 Audit

Audit capabilities are required only for events that may indicate a manipulation or a security breach attempt. It is not required for the normal exercising of rights even if relevant to security.

AUD_201 The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).

AUD_202 The events affecting the security of the VU are the following:

- Security breach attempts:
  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorised change of motion sensor,
  - card data input integrity error,
  - stored user data integrity error,
  - internal data transfer error,
  - unauthorised case opening,
  - hardware sabotage,
- Last card session not correctly closed,
- Motion data error event,
- Power supply interruption event,
- VU internal fault,

–

AUD_203 The VU shall enforce audit records storage rules (requirement 094 and 096).

AUD_204 The VU shall store audit records generated by the motion sensor in its data memory.

AUD_205 It shall be possible to print, display and download audit records.

4.5 Object reuse

REU_201 The VU shall ensure that temporary storage objects can be reused without this involving inadmissible information flow.

4.6 Accuracy

4.6.1 Information flow control policy

ACR_201 The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:

- vehicle motion data,
- VU's real time clock,
- control device calibration parameters,
- tachograph cards,
- user's inputs.

ACR_201a The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).

4.6.2 Internal data transfers

The requirements of this paragraph apply only if the VU makes use of physically separated parts.

ACR_202 If data are transferred between physically separated parts of the VU, the data shall be protected from modification.

ACR_203 Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

4.6.3 Stored data integrity

ACR_204 The VU shall check user data stored in the data memory for integrity errors.

ACR_205 Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

4.7 Reliability of service

4.7.1 Tests

RLB_201 All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. It shall not be possible to restore them for later use.

RLB_202 The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).

RLB_203 Upon detection of an internal fault during self test, the SEF shall:
- generate an audit record (except in calibration mode) (VU internal fault),
- Preserve the stored data integrity.

4.7.2 Software

RBL_204 There shall be no way to analyse or debug software in the field after the VU activation.

RLB_205 Inputs from external sources shall not be accepted as executable code.

4.7.3 Physical protection

RLB_206 If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).

If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).

RLB_207 After its activation, the VU shall detect specified (*TBD by manufacturer*) hardware sabotage.

RLB_208 In the case described above, the SEF shall generate an audit record and the VU shall: (*TBD by manufacturer*).

4.7.4 Power supply interruptions

RLB_209 The VU shall detect deviations from the specified values of the power supply, including cut-off.

RLB_210 In the case described above, the SEF shall:
- generate an audit record (except in calibration mode),
- preserve the secure state of the VU,
- maintain the security functions, related to components or processes still operational,
- preserve the stored data integrity.

4.7.5 Reset conditions

RLB_211 In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall be reset cleanly.

4.7.6 Data availability

RLB_212 The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

RLB_213 The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016)

RLB_214 In the case described above, the SEF shall generate an audit record of the event.

4.7.7 Multiple applications

RLB_215 If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.

4.8 Data exchange

This paragraph addresses data exchange between the VU and connected devices.

4.8.1 Data exchange with motion sensor

DEX_201 The VU shall verify the integrity and authenticity of motion data imported from the motion sensor

DEX_202 Upon detection of a motion data integrity or authenticity error, the SEF shall:
- generate an audit record,
- continue to use imported data.

4.8.2 Data exchange with tachograph cards

DEX_203 The VU shall verify the integrity and authenticity of data imported from tachograph cards.

DEX_204 Upon detection of card data integrity or authenticity error, the VU shall:
- generate an audit record,
- not use the data.

DEX_205 The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

4.8.3 Data exchange with external storage media (downloading function))

DEX_206 The VU shall generate an evidence of origin for data downloaded to external media.

DEX_207 The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.

DEX_208 The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.

4.9 Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions.

CSP_201 Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.

CSP_202 If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes.

CSP_203 If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.

CSP_204 If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.

CSP_205 If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.

5. Definition of security mechanisms

Required security mechanisms are specified in sub-appendix 11.

All other security mechanisms are to be defined by manufacturers.

6. Minimum strength of security mechanisms

The minimum strength of the Vehicle Unit security mechanisms is **High**, as defined in [ITSEC].

7. Level of assurance

The target level of assurance for the Vehicle Unit is ITSEC level **E3**, as defined in [ITSEC].

8. Rationale

The following matrixes give a rationale for the SEFs by showing:
- which SEFs or means counteract which threats,
- which SEFs fulfil which IT security objectives.

	Threats																	IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Physical Personnel Procedural Means																											
Development			x	x	x																						
Manufacturing				x	x																						
Delivery													x														
Activation	x												x														
Security Data Generation																	x										
Security Data Transport																	x										
Card Availability		x																									
One Driver Card		x																									
Card Traceability		x																									
Approved Workshops						x		x																			
Regular Inspection Calibration						x		x			x				x			x									

	Threats																		IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Faithful workshops						x		x																				
Faithful drivers		x																									
Law enforcement controls		x				x		x	x		x		x		x		x	x									
Software Upgrade																		x									
Security Enforcing Functions																											
Identification and Authentication																											
UIA_201 Sensor identification										x		x										x					x
UIA_202 Sensor identity										x		x										x					
UIA_203 Sensor authentication										x		x										x					x
UIA_204 Sensor re-identification and re-authentication										x		x										x					x
UIA_205 Unforgeable authentication										x		x										x					
UIA_206 Authentication failure										x		x									x					x	
UIA_207 Users identification	x	x								x									x			x					x
UIA_208 User identity	x	x								x									x			x					
UIA_209 User authentication	x	x								x									x			x					x
UIA_210 User re-authentication	x	x								x									x			x					x
UIA_211 Authentication means	x	x								x									x			x					
UIA_212 PIN checks	x	x				x		x											x			x					
UIA_213 Unforgeable authentication	x	x								x									x			x					
UIA_214 Authentication failure	x	x								x											x						
UIA_215 Remote user identification	x	x																	x			x					x
UIA_216 Remote user identity	x	x																	x			x					

		Threats																			IT Objectives									
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
UIA_217	Remote user authentication	x	x																		x			x					x
UIA_218	Authentication means	x	x																		x			x					
UIA_219	Unforgeable authentication	x	x																		x			x					
UIA_220	Authentication failure	x	x																										
UIA_221	Management device Identification	x	x																		x			x					
UIA_222	Management device Authentication	x	x																		x			x					
UIA_223	Unforgeable authentication	x	x																		x			x					
Access Control																														
ACC_201	Access control policy	x					x		x									x		x	x									
ACC_202	Access rights to functions	x					x		x												x									
ACC_203	Access rights to functions	x					x		x												x									
ACC_204	VU ID																			x	x									
ACC_205	Connected sensor ID										x									x	x									
ACC_206	Calibration data	x					x													x	x									
ACC_207	Calibration data						x													x	x									
ACC_208	Time adjustment data								x											x	x									
ACC_209	Time adjustment data								x											x	x									
ACC_210	Security Data																	x		x	x									

	Threats																			IT Objectives									
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
ACC_211 File structure and access conditions	x					x											x		x	x								
Accountability																													
ACT_201 Drivers accountability																					x								
ACT_202 VU ID data																					x	x							
ACT_203 Workshops accountability																					x								
ACT_204 Controllers accountability																					x								
ACT_205 Vehicle movement accountability																					x								
ACT_206 Accountability data modification																			x					x			x		
ACT_207 Accountability data modification																			x					x			x		
Audit																													
AUD_201 Audit records																						x							
AUD_202 Audit events list	x						x				x	x		x	x				x			x							
AUD_203 Audit records storage rules																						x							
AUD_204 Sensor audit records																						x							
AUD_205 Audit tools																						x							
Reuse																													
REU_201 Reuse																	x								x	x			

	Threats																			IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Accuracy																												
ACR_201 Information flow control policy							x			x		x														x	x	
ACR_202 Internal transfers														x										x	x	x	
ACR_203 Internal transfers														x								x						
ACR_204 Stored data integrity																			x				x			x		
ACR_205 Stored data integrity																			x			x						
Reliability																												
RLB_201 Manufacturing tests				x	x																						x	
RLB_202 Self tests			x								x				x			x									x	
RLB_203 Self tests											x				x			x				x						
RLB_204 Software analysis					x													x									x	
RLB_205 Software input																		x						x	x	x		
RLB_206 Case opening					x				x		x			x			x	x	x					x		x		
RLB_207 Hardware sabotage											x															x		
RLB_208 Hardware sabotage											x											x						
RLB_209 Power supply interruptions															x											x		
RLB_210 Power supply interruptions															x							x						
RLB_211 Reset			x																							x		
RLB_212 Data Availability																									x	x		
RLB_213 Card release																										x		
RLB_214 card session not correctly closed																						x						

	Threats																			IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
RLB_215 Multiple Applications																											x	
Data exchange																												
DEX_201 Secured motion data import												x																x
DEX_202 Secured motion data import												x										x						
DEX_203 Secured card data import							x																					x
DEX_204 Secured card data import							x															x						
DEX_205 Secured data export to cards							x																					x
DEX_206 Evidence of origin														x											x			
DEX_207 Evidence of origin														x											x			
DEX_208 Secured export to external media														x											x			
Cryptographic support																												
CSP_201 Algorithms																											x	x
CSP_202 key generation																											x	x
CSP_203 key distribution																											x	x
CSP_204 key access																											x	x
CSP_205 key destruction																											x	x

TACHOGRAPH CARD GENERIC SECURITY TARGET

1. Introduction

This document contains a description of the tachograph card, of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms, and the required level of assurance for the development and the evaluation.

Requirements referred to in the document, are those of the body of Appendix 1B. For clarity of reading, duplication sometimes arises between Appendix 1B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Appendix 1B requirement referred by this security target requirement, the Appendix 1B body requirement shall prevail.

Appendix 1B body requirements not referred by security targets are not the subject of security enforcing functions.

A tachograph card is a standard smart card carrying a dedicated tachograph application, and shall comply to up-to-date functional and assurance security requirements applicable to smart cards. This security target therefore incorporates only the extra security requirements needed by the tachograph application.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

2. Abbreviations, definitions and references

2.1 Abbreviations

IC Integrated Circuit
(Electronic component designed to perform processing and/or memory functions),

OS Operating system,

PIN Personal Identification Number,

ROM Read Only Memory,

SFP Security Functions Policy,

TBD To Be Defined,

TOE Target of Evaluation,

TSF TOE Security Function,

VU Vehicle Unit.

2.2 Definitions

Digital tachograph	Control device.
Sensitive data	Data stored by the tachograph card that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data.

Security data	The specific data needed to support security enforcing functions (e.g. crypto keys).
System	Equipment, people or organisations involved in any way with the control device.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (when not used in the expression "user data").
User data	Sensitive data stored in the tachograph card, other than security data. User data include identification data and activity data.
Identification data	Identification data include card identification data and cardholder identification data.
Card identification data	User data related to card identification as defined by requirements 190, 191, 192, 194, 215, 231 and 235.
Cardholder identification data	User data related to cardholder identification as defined by requirements 195, 196, 216, 232 and 236.
Activity data	Activity data include cardholder activities data, events and faults data and control activity data.
Cardholder activities data	User data related to the activities carried by the cardholder as defined by requirements 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 and 237.
Events and faults data	User data related to events or faults as defined by requirements 204, 205, 207, 208 and 223.
Control activity data	User data related to law enforcement controls as defined by requirements 210 and 225.

2.3 References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.
IC PP	Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

3. Product Rationale

3.1 Tachograph card description and method of use

A tachograph card is a smart card, as described in [IC PP] and [ES PP], carrying an application intended for its use with the control device.

The basic functions of the tachograph card are:

- to store card identification and card holder identification data. These data are used by the vehicle unit to identify the cardholder, provide accordingly functions and data access rights, and ensure cardholder accountability for his activities,
- to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

A tachograph card is therefore intended to be used by a card interface device of a vehicle unit. It may also be used by any card reader (e.g. of a personal computer) which shall have full read access right on any user data.

During the end-usage phase of a tachograph card life-cycle (phase 7 of life-cycle as described in [ES PP]), vehicle units only may write user data to the card.

The functional requirements for a tachograph card are specified in Appendix 1B body text and sub-appendix 2.

3.2 Tachograph card life-cycle

The tachograph card life-cycle conforms to smart card life cycle described in [ES PP].

3.3 Threats

In addition to the smart card general threats listed in [ES PP] and [IC PP], the tachograph card may face the following threats:

3.3.1 Final aims

The final aim of attackers will be to modify user data stored within the TOE.

T.Ident_Data	A successful modification of identification data held by the TOE (e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.
T.Activity_Data	A successful modification of activity data stored in the TOE would be a threat to the security of the TOE.
T.Data_exchange	A successful modification of activity data (addition, deletion, modification) during import or export would be a threat to the security of the TOE.

3.3.2 Attack paths

TOE's assets may be attacked by:

- trying to gain illicit knowledge of TOE's hardware and software design and especially of its security functions or security data. Illicit knowledge may be gained though attacks to designer or manufacturer material (theft, bribery, ...) or through direct examination of the TOE (physical probing, inference analysis, ...).
- taking advantage of weaknesses in TOE design or realisation (exploit errors in hardware, errors in software, transmission faults, errors induced in TOE by environmental stress, exploit weaknesses of security functions such as authentication procedures, data access control, cryptographic operations,...).
- modifying the TOE or its security functions through physical, electrical or logical attacks or combination of these.

3.4 Security Objectives

The main security objective of the entire digital tachograph system is the following:

O.Main The data to be checked by control authorities must be available and reflect fully and accurately the activity of controlled drivers and vehicles in terms of driving, work, availability and rest period and in terms of vehicle speed.

Therefore the main security objectives of the TOE, contributing to this global security objective are the following :

O.Card_Identification_Data The TOE must preserve card identification data and cardholder identification data stored during card personalisation process.

O.Card_Activity_Storage The TOE must preserve user data stored in the card by vehicle units.

3.5 Information Technology security objectives

In addition to the smart card general security objectives listed in [ES PP] and [IC PP], the specific IT security objectives of the TOE that contributes to its main security objectives during its end-usage life-cycle phase are the following:

O.Data_Access The TOE must limit user data write access rights to authenticated vehicle units.

O.Secure_Communications The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application.

3.6 Physical, personnel or procedural means

The physical, personnel or procedural requirements that contribute to the security of the TOE are listed in [ES PP] and [IC PP] (chapters security objectives for the environment).

4. Security enforcing functions

This paragraph refines some of the permitted operations such as assignment or selection of [ES PP] and provides additional SEF functional requirements.

4.1 Compliance to protection profiles

CPP_301 The TOE shall comply with [IC PP].

CPP_302 The TOE shall comply with [ES PP] as refined further.

4.2 User Identification and authentication

The card must identify the entity in which it is inserted and know whether it is an authenticated vehicle unit or not. The card may export any user data whatever the entity it is connected to, except the control card and company card which may export card holder identification data to authenticated vehicle units only (such that a controller is ensured that the vehicle unit is not a fake one by seeing his name on display or printouts).

4.2.1 User identification

Assignment (FIA_UID.1.1) *List of TSF mediated actions*: none.

Assignment (FIA_ATD.1.1) *List of security attributes*:

- **USER_GROUP**: VEHICLE_UNIT, NON_VEHICLE_UNIT,
- **USER_ID:** Vehicle Registration Number (VRN) and registering Contracting Party Code (USER_ID is known for USER_GROUP = VEHICLE_UNIT only).

4.2.2 User authentication

Assignment (FIA_UAU.1.1) *List of TSF mediated actions*:

- Driver and Workshop cards: Export user data with security attributes (card data download function),
- Control card: Export user data without security attributes except cardholder identification data.

UIA_301 Authentication of a vehicle unit shall be performed by means of proving that it possesses security data that only the system could distribute.

Selection (FIA_UAU.3.1 and FIA_UAU.3.2): prevent.

Assignment (FIA_UAU.4.1) *Identified authentication mechanism(s)*: any authentication mechanism.

UIA_302 The Workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the Vehicle Unit to ensure the identity of the card holder, it is not intended to protect Workshop card content).

4.2.3 Authentication failures

The following assignments describe the card reaction for each single user authentication failure.

Assignment (FIA_AFL.1.1) *Number*: 1, *list of authentication events*: authentication of a card interface device.

Assignment (FIA_AFL.1.2) *List of actions*:

- warn the entity connected,
- assume the user as NON_VEHICLE_UNIT.

Additionally the following assignments describe the card reaction in the case of failure of the additional authentication mechanism required in UIA_302.

Assignment (FIA_AFL.1.1) *Number*: 5, *list of authentication events*: PIN checks (workshop card).

Assignment (FIA_AFL.1.2) *List of actions*:

- warn the entity connected,
- block the PIN check procedure such that any subsequent PIN check attempt will fail,
- be able to indicate to subsequent users the reason of the blocking.

4.3 Access control

4.3.1 Access control policy

During end-usage phase of its life-cycle, the tachograph card is the subject of one single access control Security Function Policy (SFP) named AC_SFP.

Assignment (FDP_ACC.2.1) *Access control SFP*: AC_SFP.

4.3.2 Access control functions

Assignment (FDP_ACF.1.1) *Access control SFP*: AC_SFP.

Assignment (FDP_ACF.1.1) *Named group of security attributes*: USER_GROUP.

Assignment (FDP_ACF.1.2) *Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*:

- GENERAL_READ: User data may be read from the TOE by any user, except cardholder identification data which may be read from control card and company card by VEHICLE_UNIT only.
- IDENTIF_WRITE: Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle.
- ACTIVITY_WRITE: Activity data may be written to the TOE by VEHICLE_UNIT only.
- SOFT_UPGRADE: No user may upgrade TOE's software.
- FILE_STRUCTURE: Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.

4.4 Accountability

ACT_301 The TOE shall hold permanent identification data.

ACT_302 There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable.

4.5 Audit

The TOE must monitor events that indicate a potential violation of its security.

Assignment (FAU_SAA.1.2) *Subset of defined auditable events*:

- cardholder authentication failure (5 consecutive unsuccessful PIN checks),
- self test error,
- stored data integrity error,
- activity data input integrity error.

4.6 Accuracy

4.6.1 Stored Data Integrity

Assignment (FDP_SDI.2.2) *Actions to be taken*: warn the entity connected,

4.6.2 Basic data authentication

Assignment (FDP_DAU.1.1) *List of objects or information types*: Activity data.

Assignment (FDP_DAU.1.2) *List of subjects*: Any.

4.7 Reliability of service

4.7.1 Tests

Selection (FPT_TST.1.1): during initial start-up, periodically during normal operation.

Note: during initial start-up means before code is executed (and not necessarily during Answer To Reset procedure).

RLB_301 The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM.

RLB_302 Upon detection of a self test error the TSF shall warn the entity connected.

RLB_303 After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life cycle state shall never be accessed during another state.

4.7.2 Software

RLB_304 There shall be no way to analyse, debug or modify TOE's software in the field.

RLB_305 Inputs from external sources shall not be accepted as executable code.

4.7.3 Power supply

RLB_306 The TOE shall preserve a secure state during power supply cut-off or variations.

4.7.4 Reset conditions

RLB_307 If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.

4.8 Data exchange

4.8.1 Data exchange with a vehicle unit

DEX_301 The TOE shall verify the integrity and authenticity of data imported from a vehicle unit.

DEX_302 Upon detection of an imported data integrity error, the TOE shall:

- Warn the entity sending the data,
- not use the data.

DEX_303 The TOE shall export user data to the vehicle unit with associated security attributes, such that the vehicle unit will be able to verify the integrity and authenticity of data received.

4.8.2 Export of data to a non - vehicle unit (download function)

DEX_304 The TOE shall be able to generate an evidence of origin for data downloaded to external media.

DEX_305 The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient.

DEX_306 The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified.

4.9 Cryptographic Support

CSP_301 If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes. Generated cryptographic session keys shall have a limited *(TBD by manufacturer and not more than 240)* number of possible use.

CSP_302 If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods.

5. Definition of Security Mechanisms

Required security mechanisms are specified in sub-appendix 11.

All other security mechanisms are to be defined by the TOE manufacturer.

6. Claimed Minimum Strength of Mechanisms

The minimum strength of mechanisms for the Tachograph Card is **High** as defined in [ITSEC].

7. Level of Assurance

The target level of assurance for the Tachograph Card is ITSEC level **E3**, as defined in [ITSEC].

8. Rationale

The following matrixes give a rationale for the additional SEFs by showing:

- which SEFs counteract which threats,
- which SEFs fulfil which IT security objectives.

		Threats											IT Objectives								
		T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
UIA_301	Authentication means																			x	
UIA_302	PIN checks																			x	
ACT_301	Identification data																				
ACT_302	Personalisation date																				
RLB_301	Software integrity												x		x						
RLB_302	Self tests												x		x						
RLB_303	Manufacturing tests					x	x						x		x						
RLB_304	Software analysis					x		x	x				x		x						
RLB_305	Software input					x	x		x				x		x						
RLB_306	Power supply									x	x		x		x						
RLB_307	Reset												x		x						
DEX_301	Secured data import											x									x
DEX_302	Secured data import											x									x
DEX_303	Secured data export to VU											x									x
DEX_304	Evidence of origin											x									x
DEX_305	Evidence of origin											x									x
DEX_306	Secured export to external media											x									x
CSP_301	key generation												x								x
CSP_302	key distribution												x								x

SUB-APPENDIX XI

COMMON SECURITY MECHANISMS

CONTENTS

1. Generalities

This sub-appendix specifies the security mechanisms ensuring:

- The mutual authentication between VUs and tachograph cards, including session key agreement,
- The confidentiality, integrity and authentication of data transferred between VUs and tachograph cards,
- The integrity and authentication of data downloaded from VUs to external storage media,
- The integrity and authentication of data downloaded from tachograph cards to external storage media.

1.1 References

The following references are used in this sub-appendix:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1 : Secure Hash Standard.* April 1995.
PKCS1	RSA Laboratories. PKCS # 1 : *RSA Encryption Standard.* Version 2.0. October 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3 : Data Encryption Standard.* Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997.
ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2 Notations and abbreviated terms

The following notations and abbreviated terms are used in this sub-appendix:

(K_a, K_b, K_c)	a key bundle for use by the Triple Data Encryption Algorithm,
CA	Certification Authority,
CAR	Certification Authority Reference,
CC	Cryptographic Checksum,
CG	Cryptogram,
CH	Command Header,
CHA	Certificate Holder Authorisation,
CHR	Certificate Holder Reference,
D()	Decryption with DES,
DE	Data Element,
DO	Data Object,
d	RSA private key, private exponent,
e	RSA public key, public exponent,
E()	Encryption with DES,
EQT	Equipment,
Hash()	hash value, an output of *Hash*,
Hash	hash function,
KID	Key Identifier,
Km	TDES key. Master Key defined in ISO 16844-3.
Km_{VU}	TDES key inserted in vehicle units.
Km_{WC}	TDES key inserted in workshop cards.
m	message representative, an integer between 0 and n-1,
n	RSA keys, modulus,
PB	Padding Bytes,
PI	Padding Indicator byte (for use in Cryptogram for confidentiality DO),
PV	Plain Value,
s	signature representative, an integer between 0 and n-1,
SSC	Send Sequence Counter,
SM	Secure Messaging,
TCBC	TDEA Cipher Block Chaining Mode of Operation
TDEA	Triple Data Encryption Algorithm,
TLV	Tag Length Value,
VU	Vehicle Unit,
X.C	the certificate of user X issued by a certification authority,
X.CA	a certification authority of user X,

$X.CA.PK_o X.C$	the operation of unwrapping a certificate to extract a public key. It is an infix operator, whose left operand is the public key of a certification authority, and whose right operand is the certificate issued by that certification authority. The outcome is the public key of the user X whose certificate is the right operand,
X.PK	RSA public key of a user X,
X.PK[I]	RSA encipherment of some information I, using the public key of user X,
X.SK	RSA private key of a user X,
X.SK[I]	RSA encipherment of some information I, using the private key of user X,
'xx'	an Hexadecimal value,
||	concatenation operator.

2. Cryptographic systems and algorithms

2.1 Cryptographic systems

CSM_001 Vehicle units and tachograph cards shall use a classical RSA public-key cryptographic system to provide the following security mechanisms:

- authentication between vehicle units and cards,
- transport of Triple-DES session keys between vehicle units and tachograph cards,
- digital signature of data downloaded from vehicle units or tachograph cards to external media.

CSM_002 Vehicle units and tachograph cards shall use a Triple DES symmetric cryptographic system to provide a mechanism for data integrity during user data exchange between vehicle units and tachograph cards, and to provide, where applicable, confidentiality of data exchange between vehicle units and tachograph cards.

2.2 Cryptographic algorithms

2.2.1 RSA algorithm

CSM_003 The RSA algorithm is fully defined by the following relations:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

A more comprehensive description of the RSA function can be found in reference [PKCS1].

Public exponent, e, for RSA calculations is an integer between 3 and n-1 satisfying gcd(e, lcm(p-1, q-1)) =1.

2.2.2 Hash algorithm

CSM_004 The digital signature mechanisms shall use the SHA-1 hash algorithm as defined in reference [SHA-1].

2.2.3 Data Encryption Algorithm

CSM_005 DES based algorithms shall be used in Cipher Block Chaining mode of operation.

3. Keys and certificates

3.1 Keys generation and distribution

3.1.1 RSA Keys generation and distribution

CSM_006 RSA keys shall be generated through three functional hierarchical levels:

- European level,
- Contracting Party level,
- Equipment level.

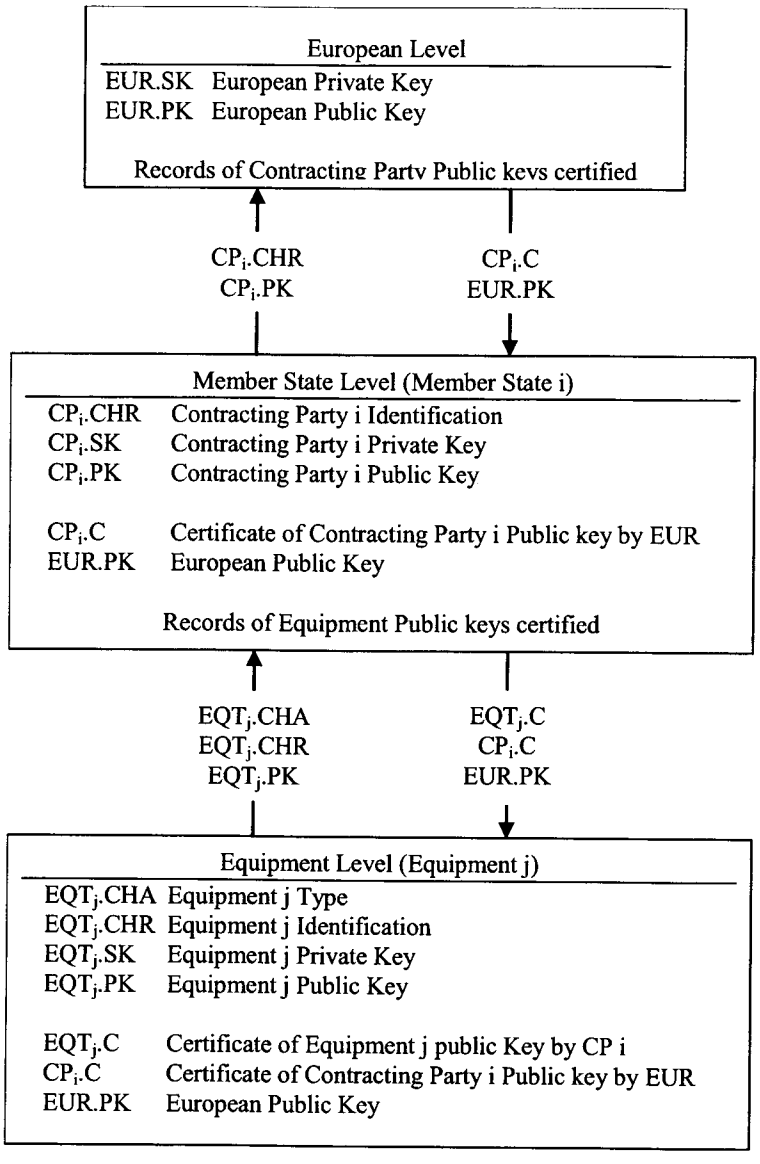
CSM_007 At European level, a single European key pair (EUR.SK and EUR.PK) shall be generated. The European private key shall be used to certify the Contracting Parties public keys. Records of all certified keys shall be kept. These tasks shall be handled by a European Certification Authority recognized at the international level.

CSM_008 At Contracting Party level, a Contracting Party key pair (CP.SK and CP.PK) shall be generated. Contracting Parties public keys shall be certified by the European Certification Authority. The Contracting Party private key shall be used to certify public keys to be inserted in equipment (vehicle unit or tachograph card). Records of all certified public keys shall be kept with the identification of the equipment to which it is intended. These tasks shall be handled by a Contracting Party Certification Authority. A Contracting Party may regularly change its key pair.

CSM_009 At equipment level, one single key pair (EQT.SK and EQT.PK) shall be generated and inserted in each equipment. Equipment public keys shall be certified by a Contracting Party Certification Authority. These tasks may be handled by equipment manufacturers, equipment personalisers or Contracting Party authorities. This key pair is used for authentication, digital signature and encipherement services

CSM_010 Private keys confidentiality shall be maintained during generation, transport (if any) and storage.

The following picture summarises the data flow of this process:



3.1.2 RSA Test keys

CSM_011 For the purpose of equipment testing (including interoperability tests) the European Certification Authority shall generate a different single European test key pair and at least two Contracting Party test key pairs, the public keys of which shall be certified with the European private test key. Manufacturers shall insert, in equipment undergoing type approval tests, test keys certified by one of these Contracting Party test keys.

3.1.3 Motion sensor keys

The confidentiality of the three TDES keys described below shall be appropriately maintained during generation, transport (if any) and storage.

In order to support control device compliant with ISO 16844, the European Certification Authority and the Contracting Party Certification Authorities shall, in addition, ensure the following:

CSM_036 The European Certification Authority shall generate Km_{VU} and Km_{WC}, two independent and unique Triple DES keys, and generate Km as :

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

The European Certification Authority shall forward these keys, under appropriately secured procedures, to Contracting Party Certification Authorities at their request.

CSM_037 Contracting Party Certification Authorities shall:

- use Km to encrypt motion sensor data requested by motion sensor manufacturers (data to be encrypted with Km is defined in ISO 16844-3),
- forward Km_{VU} to vehicle unit manufacturers, under appropriately secured procedures, for insertion in vehicle units,
- ensure that Km_{WC} will be inserted in all workshop cards (SensorInstallationSecData in Sensor_Installation_Data elementary file) during card personalisation.

3.1.4 T-DES session keys generation and distribution

CSM_012 Vehicle units and tachograph cards shall, as a part of the mutual authentication process, generate and exchange necessary data to elaborate a common Triple DES session key. This exchange of data shall be protected for confidentiality through an RSA crypt-mechanism.

CSM_013 This key shall be used for all subsequent cryptographic operations using secure messaging. Its validity shall expire at the end of the session (withdrawal of the card or reset of the card) and/or after 240 use (one use of the key = one command using secure messaging sent to the card and associated response).

3.2 Keys

CSM_014 RSA keys shall have (whatever the level) the following lengths: modulus *n* 1024 bits, public exponent *e* 64 bits maximum, private exponent *d* 1024 bits.

CSM_015 Triple DES keys shall have the form (K_a, K_b, K_a) where K_a and K_b are independent 64 bits long keys. No parity error detecting bits shall be set.

3.3 Certificates

CSM_016 RSA Public key certificates shall be "non self-descriptive" "Card Verifiable" certificates (Ref.: ISO/IEC 7816-8)

3.3.1 Certificates content

CSM_017 RSA Public key certificates are built with the following data in the following order :

Data	Format	Bytes	Observations
CPI	INTEGER	1	Certificate Profile Identifier ('01' for this version)
CAR	OCTET STRING	8	Certification Authority Reference
CHA	OCTET STRING	7	Certificate Holder Authorisation
EOV	TimeReal	4	Certificate end of validity. Optional, "FF" padded if not used.
CHR	OCTET STRING	8	Certificate Holder Reference
n	OCTET STRING	128	Public key (modulus)
e	OCTET STRING	8	Public Key (public exponent)
		164	

Notes:

1. The "Certificate Profile Identifier" (CPI) delineates the exact structure of an authentication certificate. It can be used as an equipment internal identifier of a relevant headerlist which describes the concatenation of Data Elements within the certificate.

   The headerlist associated with this certificate content is as follows:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Extended Headerlist Tag	Length of header list	CPI Tag	CPI Length	CAR Tag	CAR Length	CHA Tag	CHA Length	EOV Tag	EOV Length	CHR Tag	CHR Length	Public Key Tag (Constructed)	Length of subsequent DOs	modulus Tag	modulus length	public exponent Tag	Public exponent length

2. The "Certification Authority Reference" (CAR) has the purpose of identifying the certificate issuing CA, in such a way that the Data Element can be used at the same time as an Authority Key Identifier to reference the Public Key of the Certification Authority (for coding, see Key Identifier below).
3. The "Certificate Holder Authorisation" (CHA) is used to identify the rights of the certificate holder. It consists of the Tachograph Application ID and of the type of equipment to which the certificate is intended (according to EquipmentType data element, '00' for a Contracting Party).

4. The "Certificate Holder Reference" (CHR) has the purpose of identifying uniquely the certificate holder, in such a way that the Data Element can be used at the same time as a Subject Key Identifier to reference the Public Key of the certificate holder.
5. Key Identifiers uniquely identify certificate holder or certification authorities. They are coded as follows:

5.1 Equipment (VU or Card):

Data	Equipment serial number	Date	Type	Manufacturer
Length	4 Bytes	2 Bytes	1 Byte	1 Byte
Value	Integer	mm yy BCD coding	Manufacturer specific	Manufacturer code

In the case of a VU, the manufacturer, when requesting certificates, may or may not know the identification of the equipment in which the keys will be inserted.

In the first case, the manufacturer will send the equipment identification with the public key to its Contracting Party authority for certification. The certificate will then contain the equipment identification, and the manufacturer must ensure that keys and certificate are inserted in the intended equipment. The Key identifier has the form shown above.

In the later case, the manufacturer must uniquely identify each certificate request and send this identification with the public key to its Contracting Party authority for certification. The certificate will contain the request identification. The manufacturer must feed back its Contracting Party authority with the assignment of key to equipment (i.e. certificate request identification, equipment identification) after key installation in the equipment. The key identifier has the following form:

Data	Certificate request serial number	Date	Type	Manufacturer
Length	4 Bytes	2 Bytes	1 Byte	1 Byte
Value	integer	mm yy BCD coding	'FF'	Manufacturer code

5.2 Certification Authority:

Data	Authority Identification	Key serial number	Additional info	Identifier
Length	4 Bytes	1 Byte	2 Bytes	1 Byte
Value	1 Byte nation numerical code 3 Bytes nation alphanumerical code	Integer	additional coding (CA specific) 'FF FF' if not used	'01'

The key serial number is used to distinguish the different keys of a Contracting Party, in the case the key is changed.

6. Certificate verifiers shall implicitly know that the public key certified is an RSA key relevant to authentication, digital signature verification and encipherement for confidentiality services (the certificate contains no Object Identifier to specify it).

3.3.2 Certificates issued

CSM_018 The certificate issued is a digital signature with partial recovery of the certificate content in accordance with ISO/IEC 9796-2, except for its Annex A.4, with the "Certification Authority Reference" appended.

$$X.C = X.CA.SK[\text{'6A'} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{'BC'}] \parallel C_n \parallel X.CAR$$

With certificate content

$$= Cc = \underset{106 \text{ bytes}}{C_r} \parallel \underset{58 \text{ bytes}}{C_n}$$

Notes:

1. This certificate is 194 bytes long.
2. CAR, being hidden by the signature, is also appended to the signature, such that the Public Key of the Certification Authority may be selected for the verification of the certificate.
3. The certificate verifier shall implicitly know the algorithm used by the Certification Authority to sign the certificate.
4. The headerlist associated with this issued certificate is as follows:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV Certificate Tag (Constructed)	Length of subsequent DOs	Signature Tag	Signature Length	Remainder Tag	Remainder Length	CAR Tag	CAR Length

3.3.3 Certificate verification and unwrapping

Certificate verification and unwrapping consists in verifying the signature in accordance with ISO/IEC 9796-2, retrieving the certificate content and the public key contained : X.PK = X.CA.PK $_o$ X.C, and verifying the validity of the certificate.

CSM_019 It involves the following steps :

Verify signature and retrieve content:

- from X.C retrieve Sign, C_n' and CAR':

$$X.C = \underset{128 \text{ Bytes}}{\text{Sign}} \parallel \underset{58 \text{ Bytes}}{C_n'} \parallel \underset{8 \text{ Bytes}}{\text{CAR'}}$$

- from CAR' select appropriate Certification Authority Public Key (if not done before through other means)

- open Sign with CA Public Key : Sr'= X.CA.PK [Sign],
- check Sr' starts with '6A' and ends with 'BC'
- compute C_r' and H' from:

$$Sr' = \text{'6A'} \,||\, \underbrace{C_r'}_{106\ \text{Bytes}} \,||\, \underbrace{H'}_{20\ \text{Bytes}} \,||\, \text{'BC'}$$

- Recover certificate content C' = C_r' || C_n',
- check *Hash*(C') = H'

If the checks are OK the certificate is a genuine one, its content is C'.

Verify validity. From C':
- if applicable, check End of validity date,

Retrieve and store public key, Key Identifier, Certificate Holder Authorisation and Certificate End of Validity from C':
- X.PK = $n \,||\, e$
- X.KID = CHR
- X.CHA = CHA
- X.EOV = EOV

4. Mutual authentication mechanism

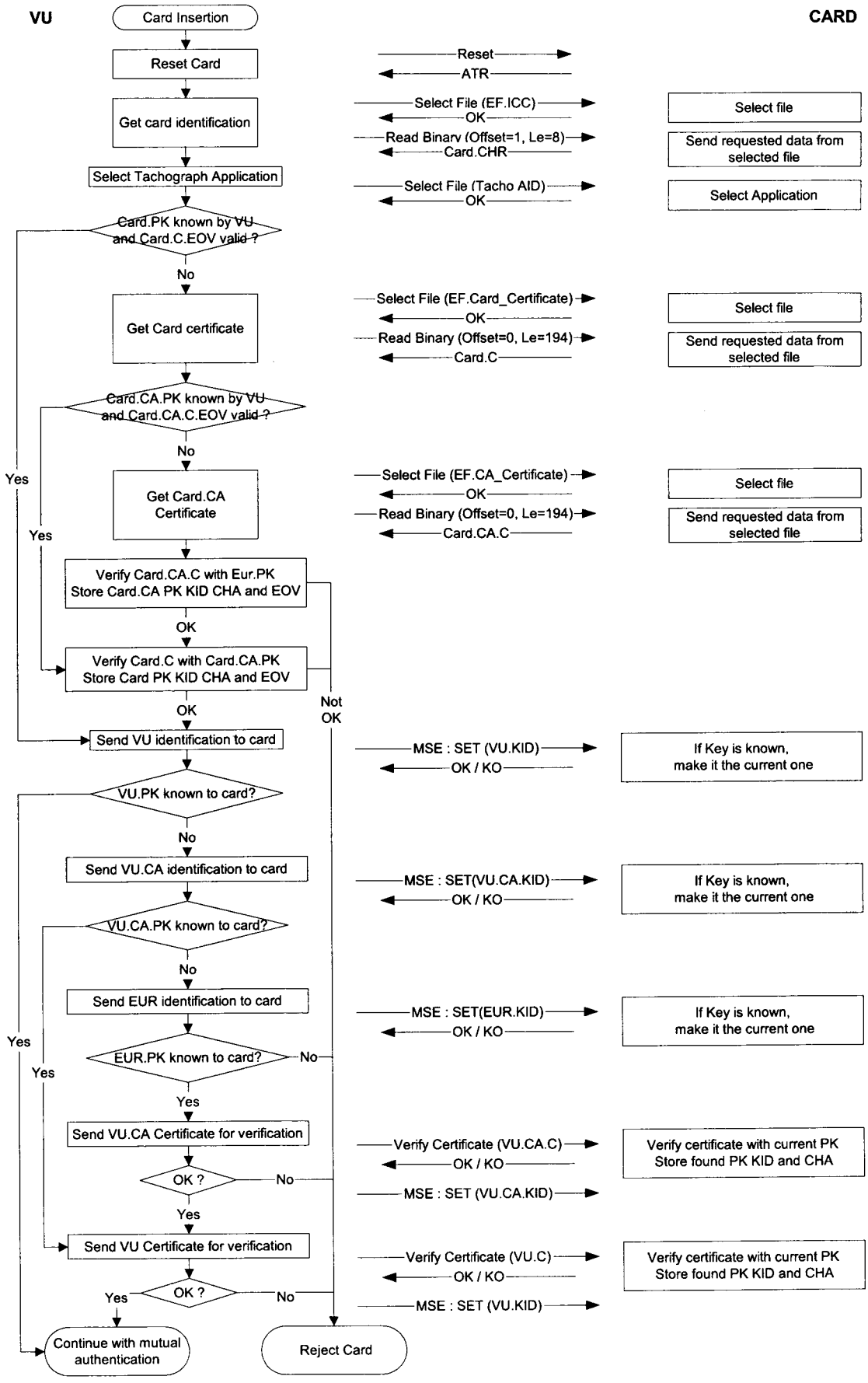
Mutual authentication between cards and VUs is based on the following principle :

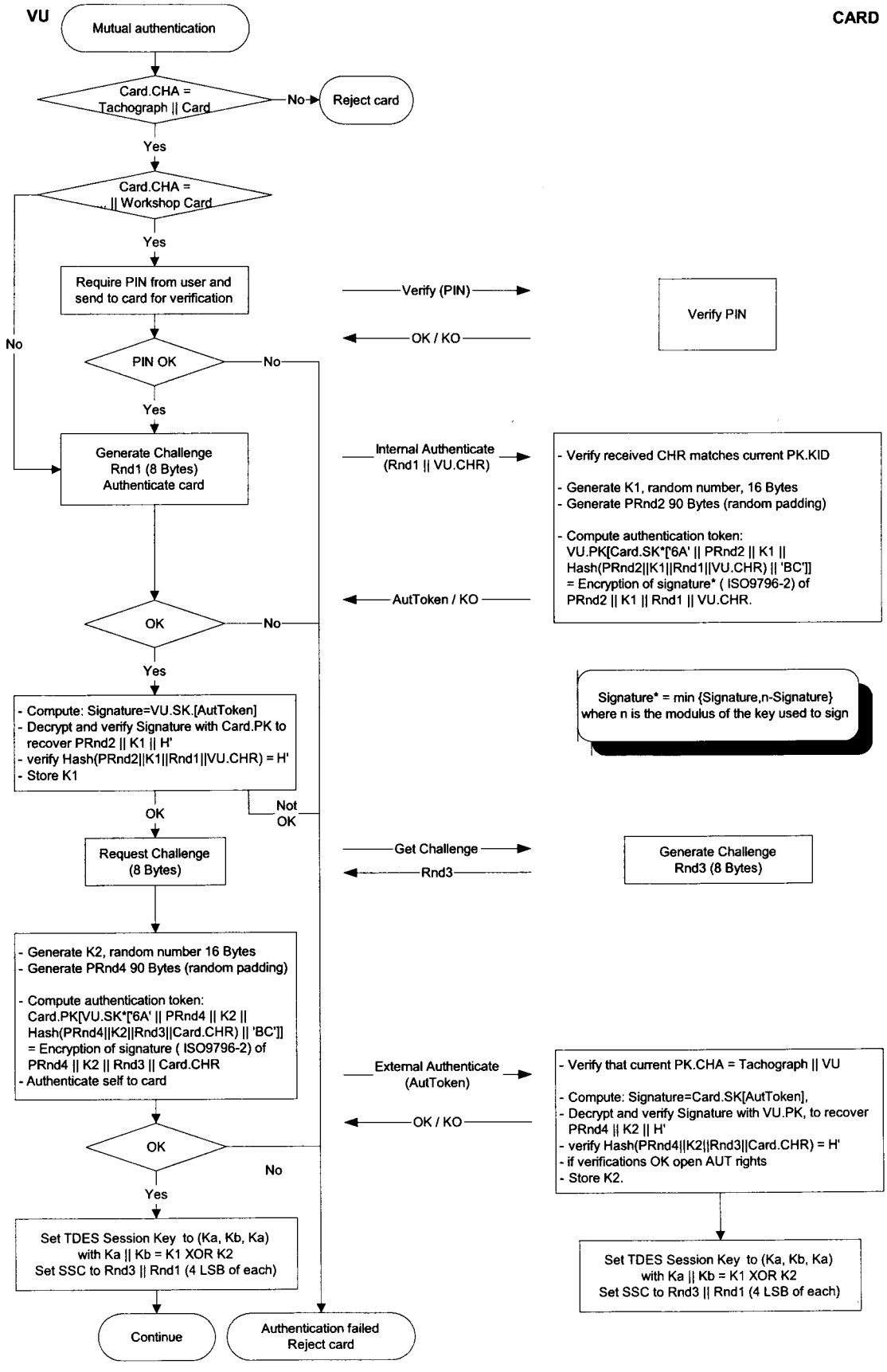
Each party shall demonstrate to the other that it owns a valid key pair, the public key of which has been certified by a Contracting Party certification authority, itself being certified by the European Certification Authority.

Demonstration is made by signing with the private key a random number sent by the other party, who must recover the random number sent when verifying this signature.

The mechanism is triggered at card insertion by the VU. It starts with the exchange of certificates and unwrapping of public keys, and ends with the setting of a session key.

CSM_020 The following protocol shall be used (arrows indicate commands and data exchanged (see sub-appendix 2)):


VU
CARD
Card Insertion
Reset Card
Get card identification
Select Tachograph Application
Card.PK known by VU and Card.C.EOV valid ?
No
Get Card certificate
Card.CA.PK known by VU and Card.CA.C.EOV valid ?
No
Yes
Get Card.CA Certificate
Yes
Verify Card.CA.C with Eur.PK Store Card.CA PK KID CHA and EOV
OK
Verify Card.C with Card.CA.PK Store Card PK KID CHA and EOV
OK
Not OK
Send VU identification to card
VU.PK known to card?
No
Send VU.CA identification to card
VU.CA.PK known to card?
No
Send EUR identification to card
Yes
EUR.PK known to card?
No
Yes
Yes
Send VU.CA Certificate for verification
OK ?
No
Yes
Send VU Certificate for verification
Yes
OK ?
No
Continue with mutual authentication
Reject Card
Reset
ATR
Select File (EF.ICC)
OK
Read Binary (Offset=1, Le=8)
Card.CHR
Select File (Tacho AID)
OK
Select File (EF.Card_Certificate)
OK
Read Binary (Offset=0, Le=194)
Card.C
Select File (EF.CA_Certificate)
OK
Read Binary (Offset=0, Le=194)
Card.CA.C
MSE : SET (VU.KID)
OK / KO
MSE : SET(VU.CA.KID)
OK / KO
MSE : SET(EUR.KID)
OK / KO
Verify Certificate (VU.CA.C)
OK / KO
MSE : SET (VU.CA.KID)
Verify Certificate (VU.C)
OK / KO
MSE : SET (VU.KID)
Select file
Send requested data from selected file
Select Application
Select file
Send requested data from selected file
Select file
Send requested data from selected file
If Key is known, make it the current one
If Key is known, make it the current one
If Key is known, make it the current one
Verify certificate with current PK Store found PK KID and CHA
Verify certificate with current PK Store found PK KID and CHA


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. VU-Cards data transfer confidentiality, integrity and authentication mechanisms

5.1 Secure Messaging

CSM_021 VU-Cards data transfers integrity shall be protected through Secure Messaging in accordance with references [ISO/IEC 7816-4] and [ISO/IEC 7816-8].

CSM_022 When data need to be protected during transfer, a Cryptographic Checksum Data Object shall be appended to the Data Objects sent within the command or the response. The Cryptographic Checksum shall be verified by the receiver.

CSM_023 The cryptographic checksum of data sent within a command shall integrate the command header, and all data objects sent (=>CLA = '0C', and all data objects shall be encapsulated with tags in which b1=1).

CSM_024 The response status-information bytes shall be protected by a cryptographic checksum when the response contains no data field.

CSM_025 Cryptographic checksums shall be 4 Bytes long.

The structure of commands and responses when using secure messaging is therefore the following:

The DOs used are a partial set of the Secure Messaging DOs described in ISO/IEC 7816-4:

Tag	Mnemonic	Meaning
'81'	T_{PV}	Plain Value not BER-TLV coded data (to be protected by CC)
'97'	T_{LE}	Value of Le in the unsecured command (to be protected by CC)
'99'	T_{SW}	Status-Info (to be protected by CC)
'8E'	T_{CC}	Cryptographic Checksum
'87'	$T_{PI\,CG}$	Padding Indicator Byte || Cryptogram (Plain Value not coded in BER-TLV)

Given an unsecured command response pair:

Command header				Command body		
CLA	INS	P1	P2	[L_c field]	[Data field]	[L_e field]
four bytes				L bytes, denoted as B_1 to B_L		

Response body	Response trailer	
[Data field]	SW1	SW2
L_r data bytes	two bytes	

The corresponding secured command response pair is:

Secured command:

Command header (CH)				**Command body**									
CLA	INS	P1	P2	[New L_c field]	[New Data field]								[New L_e field]
'OC'				Length of New Data field	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Data field	'97'	'01'	L_e	'8E'	'04'	CC	

Data to be integrated in checksum = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB
PB = Padding Bytes (80 .. 00) in accordance with ISO-IEC 7816-4 and ISO 9797 method 2.
DOs PV and LE are present only when there is some corresponding data in the unsecured command.

Secured response:

1. Case where response data field is not empty and needs not to be protected for confidentiality:

Response body						**Response trailer**
[New Data field]						new SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Data field	'8E'	'04'	CC	

Data to be integrated in checksum = T_{PV} || L_{PV} || PV || PB

2. Case where response data field is not empty and needs to be protected for confidentiality:

Response body						**Response trailer**
[New Data field]						new SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Data to be carried by CG : non BER-TLV coded data and padding bytes.
Data to be integrated in checksum = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Case where response data field is empty:

Response body						Response trailer
[New Data field]						new SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	New SW1 SW2	'8E'	'04'	CC	

Data to be integrated in checksum = T_{SW} || L_{SW} || SW || PB

5.2 Treatment of Secure Messaging errors

CSM_026 When the tachograph card recognises an SM error while interpreting a command, then the status bytes must be returned without SM. In accordance with ISO/IEC 7816-4, the following status bytes are defined to indicate SM errors:

'66 88': Verification of Cryptographic Checksum failed,

'69 87': Expected SM Data Objects missing,

'69 88': SM Data Objects incorrect.

CSM_027 When the tachograph card returns status bytes without SM DOs or with an erroneous SM DO, the session must be aborted by the VU.

5.3 Algorithm to compute Cryptographic Checksums

CSM_028 Cryptographic checksums are built using a retail MACs in accordance with ANSI X9.19 with DES:

- Initial stage: The initial check block y0 is E(Ka, SSC).
- Sequential stage: The check blocks y1, .. , yn are calculated using Ka.
- Final stage: The cryptographic checksum is calculated from the last check block yn as follows: E(Ka, D(Kb, yn)).

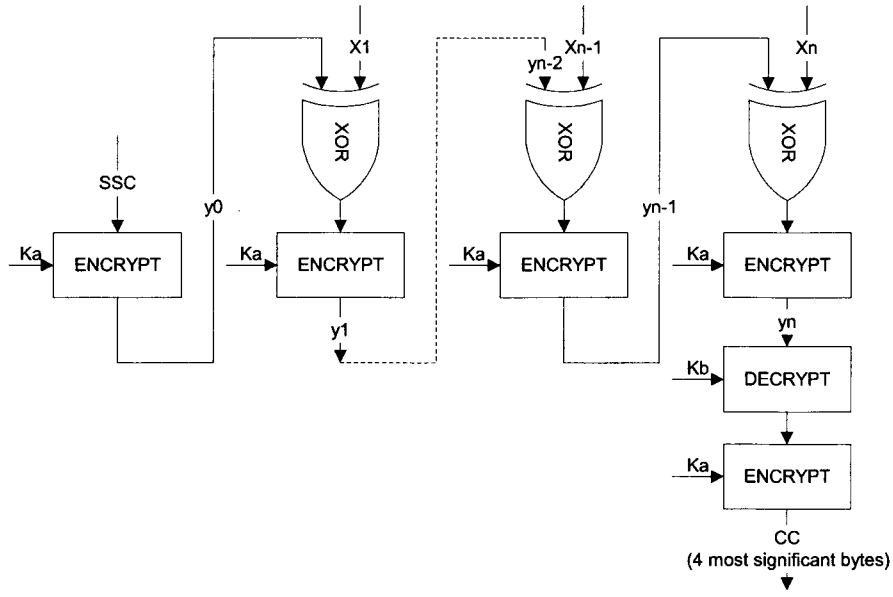
where E() means encryption with DES, and D() means decryption with DES.

The four most significant bytes of the cryptographic checksum are transferred

CSM_029 The Send Sequence Counter (SSC) shall be initiated during key agreement procedure to:
Initial SSC: Rnd3 (4 least significant bytes) || Rnd1 (4 least significant bytes).

CSM_030 The Send Sequence Counter shall be increased by 1 each time before a MAC is calculated (i.e. the SSC for the first command is Initial SSC + 1, the SSC for the first response is Initial SSC + 2).

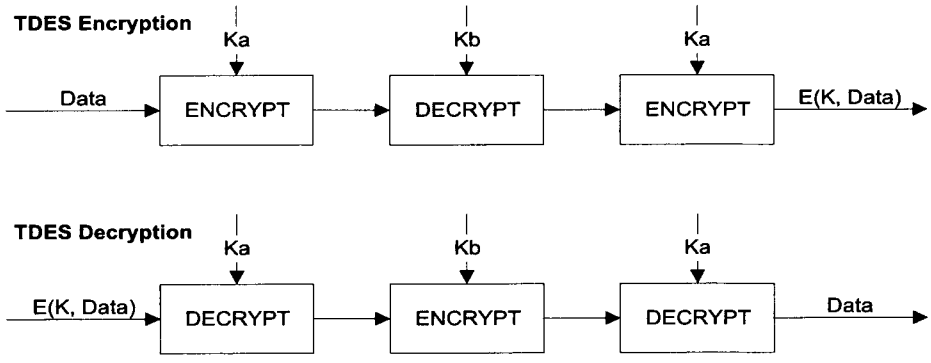
The following figure shows the calculation of the retail MAC:



5.4 Algorithm to compute cryptograms for confidentiality DOs

CSM_031 Cryptograms are computed using TDEA in TCBC mode of operation in accordance with references [TDES] and [TDES-OP] and with the Null vector as Initial Value block.

The following figure shows the application of keys in TDES:



6. Data download digital signature mechanisms

CSM_032 The Intelligent Dedicated Equipment (IDE) stores data received from an equipment (VU or card) during one download session within one physical data file. This file must contain the certificates $CP_i.C$ and EQT.C. The file contains digital signatures of data blocks as specified in sub-appendix 7 (Data Downloading Protocols).

CSM_033 Digital signatures of downloaded data shall use a digital signature scheme with appendix such, that downloaded data may be read without any decipherment if desired.

6.1 Signature generation

CSM_034 Data signature generation by the equipment shall follow the signature scheme with appendix defined in reference [PKCS1] with the SHA-1 hash function :

Signature = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(Data))]

PS = Padding string of octets with value 'FF' such that length is 128.

DER(SHA-1(*M*)) is the encoding of the algorithm ID for the hash function and the hash value into an ASN.1 value of type `DigestInfo` (distinguished encoding rules):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hash Value.

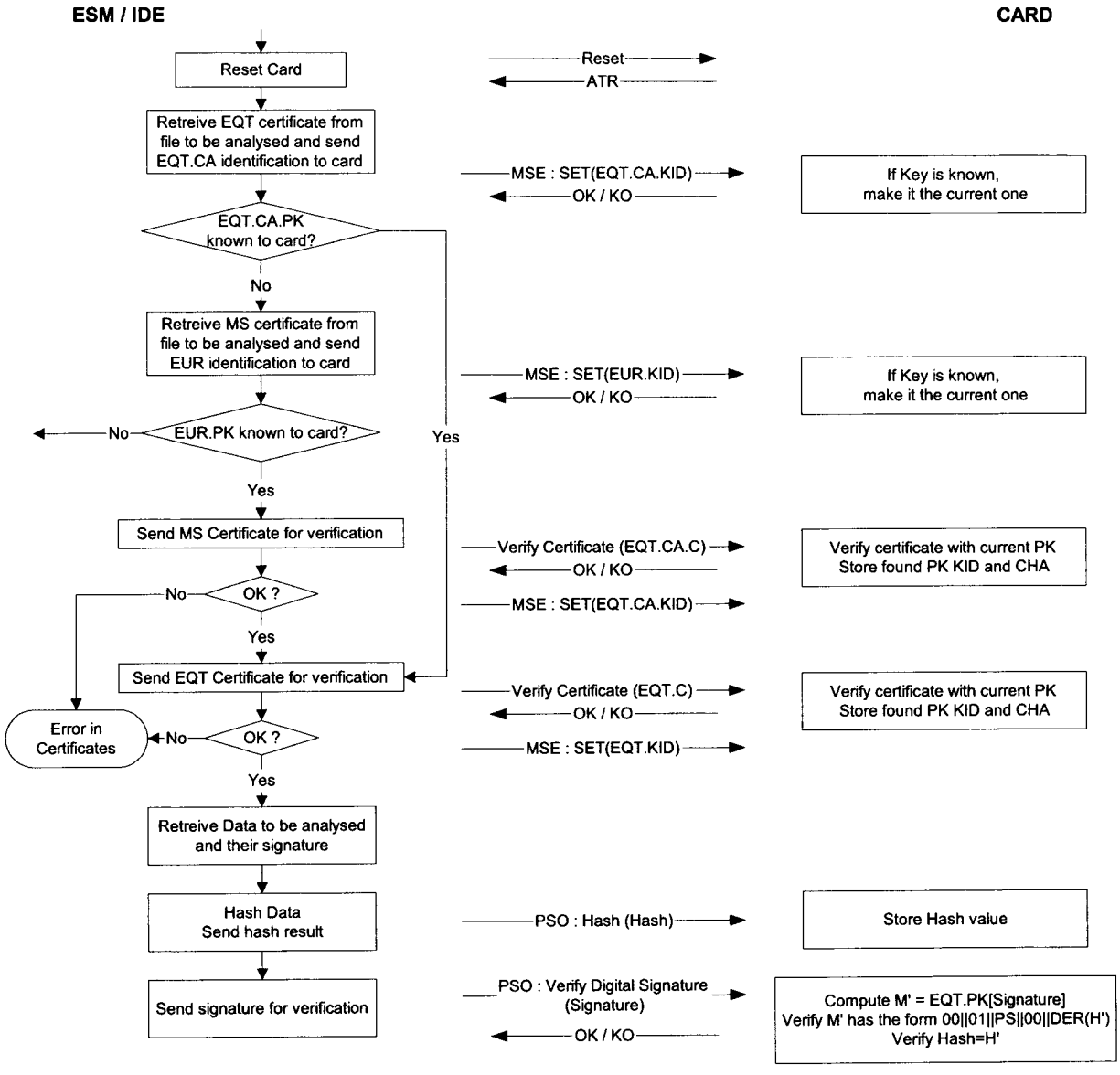
6.2 Signature verification

CSM_035 Data signature verification on downloaded data shall follow the signature scheme with appendix defined in reference [PKCS1] with the SHA-1 hash function.

The European public key EUR.PK needs to be known independently (and trusted) by the verifier.

The following table illustrates the protocol an IDE carrying a Control card can follow to verify the integrity of data downloaded and stored on the ESM (External Storage media). The control card is used to perform the decipherement of digital signatures. This function may in this case not be implemented in the IDE.

The equipment that has downloaded and signed the data to be analysed is denoted EQT.


ESM / IDE
CARD
Reset Card
Reset
ATR
Retreive EQT certificate from file to be analysed and send EQT.CA identification to card
MSE : SET(EQT.CA.KID)
OK / KO
If Key is known, make it the current one
EQT.CA.PK known to card?
No
Retreive MS certificate from file to be analysed and send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
No
EUR.PK known to card?
Yes
Yes
Send MS Certificate for verification
Verify Certificate (EQT.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
No
OK ?
MSE : SET(EQT.CA.KID)
Yes
Send EQT Certificate for verification
Verify Certificate (EQT.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Error in Certificates
No
OK ?
MSE : SET(EQT.KID)
Yes
Retreive Data to be analysed and their signature
Hash Data
Send hash result
PSO : Hash (Hash)
Store Hash value
Send signature for verification
PSO : Verify Digital Signature (Signature)
OK / KO
Compute M' = EQT.PK[Signature]
Verify M' has the form 00||01||PS||00||DER(H')
Verify Hash=H'

- - - - -

ДОБАВЛЕНИЕ 1В К ПРИЛОЖЕНИЮ ЕСТР

ТРЕБОВАНИЯ К КОНСТРУКЦИИ, ИСПЫТАНИЯМ, УСТАНОВКЕ И ИНСПЕКЦИИ ЦИФРОВОГО КОНТРОЛЬНОГО УСТРОЙСТВА, ИСПОЛЬЗУЕМОГО НА АВТОМОБИЛЬНОМ ТРАНСПОРТЕ

(Сводный вариант)

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

Стр.

ПОДРАЗДЕЛЫ

I. ОПРЕДЕЛЕНИЯ

В настоящем приложении:

a) **"активация" означает:**

режим, в котором контрольное устройство становится полностью работоспособным и выполняет все функции, в том числе функции защиты;

Активация контрольного устройства производится с использованием карточки предприятия и присвоенного ей PIN-кода.

b) **"аутентификация" означает:**

функция, имеющая целью установить и проверить идентичность введенных данных;

c) **"аутентичность" означает:**

параметр, подтверждающий, что соответствующая информация вводится стороной, идентификационные данные которой могут быть проверены;

d) **"встроенная система проверки (BIT)" означает:**

проверки, производимые по команде, данной оператором или соответствующим внешним устройством;

e) **"календарный день" означает:**

сутки в интервале от 00:00 часов до 24:00 часов. Все календарные дни определяются по системе универсального времени (время UTC);

f) **"калибровка" означает:**

обновление или подтверждение параметров транспортного средства, которые должны храниться в блоке памяти. Параметры транспортного средства включают идентификационные данные транспортного средства (VIN, VRN и Договаривающейся стороны регистрации) и характеристики транспортного средства (w, k, l, размер шин, параметры регулировки устройства ограничения скорости

(в случае применимости), текущее время UTC, текущие показания счетчика пробега);

Калибровка контрольного устройства предполагает необходимость использования карточки предприятия.

g) **"номер карточки" означает:**

номер в виде 16 буквенно-цифровых знаков, который однозначно идентифицирует карточку тахографа в данной Договаривающейся стороне. Номер карточки включает порядковый индекс (в случае применимости), индекс замены и индекс возобновления;

Таким образом карточка однозначно идентифицируется с помощью кода выдавшей ее Договаривающейся стороны и номера карточки.

h) **"порядковый индекс карточки" означает:**

14-й буквенно-цифровой знак номера карточки, который используется для дифференциации различных карточек, выданных соответствующему предприятию или органу, которые имеют право на получение нескольких карточек тахографа. Данное предприятие или орган однозначно идентифицируются с помощью первых 13 знаков номера карточки;

i) **"индекс возобновления карточки" означает:**

16-й буквенно-цифровой знак номера карточки, который увеличивается в каждом случае возобновления карточки;

j) **"индекс замены карточки" означает:**

15-й буквенно-цифровой знак номера карточки, который увеличивается в каждом случае замены карточки тахографа;

k) **"характеристический коэффициент транспортного средства" означает:**

числовая характеристика, придающая соответствующее значение выходному сигналу, подаваемому компонентом транспортного средства, связывающим его с контрольным устройством (вторичный вал коробки передач или ось) после пробега

транспортным средством расстояния в 1 км в стандартных условиях испытания (см. главу VI-5). Характеристический коэффициент выражается в импульсах на километр (w = ... имп./км);

l) **"карточка предприятия" означает:**

карточка тахографа, выданная компетентными органами Договаривающейся стороны владельцу или держателю транспортных средств, оснащенных контрольными устройствами;

Карточка предприятия идентифицирует предприятие и позволяет выводить на дисплей, загружать и распечатывать данные, хранящиеся в контрольном устройстве, на котором была установлена блокировка данным предприятием.

m) **"постоянная контрольного устройства" означает:**

числовая характеристика, придающая соответствующее значение входному сигналу, который необходим для просмотра и регистрации расстояния пробега в 1 км; эта постоянная выражается в импульсах на километр (k = ... имп./км)

n) **"продолжительность управления", рассчитываемая контрольным устройством**[1], означает непрерывное время управления транспортным средством, рассчитываемое в качестве суммы накопленного времени управления конкретным водителем с момента завершения его последнего периода ГОТОВНОСТЬ (AVAILABILITY) или ПЕРЕРЫВ/ОТДЫХ (BREAK/REST) или НЕТ ДАННЫХ (UNKNOWN)[2] продолжительностью 45 мин. или более (этот период может разбиваться на несколько периодов продолжительностью 15 мин. или более). В процессе этих расчетов учитываются, при необходимости, данные о прошлых видах деятельности, записанные в карточке водителя. Если водитель не вставил свою карточку, расчеты производятся на основе записанных данных, которые

---

[1] Этот способ расчета продолжительности управления и совокупной продолжительности времени перерывов используется контрольным устройством для расчета времени подачи предупредительного сигнала, указывающего на непрерывное время вождения. Он не предопределяет правовое толкование этих периодов времени.

[2] Периоды "НЕТ ДАННЫХ" соответствуют периодам, в течение которых карточка водителя не была вставлена в контрольное устройство и в отношении которых ручной ввод данных водителем о своей деятельности произведен не был.

относятся к текущему периоду времени, в течение которого карточка не вставлялась, и к соответствующему считывающему устройству;

o) **"карточка контролера" означает:**

карточка тахографа, выданная властями Договаривающейся стороны национальному компетентному контрольному органу;

Карточка контролера позволяет идентифицировать контрольный орган и, при возможности, сотрудника контрольного органа и открыть доступ к данным, хранящимся в блоке памяти, или в карточках водителя, для их просмотра, распечатки и/или загрузки.

p) **"совокупное время перерывов", рассчитываемое контрольным устройством, означает:**

совокупная продолжительность перерывов в течение всего времени управления, рассчитываемая в качестве совокупных периодов ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ или НЕТ ДАННЫХ[2] продолжительностью 15 мин. или более применительно к конкретному водителю с момента завершения его последнего периода ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ или НЕТ ДАННЫХ[2] продолжительностью 45 мин. или более (этот период может разбиваться на несколько периодов продолжительностью 15 мин. или более).

В процессе расчета учитываются, при необходимости, данные о прошлых видах деятельности, записанных на карточке водителя. Периоды, за которые нет данных и продолжительность которых отображается знаком "минус" (начало периода, за который нет данных, наступившее раньше завершения этого же периода), что обусловлено нестыковкой во времени между двумя различными контрольными устройствами, в процессе расчета не учитываются.

Если водитель не вставил карточку, расчет производится на основе данных, записанных в блоке памяти и относящихся к периоду, в течение которого карточка вставлена не была, и к соответствующему считывающему устройству.

q) **"блок памяти" означает:**

электронное устройство хранения данных, встроенное в контрольное устройство;

r) **"цифровая подпись" означает:**

данные, прилагаемые к массиву данных, или криптографическое преобразование этого массива, которые позволяют лицу, получившему доступ к этому массиву данных, подтвердить его аутентичность и целостность;

s) **"загрузка" означает:**

копирование вместе с цифровой подписью части или всего массива данных, записанных в блоке памяти транспортного средства или в блоке памяти карточки тахографа;

Загрузка не должна приводить к изменению или стиранию каких бы то ни было записанных данных.

t) **"карточка водителя" означает:**

карточка тахографа, выданная властями Договаривающейся стороны конкретному водителю;

Карточка водителя позволяет идентифицировать водителя и хранить данные о деятельности водителя.

u) **"эффективная окружность шин" означает:**

среднее значение расстояний, пройденных каждым из колес, приводящих в движение транспортное средство (ведущими колесами) за один полный оборот. Измерение этих расстояний производится в нормальных условиях испытания (глава VI-5) и выражается в виде "l = ... мм". Изготовители транспортных средств могут использовать вместо фактического измерения этого расстояния теоретический метод расчета, который учитывает распределение веса на оси транспортного средства в снаряженном состоянии без груза[3]. Методы такого теоретического расчета утверждаются компетентным органом Договаривающейся стороны;

---

[3] Измерение расстояний производится в соответствии с положениями директивы Совета № 97/27/EC от 22 июля 1997 года, касающейся массы и габаритов некоторых категорий автотранспортных средств и их прицепов и изменяющей директиву 70/156/EEC (OJ No. L 233, 25.08.97).

v) **"событие" означает:**

сбой в работе, обнаруженный контрольным устройством, который может быть вызван попыткой фальсификации;

w) **"неисправность" означает:**

сбой в работе, обнаруженный контрольным устройством, который может быть обусловлен неисправностью или выходом из строя устройства;

x) **"установка" означает:**

установка контрольного устройства на транспортном средстве;

y) **"датчик движения" означает:**

компонент контрольного устройства, подающий сигнал, который отображает скорость транспортного средства и/или пройденное расстояние;

z) **"карточка недействительна" означает:**

карточка, которая определена в качестве неисправной, или которую не удалось идентифицировать, или срок действия которой еще не наступил, или срок действия которой уже истек;

aa) **"неприменимо" означает:**

случай, когда использовать контрольное устройство в соответствии с положениями настоящего Соглашения не требуется;

bb) **"превышение скорости" означает:**

превышение разрешенной скорости транспортного средства, определяемое в качестве любого периода продолжительностью более 60 сек., в течение которого

измеренная скорость транспортного средства превышает предельное значение, на которое отрегулировано устройство ограничения скорости[4];

cc) "периодическая инспекция" означает:

ряд операций, выполняемых в целях проверки надлежащей работы контрольного устройства и соответствия его регулировки параметрам транспортного средства;

dd) "печатающее устройство" означает:

компонент контрольного устройства, который позволяет распечатывать записанные данные;

ee) "контрольное устройство" означает:

комплект оборудования, предназначенный для установки на автотранспортных средствах в целях просмотра, регистрации и хранения в автоматическом и полуавтоматическом режиме данных о движении таких транспортных средств и некоторых периодах работы их водителей;

ff) "возобновление" означает:

выдача новой карточки тахографа, когда срок действия используемой карточки подходит к концу или когда она обнаруживает сбой в работе и возвращена выдавшему ее органу. Возобновление всегда однозначно указывает на то, что две действующие карточки одновременно использоваться не могут;

gg) "ремонт" означает:

любой ремонт датчика движения или бортового устройства, который предполагает необходимость его отсоединения от источника питания или от любого другого компонента контрольного устройства или его вскрытие;

---

[4] Предельное значение регулировки устройства ограничения скорости соответствует положениям директивы Совета № 92/6/ЕС от 10 февраля 1992 года, касающейся установки и использования устройства ограничения скорости некоторых категорий автотранспортных средств в Сообществе (OJ No. L 057, 02/03/1992).

hh) "замена" означает:

выдача карточки тахографа вместо существующей карточки, которая, на основании полученного заявления, была потеряна, похищена или давала сбои в работе и не была возвращена выдавшему ее органу. Замена всегда предполагает наличие риска существования в одно и то же время двух действующих карточек;

ii) "сертификация защиты" означает:

процесс подтверждения сертифицирующим органом[5], что контрольное устройство (или компонент) или карточка тахографа, подвергаемые контролю, выполняют требования в отношении защиты, определенные в подразделе 10 "Общие контрольные показатели защиты";

jj) "самопроверка" означает:

проверки, производимые на периодической основе и в автоматическом режиме контрольным устройством на предмет обнаружения неисправностей;

kk) "карточка тахографа" означает:

карточку со встроенной микросхемой, предназначенной для использования в контрольном устройстве. Карточки тахографа позволяют контрольному устройству проверить идентификационные данные держателя карточки (или идентификационные данные соответствующей группы) и передавать и хранить данные. Карточки тахографов могут быть следующего вида:

- карточка водителя,
- карточка контролера,
- карточка мастерской,
- карточка предприятия;

---

[5] Положения, регламентирующие защиту, соответствуют положениям, изложенным в рекомендации Совета 95/144/CE от 7 апреля 1995 года, касающейся общих критериев оценки безопасности информационных технологий (O.J. No. L093, 26/04/1995).

ll) "официальное утверждение типа" означает:

процесс подтверждения Договаривающейся стороной того факта, что данное контрольное устройство (или компонент) или карточка тахографа, подвергаемые проверке, удовлетворяют требованиям ЕСТР;

mm) "размер шины" означает:

обозначение размеров шин (внешних ведущих колес) в соответствии с Правилами ЕЭК № 54[6];

nn) "идентификация транспортного средства" означает:

номера, идентифицирующие транспортное средство: номер регистрации транспортного средства (VRN) с указанием Договаривающейся стороны регистрации и опознавательный номер транспортного средства (VIN)[7];

oo) "бортовое устройство (БУ)" означает:

контрольное устройство, за исключением датчика движения и электропроводки для подсоединения датчика движения. Бортовое устройство может представлять собой либо единое устройство, либо несколько устройств, установленных в различных местах транспортного средства, при условии что оно соответствует требованиям ЕСТР в отношении защиты;

pp) "неделя" для целей расчетов, производимых контрольным устройством, означает:

период с 00:00 часов UTC в понедельник до 24:00 часов UTC в воскресенье;

---

[6] Исходным текстом, действующим в ЕС, является директива 92/23/EEC от 31 марта 1992 года, касающаяся шин автотранспортных средств и их прицепов и их установки (OJ No. L 129, 14/05/1992).

[7] Идентификация транспортного средства соответствует положениям директивы Совета № 76/114/EEC от 18 декабря 1975 года, касающейся сближения законодательства государств-членов, регламентирующего предусмотренные таблички с данными и маркировку автотранспортных средств и их прицепов и местоположение и метод их нанесения (OJ, No. L 24, 30/01/1976).

qq) "карточка мастерской" означает:

карточка тахографа, выданная властями Договаривающейся стороны изготовителю контрольного устройства, механику, изготовителю транспортного средства или мастерской, уполномоченных данной Договаривающейся стороной.

Карточка мастерской позволяет идентифицировать держателя карточки и производить проверку, калибровку и/или загрузку данных с контрольного устройства.

II. ОБЩИЕ ХАРАКТЕРИСТИКИ И ФУНКЦИИ КОНТРОЛЬНОГО УСТРОЙСТВА

000 Любое транспортное средство, оснащенное контрольным устройством, удовлетворяющим положениям настоящего добавления, должно быть оборудовано спидометром и счетчиком пробега. Эти функции могут быть включены в контрольное устройство.

1. Общие характеристики

Цель контрольного устройства состоит в регистрации, хранении, отображении, распечатке и генерации данных о деятельности водителя.

001 Контрольное устройство включает электропроводку, датчик движения и бортовое устройство.

002 Бортовое устройство включает устройство обработки данных, блок памяти, часы, работающие в реальном масштабе времени, два интерфейса для карточек с встроенной микросхемой (для водителя и второго водителя), печатающее устройство, дисплей, систему визуального предупреждения, калибровочный/ загрузочный разъем и устройство ввода данных пользователем.

Контрольное устройство может подсоединяться к другим устройствам с помощью дополнительных разъемов.

003 Любое включение или подсоединение к контрольному устройству любой функции, устройства или устройств, сертифицированных или не сертифицированных, не должно нарушать или создавать помехи, которые могут нарушить надлежащую и безопасную работу контрольного устройства и привести к нарушению положений настоящего Соглашения.

Пользователи контрольного устройства вводят свои идентификационные данные в данное устройство с помощью карточек тахографа.

004 Контрольное устройство предоставляет право селективного доступа к данным и функциям в зависимости от вида и/или идентификационных данных пользователя.

Контрольное устройство регистрирует и хранит данные в блоке памяти и в карточках тахографа.

Эти функции выполняются в соответствии с Европейскими положениями, регламентирующими защиту частных лиц в части обработки личных данных и беспрепятственной передачи таких данных[8].

2. Функции

005 Контрольное устройство должно выполнять следующие функции:

- контроль за вводом и извлечением карточек,
- измерение скорости и пробега,
- измерение времени,
- контроль за деятельностью водителя,
- контроль за статусом управления,
- различные виды ручного ввода данных:
  - ввод данных о местах, в которых начинаются или заканчиваются еще дневные периоды работы,
  - ручной ввод данных о деятельности водителя,
  - ввод данных об особых ситуациях,
- реагирование на блокировку, установленную предприятием,
- контроль за операциями по проверке,
- обнаружение соответствующих событий и/или неисправностей,
- проведение проверки и самопроверки,
- считывание данных из блока памяти,
- регистрация и хранение данных в блоке памяти,
- считывание данных с карточек тахографа,

---

[8] Защита частных лиц в части обработки личных данных и беспрепятственной передачи таких данных соответствует положениям Директивы Совета № 95/46/ЕС от 24 октября 1995 года с включенными в нее последними поправками (OJ, No. L 281, 23/11/1995).

- регистрация и хранение данных в карточках тахографа,
- вывод данных на дисплей,
- распечатка,
- предупреждение,
- загрузка данных на внешние носители,
- вывод данных на дополнительные внешние устройства,
- калибровка,
- корректировка времени.

3. Режимы работы

006 Контрольное устройство должно иметь четыре режима работы:

- рабочий режим,
- режим контроля,
- режим калибровки,
- режим предприятия.

007 Контрольное устройство должно переходить в следующий режим работы в соответствии с действующими карточками тахографа, вставленными в считывающее устройство карточки:

Режим работы		Считывающее устройство "Водитель"				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена	Рабочий	Рабочий	Контроль	Калибровка	Предприятие
	Карточка водителя	Рабочий	Рабочий	Контроль	Калибровка	Предприятие
	Карточка контролера	Контроль	Контроль	Контроль*	Рабочий	Рабочий
	Карточка мастерской	Калибровка	Калибровка	Рабочий	Калибровка*	Рабочий
	Карточка предприятия	Предприятие	Предприятие	Рабочий	Рабочий	Предприятие*

008 * В этих случаях контрольное устройство будет использовать только карточку тахографа, вставленную в считывающее устройство "Водитель".

009 Контрольное устройство не реагирует на вставленные недействительные карточки, за исключением вывода на дисплей, на печать или загрузки данных, содержащихся на карточке, срок действия которой истек. Эти функции должны быть возможны.

010 Все функции, перечисленные в пункте II.2, должны работать во всех режимах с учетом следующих исключений:

- функция калибровки доступна только в режиме калибровки,
- функция корректировки времени ограничена, за исключением режима калибровки,
- функции ручного ввода данных водителем доступны только в рабочем режиме или режиме калибровки,
- функция блокировки, производимой предприятием, доступна только в режиме предприятия,
- функция контроля операций по проверке работает только в режиме контроля,
- функция загрузки данных в рабочем режиме недоступна (за исключением случая, предусмотренного требованием 150).

011 Контрольное устройство может выводить любые данные на дисплей, печать или на внешние интерфейсы с учетом следующих исключений:

- в рабочем режиме любые личные идентификационные данные (фамилия и имя (имена), не соответствующие данным на вставленной карточке тахографа, должны гаситься, а любой номер карточки, не соответствующий данным на вставленной карточке тахографа, должен гаситься частично (должен гаситься каждый нечетный знак слева направо),
- в режиме предприятия данные, касающиеся водителя (требования 081, 084 и 087), могут выводиться только в течение периодов, когда они не заблокированы другим предприятием (идентифицируемым с помощью первых 13 цифр номера карточки предприятия),

- когда в контрольное устройство карточка не вставлена, данные, касающиеся водителя, могут выводиться только за текущий и восемь предыдущих календарных дней.

4. Защита

Система защиты имеет целью предохранить блок памяти от несанкционированного доступа к зарегистрированным данным и их манипуляции и регистрировать любые случаи таких попыток, предохранить целостность и аутентичность данных, передаваемых по каналу связи между датчиком движения и бортовым устройством, предохранить целостность и аутентичность данных, передаваемых по каналу связи между контрольным устройством и карточками тахографа, и проверять целостность и аутентичность загружаемых данных.

012 В целях обеспечения защиты системы контрольное устройство должно удовлетворять требованиям, предъявляемым к защите, которые предусмотрены общими контрольными показателями защиты датчика движения и бортового устройства (подраздел 10).

III. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КОНТРОЛЬНОГО УСТРОЙСТВА

1. Контроль за вводом и извлечением карточек

013 Контрольное устройство должно контролировать интерфейс для считки карточек в целях обнаружения факта ввода и извлечения карточки.

014 После ввода карточки контрольное устройство должно установить, является ли вставленная карточка действующей карточкой тахографа, и определить тип карточки.

015 Контрольное устройство должно быть сконструировано таким образом, чтобы карточки тахографов, после того как они были надлежащим образом вставлены в интерфейс для считки каточек, блокировались в нем в правильном положении.

016 Извлечение карточки тахографа должно быть возможным только в случае остановки транспортного средства и после записи соответствующих данных в память карточки. Извлечение карточки производится посредством преднамеренного действия пользователя.

2. Измерение скорости и пробега

017 Эта функция должна обеспечивать постоянное измерение и указывать величину пробега, соответствующего полному расстоянию, пройденному транспортным средством.

018 Эта функция должна обеспечивать постоянное измерение и указывать значение скорости транспортного средства.

019 Функция измерения скорости также обеспечивает информацию, указывающую на то, что транспортное средство движется или остановлено. Транспортное средство считается движущимся в том случае, если эта функция обнаруживает сигнал величиной 1 имп./с в течение как минимум 5 секунд, передаваемый датчиком движения; в противном случае транспортное средство считается остановленным.

Устройства, показывающие скорость (спидометр) и общее пройденное расстояние (счетчик пробега), установленные на любом транспортном средстве, оснащенном контрольным устройством, соответствующим положениям настоящего Соглашения,

должны удовлетворять требованиям, касающимся максимальных допусков, указанных в настоящем добавлении (главы III.2.1 и III.2.2).

2.1 Измерение пробега

020 Пробег может измеряться таким образом:

- чтобы он включал суммарное перемещение как вперед, так и назад или
- чтобы он включал только перемещение вперед.

021 Контрольное устройство должно иметь возможность измерять расстояние от 0 до 9 999 999,9 км.

022 Пробег должен измеряться с соблюдением следующих допусков (расстояния не менее 1 000 м):

- ± 1% до установки,
- ± 2% при установке и периодических инспекциях,
- ± 4% в процессе эксплуатации.

023 Пробег должен измеряться с точностью не менее 0,1 км.

2.2 Измерение скорости

024 Контрольное устройство должно обеспечивать измерение скорости в диапазоне от 0 до 220 км/ч.

025 В целях обеспечения максимального допуска на показываемую скорость на уровне ± 6 км/ч в процессе эксплуатации и с учетом:

- допуска ± 2 км/ч на разброс входных данных (разброс, обусловленный шинами, …),

- допуска ± 1 км/ч на измерения, производимые во время установки или периодических инспекций,

контрольное устройство должно обеспечивать, в диапазоне скоростей от 20 до 180 км/ч, и специфических коэффициентов транспортного средства от 4 000

до 25 000 имп./км, измерение скорости с точностью ± 1 км/ч (при постоянной скорости).

Примечание: Точность хранения данных обуславливает дополнительный допуск на данные скорости, регистрируемой контрольным устройством, на уровне ± 0,5 км/ч.

025a Скорость должна измеряться правильно в пределах нормальных допусков в течение 2 секунд с момента завершения фазы изменения скорости, в условиях, когда показатель изменения скорости составляет не более 2 м/с^2.

026 Точность измерения скорости должна составлять не менее 1 км/ч.

3. Измерение времени

027 Функция измерения времени должна обеспечивать постоянное измерение времени и цифровое отображение даты и времени UTC.

028 Дата и время UTC должны использоваться для датирования всех операций, осуществляемых контрольным устройством (регистрация, распечатка, обмен данными, вывод на дисплее, …).

029 Для визуализации местного времени необходимо предусмотреть возможность изменения разницы в выводимом на дисплей времени с помощью получасовых интервалов.

030 Отклонение времени не должно превышать ± 2 секунды в день в условиях, предусмотренных для официального утверждения типа.

031 Точность измерения времени должна составлять не менее 1 секунды.

032 Измерение времени не должно нарушаться в результате прекращения электропитания от внешнего источника в течение менее 12 месяцев в условиях, предусмотренных для официального утверждения типа.

4. Контроль за деятельностью водителя

033 Эта функция должна обеспечивать постоянный и отдельный контроль за деятельностью одного водителя и одного второго водителя.

034 Деятельность водителя должна включать DRIVING, WORK, AVAILABILITY или BREAK/REST (УПРАВЛЕНИЕ, РАБОТА, ГОТОВНОСТЬ ИЛИ ПЕРЕРЫВ/ОТДЫХ).

035 Водитель и/или второй водитель должны иметь возможность выбирать вручную функцию WORK, AVAILABILITY или BREAK/REST (РАБОТА, ГОТОВНОСТЬ ИЛИ ПЕРЕРЫВ/ОТДЫХ).

036 Когда транспортное средство движется, функция DRIVING (УПРАВЛЕНИЕ) выбирается автоматически в случае водителя, а функция AVAILABILITY (ГОТОВНОСТЬ) выбирается автоматически в случае второго водителя.

037 Когда транспортное средство останавливается, в случае водителя автоматически выбирается функция WORK (РАБОТА).

038 Считается, что первое изменение вида деятельности в течение 120 секунд после автоматического переключения на функцию WORK (РАБОТА) в связи с остановкой транспортного средства производится в момент остановки транспортного средства (что может предполагать отмену перехода на функцию РАБОТА.

039 Эта функция должна обеспечивать передачу данных об изменении вида деятельности в устройство регистрации с интервалом в одну минуту.

040 Если в течение данной календарной минуты регистрируется факт деятельности DRIVING (УПРАВЛЕНИЕ), то вся эта минута регистрируется как УПРАВЛЕНИЕ.

041 Если применительно к данной календарной минуте любая деятельность, относящаяся к категории УПРАВЛЕНИЯ, зарегистрирована непосредственно до этой минуты или сразу же после нее, то вся эта минута зачитывается как УПРАВЛЕНИЕ.

042 Если данная календарная минута не зачитывается в соответствии с предыдущими требованиями в качестве УПРАВЛЕНИЯ, то вся эта минута зачитывается в качестве того же вида деятельности, что и деятельность, которая осуществлялась непрерывно дольше всего в течение этой минуты (или самая последняя в случае нескольких видов деятельности одинаковой продолжительности).

043 Эта функция также обеспечивает постоянный контроль за непрерывным временем управления и совокупным временем перерывов в работе водителя.

5. Контроль за управлением

044 Эта функция обеспечивает постоянный и автоматический контроль за статусом управления.

045 Если в устройство вставляются две действительные карточки водителя, то регистрируется статус управления GREW (ЭКИПАЖА), а во всех других случаях регистрируется статус управления SINGE (ОДИН).

6. Ввод данных водителем вручную

6.1 Ввод названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы

046 Эта функция позволяет вводить названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы водителя и/или второго водителя.

047 Места определяются в виде названия страны и дополнительно, в случае применимости, названия района.

048 В момент извлечения карточки водителя (или мастерской) контрольное устройство предлагает второму водителю ввести "название места, в котором заканчивается ежедневный период работы" (place where the daily work period ends).

049 Контрольное устройство должно давать возможность игнорировать это предложение.

050 Должна быть предусмотрена возможность ввода названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, без карточки или в другое время, помимо моментов ввода и извлечения карточки.

6.2 Ручной ввод водителем данных о своей деятельности

050a После ввода карточки водителя (или мастерской) и только в этот момент контрольное устройство должно:

– напомнить держателя карточки дату и время последнего извлечения им своей карточки и

– предложить держателя карточки указать, означает ли данный ввод карточки продолжение текущего ежедневного периода работы.

Контрольное устройство должно давать возможность держателя карточки игнорировать данный вопрос, не отвечая на него или отвечая положительно или отрицательно:

– В том случае, если держатель карточки игнорирует вопрос, контрольное устройство предлагает держателю карточки указать "название места, в котором начинается ежедневный период работы" (place where the daily work period begins). Контрольное устройство должно давать возможность игнорировать это предложение. Если название места введено, то оно регистрируется в блоке памяти и в карточке тахографа с указанием времени ввода карточки

– В случае отрицательного или положительного ответа контрольное устройство должно предложить держателю карточки ввести данные о деятельности вручную с указанием дат и времени начала и завершения этой деятельности только из числа следующих видов деятельности: WORK, AVAILABILITY или BREAK/REST (РАБОТА, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ), которые должны строго относиться только к периоду между моментом последнего извлечения карточки и моментом нынешнего ввода, не допуская при этом накладок таких видов деятельности. Это должно производиться в соответствии со следующими процедурами:

– В том случае, если держатель карточки утвердительно отвечает на указанный вопрос, контрольное устройство предлагает держателю карточки ввести вручную данные о деятельности в хронологическом порядке за период между моментом последнего извлечения карточки и текущим моментом ввода. Этот процесс заканчивается, когда время завершения деятельности, введенное вручную, соответствует времени ввода карточки.

– В том случае, если держатель карточки отвечает отрицательно на указанный вопрос, контрольное устройство:

  – предлагает держателю карточки ввести данные о деятельности вручную в хронологическом порядке с момента извлечения карточки до момента завершения соответствующего ежедневного периода работы (или деятельности, относящейся к данному транспортному средству в том

случае, если продолжение ежедневного периода работы записывается на регистрационном листке). В этом случае контрольное устройство, прежде чем предложить держателю карточки ввести данные о каждом виде деятельности вручную, предлагает ему указать, является ли время завершения последней зарегистрированной деятельности временем завершения предыдущего периода работы (см. примечание ниже),

Примечание: В том случае, если держатель карточки не указывает, когда завершился предыдущий период работы, и вводит вручную данные о деятельности, время завершения которой соответствует времени вводу карточки, контрольное устройство,

- допускает, что ежедневный период работы завершился в начале первого периода ОТДЫХА (или периода, за который НЕТ ДАННЫХ) после извлечения или в момент извлечения карточки, если данные о периоде отдыха введены не были (и если ни одного периода, за который НЕТ ДАННЫХ, не осталось),

- допускает, что время начала (см. ниже) соответствует времени ввода карточки,

- производит операции, изложенные ниже.

- Затем, если время завершения соответствующего периода работы отличается от времени извлечения карточки или если в этот момент времени не было введено название места завершения ежедневного периода работы, предлагает держателю карточки "подтвердить или ввести название места, в котором завершился ежедневный период работы" (confirm or enter the place where the daily work period ended) (контрольное устройство допускает возможность пропустить это предложение). Если название места введено, оно регистрируется только в карточке тахографа и только в том случае, если оно отличается от места, введенного в момент извлечения карточки (если оно было введено) с указанием времени завершения периода работы.

- Затем предлагает держателю карточки "ввести время начала" (enter a start time) текущего ежедневного периода работы (или деятельности, относящейся к данному транспортному средству, в том случае, если до этого держатель карточки использовал в течение этого периода

регистрационный листок) и предлагает держателю карточки указать "место, в котором начинается ежедневный период работы" (place where the daily work period begins) (контрольное устройство допускает возможность пропустить это предложение). Если название места введено, оно регистрируется в карточке тахографа с указанием этого времени начала деятельности. Если это время начала соответствует времени ввода карточки, то название места также регистрируется в блоке памяти.

– Затем, если это время начала отличается от времени ввода карточки, предлагает держателю карточки ввести вручную данные о деятельности в хронологическом порядке за период со времени начала до момента ввода карточки. Этот процесс заканчивается, когда время завершения деятельности, введенное вручную, соответствует времени ввода карточки.

– После этого контрольное устройство дает держателю карточки возможность изменить любые данные о деятельности, введенные вручную, до их подтверждения с помощью выбранной конкретной команды, после чего любые такие изменения произвести невозможно.

– Если такие ответы на первоначальный вопрос не подтверждаются вводом соответствующих данных о деятельности, контрольное устройство интерпретирует это так, как если бы держатель карточки пропустил этот вопрос.

В течение всего этого процесса контрольное устройство ждет ввод данных не дольше следующих интервалов времени:

- в случае отсутствия действий со стороны человека на уровне интерфейса "человек-устройство" в течение одной минуты (с подачей визуального и, в случае возможности, звукового предупреждения по истечении 30 с.) или

- если карточка извлечена или вставлена другая карточка водителя (или предприятия) или

- как только транспортное средство приходит в движение,

в этом случае контрольное устройство регистрирует любые данные, которые уже были введены.

6.3 Ввод данных об особых ситуациях

050b Контрольное устройство дает возможность водителю ввести в реальном масштабе времени следующие две особые ситуации:

"OUT OF SCOPE" ("НЕПРИМЕНИМО") (начало, конец)

"FERRY / TRAIN CROSSING" ("ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ")

Функция "FERRY / TRAIN CROSSING" может не открыться, если открыта функция "OUT OF SCOPE".

Открытая функция "OUT OF SCOPE" должна автоматически закрываться контрольным устройством в случае ввода или извлечения карточки водителя.

7. Установка блокировки предприятием

051 Эта функция позволяет предприятию устанавливать блокировку в целях ограничения доступа к данным в режиме работы "предприятия" только для уполномоченных им лиц.

052 Функция блокировки предприятием заключается в указании даты/времени начала (блокировка) и даты/времени завершения (разблокировка) в увязке с идентификацией предприятия с помощью номера карточки предприятия (в момент блокировки).

053 Блокировку можно поставить в положение "in" ("включено") или "out" ("выключено") только в реальном масштабе времени.

054 Разблокировку может произвести только предприятие, которое произвело блокировку (идентифицируемое с помощью первых 13 цифр номера карточки предприятия), или

055 Разблокировка производится автоматически, если блокировку производит другое предприятие.

055a В том случае, если какое-либо предприятие производит блокировку и если предыдущая блокировка была произведена этим же предприятием, то в данном

случае предполагается, что предыдущая блокировка не была снята и все еще находится в положении "включено".

8. Контроль за функциями проверки

056 Эта функция предусмотрена для осуществления контроля за операциями DISPLAYING, PRINTING, VU (ВЫВОД НА ДИСПЛЕЙ, ВЫВОД НА ПЕЧАТЬ, БОРТОВОЕ УСТРОЙСТВО) и за функцией DOWNLOADING (ЗАГРУЗКА), осуществляемой в режиме контроля.

057 Эта функция также предусматривает осуществление операций OVER SPEEDING CONTROL (КОНТРОЛЬ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ) в режиме контроля. Считается, что контроль за превышением скорости производится в том случае, если в режиме контроля на принтер или на дисплей выведена надпись "over speeding" или когда из блока памяти для записей данных бортового устройства загружаются данные "events and faults" ("события и неисправности").

9. Обнаружение событий и/или неисправностей

058 Эта функция позволяет обнаруживать следующие события и/или неисправности:

9.1 "Insertion of a non valid card" (ввод недействительной карточки)

059 Этот факт отражается в случае ввода любой недействительной карточки и/или в случае истечения срока действия вставленной карточки.

9.2 "Card conflict" (несовместимость карточек)

060 Этот факт отображается в том случае, когда имеет место комбинация из любых действительных карточек, отмеченных в следующей таблице знаком "X":

Несовместимость корточки		Считывающее устройство "Водитель"				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена					
	Карточка водителя				X	
	Карточка контролера			X	X	X
	Карточка мастерской		X	X	X	X
	Карточка предприятия			X	X	X

9.3 "Time overlap" (нестыковка во времени)

061 Этот факт отражается в том случае, когда текущая дата/время ввода карточки в контрольное устройство, считанное с карточки, предшествует дате/времени последнего извлечения карточки водителя.

9.4 "Driving without an appropriate card" (управление без соответствующей карточки)

062 Этот факт отображается в случае любой комбинации карточек тахографа, отмеченной знаком "X" в следующей таблице, когда вид деятельности водителя изменяется на DRIVING (УПРАВЛЕНИЕ) или когда изменяется режим работы в то время, когда деятельность водителя соответствует функции УПРАВЛЕНИЕ:

Управление без соответствующей карточки		Считывающее устройство "Водитель"				
		Карточка не вставлена (или недействительная карточка)	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена (или недействительная карточка)	X		X		X
	Карточка водителя	X		X	X	X
	Карточка контролера	X	X	X	X	X
	Карточка мастерской	X	X	X		X
	Карточка предприятия	X	X	X	X	X

9.5 "Card insertion while driving" (ввод карточки во время управления)

063 Этот факт отображается в том случае, когда карточка тахографа вставляется в любое считывающее устройство в то время, когда вид деятельности водителя соответствует функции DRIVING (УПРАВЛЕНИЕ).

9.6 "Last card session not correctly closed" (неправильное завершение последнего сеанса использования карточки)

064 Этот факт отображается в том случае, когда в момент ввода карточки в контрольное устройство оно обнаруживает, что, несмотря на положение, изложенное в пункте III.1, предыдущий сеанс использования карточки был завершен неправильно (карточка была извлечена прежде, чем на ней были записаны соответствующие данные). Этот факт касается только карточек водителя и мастерской.

9.7 "Over speeding" (превышение скорости)

065 Этот факт отображается в каждом случае превышения скорости.

9.8 "Power supply interruption" (прекращение электропитания)

066 Этот отображается, за исключением режима калибровки, в случае прекращения питания датчика движения и/или бортового устройства в течение более 200 мс. В случае падения напряжения в результате запуска двигателя транспортного средства этот факт отображаться не должен.

9.9 "Motion data error" (ошибочные данные о движении)

067 Этот факт отображается в случае нарушения нормального потока данных между датчиком движения и бортовым устройством и/или в случае ошибки, указывающей на нарушение целостности или аутентичности данных в процессе передачи данных датчиком движения в бортовое устройство.

9.10 "Security breach attempt" (попытка нарушения системы защиты)

068 Этот факт отображается в случае любого другого факта нарушения защиты датчика движения и/или бортового устройства, предусмотренной общими контрольными показателями защиты этих компонентов, за исключением режима калибровки.

9.11 Отказ "Card" (сбой в работе карточки)

069 Этот факт отображается в случае неисправности карточки тахографа, возникшей в процессе работы.

9.12 Отказ "Control device" (сбой в работе контрольного устройства)

070 Этот факт отображается в случае любых отказов, за исключением режима калибровки:

- внутренняя неполадка бортового устройства
- сбой в работе печатающего устройства
- неполадка дисплея
- сбой в работе системы загрузки
- сбой в работе датчика

10. Встроенная система проверки и самопроверки

071 Контрольное устройство должно самостоятельно обнаруживать неисправности посредством проведения самопроверки и с помощью встроенной системы проверки в соответствии со следующей таблицей:

Компонент, подвергаемый проверке	**Самопроверка**	**Встроенная система проверки**
Программное обеспечение		Целостность
Блок памяти	Доступ	Доступ, целостность данных
Интерфейсы для считки карточек	Доступ	Доступ
Клавиатура		Ручная проверка
Печатающее устройство	(по усмотрению изготовителя)	Распечатка
Дисплей		Визуальная проверка
Загрузка (осуществляется только в процессе загрузки)	Надлежащая работа	
Датчик	Надлежащая работа	Надлежащая работа

11. Считывание данных, содержащихся в памяти

072 Контрольное устройство должно быть способным считывать любые данные, содержащиеся в его памяти.

12. Регистрация и хранение данных в блоке памяти

Для целей этого пункта

- "365 дней" означает 365 календарных суток усредненной продолжительности деятельности водителя на транспортном средстве. Усредненная продолжительность деятельности в день на транспортном средстве определяется в расчете как минимум 6 водителей или вторых водителей, 6 циклов ввода и извлечения карточек и 256 фактов изменения деятельности. Таким образом, термин "365 дней" включает данные, касающиеся как минимум 2 190 водителей (вторых водителей), 2 190 циклов ввода и извлечения карточек и 93 440 случаев изменения деятельности,

- время регистрируется с точностью до одной минуты, если не предусмотрено иное,

- показания счетчика пробега регистрируются с точностью до одного километра,

- скорость регистрируется с точностью 1 км/ч.

073 Данные, которые хранятся в блоке памяти, не должны нарушаться в результате прекращения внешнего электропитания продолжительностью не более 12 месяцев в условиях, предусмотренных официальным утверждением типа.

074 Контрольное устройство должно быть способно регистрировать и хранить самостоятельно или по команде следующие данные в своей памяти:

12.1 Идентификационные данные оборудования

12.1.1 Идентификационные данные бортового устройства

075 Контрольное устройство должно быть способно хранить в своей памяти следующие идентификационные данные бортового устройства:

- наименование изготовителя,
- адрес изготовителя,
- номер компонентов,

- серийный номер,
- номер версии программного обеспечения,
- дата установки версии программного обеспечения,
- год изготовления устройства,
- номер официального утверждения.

076 Идентификационные данные бортового устройства регистрируются и хранятся раз и навсегда изготовителем бортового устройства, за исключением даты и номера официального утверждения программного обеспечения, которые могут быть изменены в случае перехода на улучшенную версию программы.

12.1.2 Идентификационные данные датчика движения

077 Датчик движения должен быть способен хранить в своей памяти следующие идентификационные данные:

- наименование изготовителя,
- номер деталей,
- серийный номер,
- номер официального утверждения.
- идентификатор встроенного компонента защиты (например, номер встроенной интегральной схемы/процессора),
- идентификатор операционной системы (например, номер версии программного обеспечения).

078 Идентификационные данные датчика движения регистрируются и хранятся раз и навсегда в памяти датчика движения изготовителем.

079 Бортовое устройство должно быть способно регистрировать и хранить в своей памяти следующие идентификационные данные датчика движения, к которому он подсоединен:

- серийный номер,
- номер официального утверждения,
- дата первого подсоединения,

12.2 Элементы защиты

080 Контрольное устройство должно быть способно хранить следующие элементы защиты:

- европейский код общего пользования,
- сертификат Договаривающейся стороны,
- сертификат на устройство,
- закрытый ключ устройства.

Элементы защиты контрольного устройства встраиваются в оборудование изготовителем бортового устройства.

12.3 Данные о вводе и извлечении карточки водителя

081 В случае каждого цикла ввода в устройство карточки водителя или мастерской и ее извлечения из него контрольное устройство должно регистрировать и хранить в своей памяти следующие данные:

- фамилия и имя (имена) держателя карточки, записанные в блоке памяти карточки:

- номер карточки, название выдавшей ее Договаривающейся стороны и дата истечения срока действия, записанные в блоке памяти карточки:

- дата и время ввода,

- показание счетчика пробега транспортного средства в момент ввода карточки,

- считывающее устройство, в которое вставляется карточка,

- дата и время извлечения,

- показания счетчика пробега транспортного средства в момент извлечения карточки,

- следующая информация о предыдущем транспортном средстве, использованном водителем, записанная в блоке памяти карточки:

- VRN (регистрационный номер транспортного средства) и Договаривающаяся сторона регистрации,

- дата и время извлечения карточки,

- метка, указывающая на то, ввел держатель карточки данные о своей деятельности вручную или нет в момент ввода карточки.

082 Блок памяти должен быть способен хранить эти данные в течение не менее 365 дней.

083 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.4 Данные о деятельности водителя

084 Контрольное устройство должно регистрировать и хранить в своей памяти все факты изменения деятельности водителя и/или второго водителя и/или все случаи изменения статуса управления и/или все случаи ввода или извлечения карточки водителя или мастерской:

- статус управления (CREW, SINGLE) (ЭКИПАЖ, ОДИН)

- считывающее устройство (DRIVER, CO-DRIVER) (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ),

- положение карточки в соответствующем считывающем устройстве (INSERTED, NOT INSERTED) (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА) (см. примечание),

- вид деятельности (DRIVING, AVAILABILITY, WORK, BREAK/REST) (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ),

- дата и время изменения.

Примечание: INSERTED означает, что в считывающее устройство вставлена действительная карточка водителя или мастерской. NOT INSERTED означает обратное, т. е. в считывающем устройстве нет ни действительной карточки водителя, ни действительной карточки мастерской (например, вставлена карточка предприятия или никакая карточка не вставлена).

Примечание: Данные о деятельности, которые вводятся водителем вручную, в памяти не регистрируются.

085 Блок памяти должен быть способен хранить данные о деятельности водителя как минимум за 365 дней.

086 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.5 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы

087 Контрольное устройство должно регистрировать и хранить в своей памяти все случаи ввода водителем (вторым водителем) названия места, в котором начинается и/или заканчивается ежедневный период работы:

- в случае применимости, номер карточки водителя (второго водителя) и название Договаривающейся стороны, выдавшей карточку,
- дата и время ввода данных (или дата/время, относящиеся к вводу данных в том случае, когда эта операция производится во время процедуры ручного ввода данных),
- тип ввода (начало или конец, условие ввода),
- введенное название страны и района,
- показания счетчика пробега транспортного средства.

088 Блок памяти должен быть способен хранить данные о начале и/или завершении ежедневных периодов работы в течение как минимум 365 дней (при предположении, что один водитель вводит две записи в день).

089 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.6 Данные о пробеге

090 Контрольное устройство должно регистрировать в своей памяти показания счетчика пробега транспортного средства и соответствующую дату в полночь каждого календарного дня.

091 Блок памяти должен быть способен хранить показания счетчика пробега, зарегистрированные в полночь каждый день, в течение как минимум 365 календарных дней.

092 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.7 Детальные данные о скорости

093 Контрольное устройство должно регистрировать и хранить в своей памяти мгновенную скорость транспортного средства и соответствующую дату и время с интервалом в 1 секунду как минимум за последние 24 часа, в течение которых транспортное средство находилось в процессе движения.

12.8 Данные о событиях

Для целей данного подпункта время регистрируется с точностью до 1 секунды.

094 Устройство должно регистрировать и хранить в своей памяти следующие данные по каждому событию, обнаруженному в соответствии со следующими правилами хранения:

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
Несовместимость карточек	- 10 самых последних событий	- дата и время начала события - дата и время наступления события - дата и время завершения события - тип карточки, номер карточки и Договаривающаяся сторона, выдавшая две карточки, которые явились причиной несовместимости
Управление без соответствующей карточки	- наиболее длительное событие за каждые из 10 последних дней - 5 наиболее продолжительных событий за последние 365 дней	- дата и время начала события - дата и время завершения события - тип карточки, номер карточки и Договаривающаяся сторона, выдавшая любую карточку, вставленную на момент начала и/или завершения данного события - число аналогичных событий за данный день
Ввод карточки в процессе управления	- последнее событие за каждый из последних 10 дней	- дата и время события - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона - число аналогичных событий за указанный день
Неправильное завершение последнего сеанса использования карточки	- 10 самых последних событий	- дата и время ввода карточки - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона - последняя дата сеанса использования, записанная на карточке:

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
		- дата и время ввода карточки, - регистрационный номер транспортного средства и Договаривающая сторона регистрация
Превышение скорости (1)	- наиболее серьезное событие за последние 10 дней (т.е. случай регистрации самой высокой средней скорости) - 5 наиболее серьезных событий за последние 365 дней, - первое событие, наступившее после последней калибровки.	- дата и время начала события - дата и время конца события - максимальная скорость, измеренная во время события - среднее арифметическое скорости, измеренной во время события - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона водителя (в случае применимости) - число аналогичных событий в указанный день
Прекращение электропитания (2)	- самое длительное событие за каждый из 10 последних дней - 5 самых длительных событий за последние 365 дней	- дата и время начала события - дата и время конца события - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события - число аналогичных событий в указанный день
Ошибочные данные о движении	- самое длительное событие за каждый из 10 последних дней - 5 самых длительных событий за последние 365 дней	- дата и время начала события - дата и время конца события - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку,

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
		вставленную в начале и/или конце события - число аналогичных событий в указанный день
Попытка нарушения системы защиты	- 10 самых последних событий по типу события	- дата и время начала события - дата и время конца события (в случае применимости) - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события - тип события

095 1) Контрольное устройство должно также регистрировать и хранить в своей памяти :

- дату и время последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ (OVER SPEEDING CONTROL),

- дату и время первого превышения скорости после этого КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ,

- число случаев превышения скорости после последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ.

2) Эти данные могут регистрироваться только при восстановлении электропитания, при этом время должно быть известно с точностью до минуты.

12.9 Данные о неисправностях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

096 Контрольное устройство должно быть способно регистрировать и хранить в своей памяти следующие данные по каждому обнаруженному сбою в работе в соответствии со следующими правилами хранения:

Неисправность	Правила хранения	Данные о неисправности, подлежащей регистрации
Сбой в работе карточки	- 10 самых последних сбоев в работе карточки водителя	- дата и время начала сбоя - дата и время конца сбоя - тип карточки, номер и выдавшая ее Договаривающаяся сторона
Сбой в работе контрольного устройства	- 10 самых последних сбоев по каждому типу сбоя - первый сбой после последней калибровки	- дата и время начала сбоя - дата и время конца сбоя - тип ошибки - тип карточки, номер и Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце ошибки

12.10 Данные калибровки

097 Контрольное устройство должно регистрировать и хранить в своей памяти данные, касающиеся:

- известных параметров калибровки в момент включения,
- самые первые параметры калибровки после включения,
- самые первые параметры калибровки на данном транспортном средстве (идентифицируемом с помощью его опознавательного номера VIN),
- самые последние 5 калибровок (если последние калибровки производятся в течение одного календарного дня, должны храниться данные только о самой последней калибровке в указанный день).

098 По каждой из этих калибровок должны регистрироваться следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция),
- название и адрес мастерской,

- номер карточки мастерской, Договаривающаяся сторона, выдавшая карточку, и дата истечения срока действия карточки,

- идентификация транспортного средства,

- обновленные или подтвержденные параметры: w, k, l, размер шин, регулировка устройства ограничения скорости, счетчик пробега (прежние и новые показания), дата и время (прежние и новые значения).

099 Датчик движения должен регистрировать и хранить в своей памяти следующие данные, касающиеся установки датчика движения:

- первое подсоединение к бортовому устройству (БУ) (дата, время, номер официального утверждения, серийный номер БУ),

- последнее подсоединение к бортовому устройству БУ (дата, время, номер официального утверждения, серийный номер БУ).

12.11 Данные о корректировке времени

100 Контрольное устройство должно регистрировать и хранить в своей памяти данные, касающиеся:

- самых последних корректировок времени,
- пяти наиболее серьезных корректировок времени после последней калибровки,

произведенных в режиме калибровки, не относящейся к системе регулярной калибровки (определение f)).

101 Для каждой из этих корректировок времени должны регистрироваться следующие данные:

- дата и время, прежнее значение,
- дата и время, новое значение,
- название и адрес мастерской,
- номер карточки мастерской, Договаривающаяся сторона, выдавшая карточку, и дата истечения срока действия карточки.

12.12 Данные о контрольных операциях

102 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся самых последних 20 контрольных операций:

- дата и время контроля,
- номер карточки контролера и Договаривающаяся сторона, выдавшая карточку,
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с бортового устройства и/или загрузка с карточки).

103 В случае загрузки данных регистрируются также даты самого раннего и самого последнего дня загрузки.

12.13 Данные о блокировке, установленной предприятием

104 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся 20 самых последних случаев блокировки, установленной предприятием:

- дата и время блокировки,
- дата и время разблокировки,
- номер карточки предприятия и Договаривающаяся сторона, выдавшая карточку,
- название и адрес предприятия.

12.14 Данные об операциях по загрузке

105 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся последней операции по загрузке данных из блока памяти на внешний носитель в режиме предприятия или калибровки:

- дата и время загрузки,
- номер карточки предприятия или мастерской, Договаривающая сторона, выдавшая карточку,
- название предприятия или мастерской.

12.15 Данные об особых ситуациях

105 a) Контрольное устройство должно регистрировать в своей памяти следующие данные, касающиеся особых ситуаций:

- дата и время ввода данных;
- тип особой ситуации.

105 b) Блок памяти данных должен быть способен хранить данные об особых ситуациях как минимум за 365 дней (при предположении, что в среднем ежедневно открывается и закрывается одна позиция, указывающая на особую ситуацию). Когда объем памяти заполнен, новые данные записываются на самые старые данные.

13. Считывание данных с карточки тахографа

106 Контрольное устройство должно быть способно считывать с карточек тахографа в соответствующих случаях необходимые данные в целях:

- идентификации типа карточки, держатель карточки, ранее использованного транспортного средства, даты и времени последнего извлечения карточки и вида деятельности, выбранного в тот момент;

- проверки правильности завершения последнего сеанса использования карточки;

- расчета непрерывного времени управления транспортным средством водителем, совокупное время перерывов и совокупное время управления за предыдущую и текущую неделю;

- вывод на печать требуемых данных, записанных на карточке водителя;

- загрузки данных с карточки водителя на внешний носитель.

107 В случае ошибки при считывании записывающее устройство должно произвести очередную попытку (максимум три раза) выполнения той же команды на считывание данных, после чего, если считать данные не удалось, сообщить, что карточка неисправна и недействительна.

14. Регистрация и хранение данных на карточках тахографа

108 Контрольное устройство должно записать "данные о сеансе использования карточки" в карточке водителя или мастерской сразу же после ее ввода.

109 Контрольное устройство должно обновлять данные, хранящиеся на действующей карточке водителя, мастерской и/или контролера, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка была вставлена в устройство, и к держателю карточки. Данные, хранящиеся на этих карточках, указываются в главе IV.

109 а) Контрольное устройство должно обновлять данные о деятельности водителя и месте (как указано в пунктах 5.2.5 и 5.2.6 главы IV), хранящиеся на действующей карточке водителя и/или предприятия, с учетом данных о виде деятельности и месте, введенных держателем карточки вручную.

110 Порядок обновления данных в карточках тахографа должен быть таковым, чтобы в случае необходимости и с учетом фактического объема памяти хранения самые последние данные записывались на самые старые данные.

111 В случае ошибки при записи контрольное устройство должно сделать еще одну попытку (максимум три раза) выполнить ту же команду на запись, после чего, если считать данные не удалось, сообщить, что карточка неисправна и недействительна.

112 До высвобождения карточки водителя и после сохранения на ней всех соответствующих данных контрольное устройство должно установить "данные о сеансе использования карточки" в исходное состояние.

15. Индикация данных

113 Отображаемое сообщение должно включать не менее 20 знаков.

114 Минимальный размер знака должен быть 5 мм по высоте и 3,5 мм по ширине.

114 а) Дисплей должен поддерживать наборы латинских типа 1 и греческих знаков, определенных в частях 1 и 7 стандарта ISO 8859, как указано в главе 4 "Наборы знаков" подраздела 1. Для индикации данных могут использоваться упрощенные наборные знаки (например, ударные знаки могут отображаться без знака ударения или строчные буквы могут отображаться в виде прописных букв).

115 Дисплей должен быть оснащен надлежащей неослепляющей подсветкой.

116 Индикация должна быть видимой вне контрольного устройства.

117 Контрольное устройство должно быть способно выводить на дисплей:

- данные по умолчанию;
- данные предупреждения;
- данные о доступе к меню;
- другие данные, запрашиваемые пользователем.

Контрольное устройство может выводить на дисплей дополнительную информацию при условии, что ее можно четко отличить от информации, требуемой выше.

118 Дисплей контрольного устройства должен использовать пиктограммы или комбинации пиктограмм, перечисленные в подразделе 3. На дисплей могут также выводиться дополнительные пиктограммы или комбинации пиктограмм при условии, что их можно четко отличить от пиктограмм или комбинаций пиктограмм, упомянутых выше.

119 Когда транспортное средство находится в процессе движения, дисплей должен быть всегда включен.

120 Контрольное устройство может быть оснащено ручной или автоматической функцией, позволяющей отключать дисплей, когда транспортное средство остановлено.

Формат отображения данных указан в подразделе 5.

15.1 Индикация данных по умолчанию

121 Когда иную информацию на дисплей выводить не требуется, контрольное устройство отображает по умолчанию следующие данные:

- местное время (время UTC плюс корректировка, сделанная водителем);
- режим работы;
- текущий вид деятельности водителя и текущий вид деятельности второго водителя;

- информация, касающаяся водителя:

  - если его текущим видом деятельности является УПРАВЛЕНИЕ (DRIVING) - текущее время непрерывного управления и текущая продолжительность совокупных перерывов;

  - если его текущим видом деятельности не является УПРАВЛЕНИЕ (DRIVING) - продолжительность его текущей деятельности (с момента выбора этой функции) и совокупная продолжительность перерывов на данный момент;

- информация, касающаяся второго водителя:

  - продолжительность его текущей деятельности (с момента выбора этой функции).

122 Индикация данных, относящихся к каждому водителю, должна быть четкой, полной и однозначной. В том случае, если информацию, относящуюся к водителю и второму водителю, нельзя вывести на дисплей одновременно, контрольное устройство должно отображать информацию, относящуюся к водителю, и давать пользователю возможность выводить на дисплей информацию, относящуюся ко второму водителю.

123 В том случае, если ширина дисплея не позволяет отображать по умолчанию режим работы, контрольное устройство должно выводить на дисплей кратковременное сообщение с указанием нового режима работы в момент его изменения.

124 Контрольное устройство должно выводить на дисплей кратковременное сообщение с указанием фамилии держателя карточки в момент ее ввода.

124a Когда открывается позиция "OUT OF SCOPE" (НЕПРИМЕНИМО), то в этом случае на дисплее должен отображаться по умолчанию с использованием соответствующей пиктограммы тот факт, что эта позиция открыта (при этом допускается, что текущий вид деятельности водителя может в это время не отображаться).

15.2 Предупреждающая индикация

125 Контрольное устройство должно выводить на дисплей предупреждающую информацию с использованием прежде всего пиктограмм, указанных в подразделе 3, дополненных, в случае необходимости, дополнительной информацией в виде числового кода. Кроме того, может быть включено текстовое описание предупреждения на языке, выбранном водителем.

15.3 Меню доступа

126 Контрольное устройство должно содержать необходимые команды, подаваемые с использованием соответствующего меню.

15.4 Индикация иных данных

127 По соответствующей команде можно выводить на дисплей на выборочной основе следующие данные:

- дата и время UTC,
- режим работы (если он не указывается по умолчанию),
- продолжительность управления и совокупное время перерывов водителя,
- продолжительность управления и совокупное время управления вторым водителем,
- совокупное время управления водителем за предыдущую и текущую неделю,
- совокупное время управления второго водителя за предыдущую и текущую неделю,
- содержание любой из шести распечаток в том же формате, что и сами распечатки.

128 Вывод содержания распечаток производится в последовательном порядке построчно. Если ширина дисплея составляет менее 24 знаков, пользователь может просматривать полную информацию в соответствующей форме (несколько строк, прокрутка, ...). Строки распечатки, предназначенные для внесения информации вручную, на дисплей могут не выводиться.

16. Распечатка

129 Контрольное устройство должно быть способно выводить на печать информацию, содержащуюся в его памяти и/или в карточках тахографа, в виде следующих шести видов распечаток:

- ежедневная распечатка данных о деятельности водителя, записанных в карточке,
- ежедневная распечатка данных о деятельности водителя, записанных в бортовом устройстве,
- распечатка данных о событиях и ошибках, хранящихся на карточке,
- распечатка данных о событиях и неисправностях, записанных в бортовом устройстве,
- распечатка технических данных,
- распечатка данных о превышении скорости.

Детальный формат и содержание этих распечаток указываются в подразделе 4.

В конце распечаток могут содержаться дополнительные данные.

Дополнительные распечатки могут также выдаваться контрольным устройством, если они четко отличаются от шести распечаток, упомянутых выше.

130 "Ежедневная распечатка данных о деятельности водителя, записанных на карточке" (driver activities from card daily printout) и "распечатка данных о событиях и неисправностях, записанных на карточке" (Events and faults from card printout) выдается только в том случае, если в контрольное устройство вставлена карточка водителя или карточка мастерской. До выдачи распечатки контрольное устройство обновляет данные, содержащиеся в памяти соответствующей карточки.

131 Для того чтобы сделать "ежедневную распечатку данных о деятельности водителя, записанных на карточке" или "распечатку данных о событиях и неисправностях, записанных на карточке", контрольное устройство должно:

- либо автоматически выбрать карточку водителя или карточку мастерской, если в устройство вставлена только одна из этих карточек,

- либо предусматривать команду, позволяющую выбрать исходную карточку или выбрать карточку, вставленную в считывающее устройство водителя, если в контрольное устройство вставлены обе эти карточки.

132 Печатающее устройство должно быть способно печатать 24 знака на строке.

133 Минимальный размер знака должен составлять 2,1 мм по высоте и 1,5 мм по ширине.

133a Печатающее устройство должно поддерживать наборы латинских знаков типа 1 и греческих знаков, определенных в частях 1 и 7 стандарта ISO 8859, как указано в пункте "Наборы знаков" подраздела 1.

134 Печатающее устройство должно быть сконструировано таким образом, чтобы оно могло выдавать эти распечатки такой разрешающей способности, которая исключала бы всякое двоякое толкование при их чтении.

135 Распечатки должны сохранять свои размеры и содержащиеся на них данные в нормальных условиях влажности (10-90%) и температуры.

136 На бумаге, используемой контрольным устройством, должен быть нанесен соответствующий знак официального утверждения типа и указание типа (типов) контрольного устройства, на котором она используется. Распечатки должны оставаться легкочитаемыми и распознаваемыми в обычных условиях хранения (интенсивность света, влажность и температура) в течение не менее одного года.

137 Кроме того, необходимо предусмотреть возможность включения в эти документы примечаний, написанных от руки, например подписи водителя.

138 В том случае, если во время распечатки закончилась бумага, контрольное устройство должно возобновить печатание после загрузки бумаги с начала распечатки или продолжить печатание с четкой ссылкой на ту часть, которая была выдана на печать ранее.

17. Предупреждения

139 Контрольное устройство должно предупреждать водителя в случае обнаружения любого события и/или неисправности.

140 Предупреждение о прекращении электропитания может подаваться с задержкой до тех пор, пока электропитание не будет восстановлено.

141 Контрольное устройство должно предупреждать водителя за 15 мин. до момента и в тот момент, когда непрерывное время управления превысило 4 час. 30 мин.

142 Предупреждения должны быть визуальными. В дополнение к визуальным предупреждениям могут также предусматриваться звуковые предупреждения.

143 Визуальные предупреждения должны быть четко распознаваемыми пользователем, располагаться в поле визуального восприятия водителя и быть удобочитаемыми как в дневное, так и в ночное время.

144 Система визуального предупреждения может быть встроена в контрольное устройство и/или вынесена за его пределы.

145 В последнем случае она должна обозначаться буквой "T" и быть желтого или оранжевого цвета.

146 Предупреждения должны подаваться в течение как минимум 30 секунд, если только пользователь не нажимает на любую клавишу контрольного устройства в порядке подтверждения того, что он принял предупреждение к сведению. Это первое подтверждение не должно влечь за собой стирание выведенной на дисплей причины, указанной в следующем пункте.

147 Причина предупреждения должна выводиться на дисплей контрольного устройства и оставаться видимой до тех пор, пока пользователь не введет конкретный код или команду на контрольном устройстве.

148 Могут предусматриваться дополнительные предупреждения, если они не вводят водителей в заблуждение по поводу предупреждений, определенных выше.

18. Загрузка данных во внешние носители

149 Контрольное устройство должно быть способно загружать по команде данные из своей памяти или из карточки водителя на внешние носители через калибровочный/загрузочный разъем. До загрузки контрольное устройство должно обновить данные, сохраненные на соответствующей карточке.

150 В дополнение и в качестве факультативной функции контрольное устройство может загружать данные в базу данных предприятия, идентифицированного по этому каналу связи, через другой разъем. В таком случае к этой операции загрузки применяются права доступа к данным в режиме предприятия.

151 Загрузка не должна приводить к изменению или стиранию любых сохраненных данных.

Электрический интерфейс калибровочного/загрузочного разъема определяется в подразделе 6.

Протоколы загрузки определяются в подразделе 7.

19. Вывод данных на дополнительные внешние устройства

152 Когда в контрольном устройстве не предусмотрены функции вывода на дисплей показаний скорости и/или счетчика пробега, контрольное устройство должно генерировать выходной сигнал (сигналы), позволяющие выводить на дисплей скорость транспортного средства (показания спидометра) и/или общее расстояние, пройденное транспортным средством (счетчик пробега).

153 Бортовое устройство должно также быть способно выдавать следующие данные по соответствующему специально предназначенному для этой цели последовательному каналу, не зависимому от факультативного подсоединения к шине ЛСК (ISO 11898: Дорожные транспортные средства – Взаимообмен цифровой информацией – Локальная сеть контроллеров (ЛСК) для высокоскоростной передачи данных), в целях их обработки другими электронными устройствами, установленными на транспортном средстве:

- текущая дата и время UTC,
- скорость транспортного средства,
- общее расстояние, пройденное транспортным средством (счетчик пробега),
- текущий вид деятельности, выбранный водителем и вторым водителем,
- информация о том, вставлена ли в данный момент в считывающее устройство водителя и считывающее устройство второго водителя какая-либо карточка тахографа, и (в случае применимости) информация, касающаяся идентификации соответствующих карточек (номер карточки и выдавшая ее Договаривающая сторона).

В дополнение к этому минимальному перечню могут выводиться и иные данные.

Когда зажигание транспортного средства включено, эти данные должны передаваться постоянно. Когда зажигание транспортного средства выключено, должны передаваться как минимум данные об изменении вида деятельности водителя или второго водителя и/или о вводе или извлечении карточки тахографа. В том случае, если передача данных при выключенной системе зажигания транспортного средства приостанавливается, эти данные должны передаваться снова после включения зажигания транспортного средства.

20. Калибровка

154 Функция калибровки позволяет:

- автоматически подсоединять датчик движения к бортовому устройству,
- адаптировать в цифровом режиме постоянную контрольного устройства (k) к характеристическому коэффициенту транспортного средства (w) (транспортные средства с двумя передаточными числами моста или более должны оснащаться соответствующим устройством переключения, с помощью которого эти числа будут автоматически приводиться в соответствие с передаточным числом, на которое было отрегулировано устройство, установленное на транспортном средстве),
- корректировать (без ограничения) текущее время,
- корректировать текущие показания счетчика пробега,
- обновлять идентификационные данные датчика движения, записанные в блоке памяти,
- обновлять или подтверждать другие параметры, заложенные в контрольном устройстве: идентификация транспортного средства, показатели w и l, размер шин и регулировка устройства ограничения скорости (в случае применимости).

155 Подсоединение датчика движения к бортовому устройству заключается, как минимум в:

– обновлении данных установки счетчика движения, содержащихся в памяти датчика движения (при необходимости),

– копировании необходимых идентификационных данных датчика движения и блока памяти датчика движения в блок памяти бортового устройства.

156 Функция калибровки должна обеспечивать ввод необходимых данных с помощью калибровочного/загрузочного разъема в соответствии с протоколом калибровки, определенным в подразделе 8. Функция калибровки может также обеспечивать ввод необходимых данных с помощью других разъемов.

21. Корректировка времени

157 Функция корректировки времени должна позволять корректировать текущее время максимум в пределах 1 минуты с интервалами не менее 7 дней.

158 Функция корректировки времени должна обеспечивать корректировку текущего времени без каких бы то ни было ограничений в режиме калибровки.

22. Условия работы

159 Бортовое устройство должно быть полностью работоспособным в диапазоне температур от -20°C до 70°C, а датчик движения - в диапазоне температур от -40°C до 135°C. Содержание блока памяти должно сохраняться при температурах до -40°C.

160 Контрольное устройство должно быть полностью работоспособным в диапазоне мощности от 10% до 90%.

161 Контрольное устройство должно быть защищено от бросков напряжения, несоблюдения полярности источника питания и короткого замыкания.

162 Контрольное устройство должно соответствовать Правилам ЕЭК № 10[9], касающимся электромагнитной совместимости, и должно быть защищено от электростатических разрядов и помех, вызванных переходными процессами.

23. Материалы

163 Все составные части контрольного устройства должны быть изготовлены из материалов, обладающих достаточной устойчивостью и механической прочностью и стабильными электромагнитными характеристиками.

164 В обычных условиях эксплуатации все внутренние компоненты оборудования должны быть защищены от действия влаги и пыли.

165 Бортовое устройство должно соответствовать требованиям уровня защиты IP 40, а датчик движения должен удовлетворять требованиям уровня защиты IP 64 в соответствии со стандартом IEC 529.

166 Контрольное устройство должно соответствовать применимым техническим спецификациям, регламентирующим параметры эргономичности.

167 Контрольное устройство должно быть защищено от случайного повреждения.

24. Маркировка

168 Если контрольное устройство выводит на дисплей показания счетчика пробега транспортного средства и спидометра, то на дисплее должны отображаться следующие символы:

- около цифры, указывающей пройденное расстояние, - единица измерения расстояния, обозначаемая с помощью сокращения "км",

- рядом с цифрой, указывающей скорость, - сокращение "км/ч".

---

[9] Исходным текстом в ЕС является директива Комиссии 95/54/ЕС от 31 октября 1995 года, предусматривающая приведение директивы Совета 72/245/ЕЕС о сближении законодательства государств-членов, регламентирующего подавление радиопомех, производимых двигателями с искровым зажиганием, установленными на автотранспортных средствах, в соответствие с техническим прогрессом (OJ No. L 266, 08/11/1995).

Контрольное устройство может также переключаться в режим отображения скорости в милях в час; в этом случае единица измерения скорости указывается с помощью сокращения "mph" (м/ч).

169 К каждому отдельному компоненту контрольного устройства должна быть прикреплена табличка с указанием следующих данных:

- название и адрес изготовителя устройства,
- номер детали, присвоенный изготовителем, и год изготовления устройства,
- серийный номер устройства.
- знак официального утверждения типа устройства.

170 Если место для указания вышеупомянутых данных на табличке недостаточно, на ней следует, как минимум, проставить название или логотип изготовителя и номер компонента устройства.

IV. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КАРТОЧЕК ТАХОГРАФА

1. Видимые данные

На первой странице должны быть указаны:

171 слова "Driver card" ("Карточка водителя") или "Control card" ("Карточка контролера" или "Workshop card" ("Карточка мастерской") или "Company card" ("Карточка предприятия"), напечатанные крупным шрифтом на официальном языке или языках Договаривающейся стороны, выдавшей карточку, в зависимости от типа карточки[10];

172 те же слова, напечатанные на официальных языках ЕЭК ООН на фоне карточки (см. образцы в позиции 178):

EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
RU	КАРТОЧКА ВОДИТЕЛЯ	КАРТОЧКА КОНТРОЛЕРА	КАРТОЧКА МАСТЕРСКОЙ	КАРТОЧКА ПРЕДПРИЯТИЯ

173 название Договаривающейся стороны, выдавшей карточку (факультативно);

174 отличительный знак Договаривающейся стороны, выдавшей карточку. Официальные отличительные знаки Договаривающихся сторон соответствуют знакам, определенным в Венской конвенции о дорожном движении 1968 года или в Женевской конвенции о дорожном движении 1949 года. Отличительные знаки Договаривающихся сторон ЕСТР указаны ниже:

AL	Албания	GR	Греция	MD	Республика Молдова
AND	Андорра	H	Венгрия	RO	Румыния
A	Австрия	IR	Ирландия	SRB	Сербия
AM	Армения	I	Италия	SK	Словакия
AZ	Азербайджан	KZ	Казахстан	SLO	Словения
BY	Беларусь	LV	Латвия	E	Испания
B	Бельгия	FL	Лихтенштейн	S	Швеция
BIH	Босния и Герцеговина	LT	Литва	CH	Швейцария

[10] Договаривающиеся стороны сообщат в секретариат ЕЭК ООН, какие слова они используют в этом случае на своем национальном языке.

BG	Болгария	L	Люксембург	MK	БЮР Македония
HR	Хорватия	M	Мальта	TR	Турция
CY	Кипр	MNE	Черногория	TM	Туркменистан
CZ	Чешская Республика	NL	Нидерланды	UK	Соединенное Королевство
DK	Дания	N	Норвегия	UA	Украина
EST	Эстония	PL	Польша	UZ	Узбекистан
FIN	Финляндия	P	Португалия		
F	Франция	RUS	Российская Федерация		
D	Германия	RSM	Сан-Марино		

175 конкретные данные, касающиеся выданной карточки, под следующими номерами:

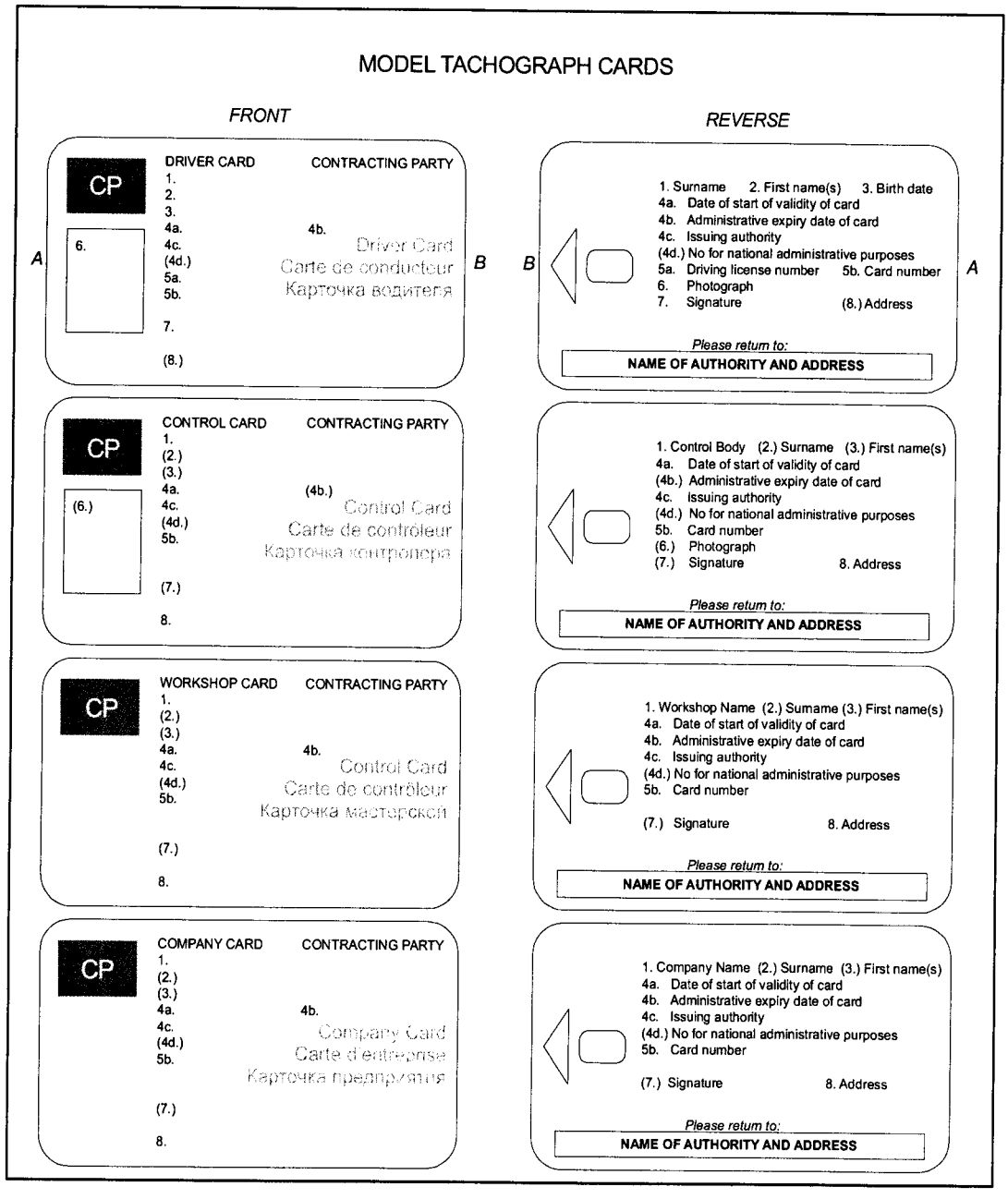
	Карточка водителя	**Карточка контроля**	**Карточка предприятия или мастерской**
1.	фамилия водителя	название контрольного органа	название предприятия или мастерской
2.	имя (имена) водителя	фамилия контролера (в случае применимости)	фамилия держателя карточки (в случае применимости)
3.	дата рождения водителя	имя (имена) контролера (в случае применимости)	имя (имена) держателя карточки (в случае применимости)
4. (a)	дата начала срока действия карточки		
(b)	дата истечения срока действия карточки (в соответствующем случае)		
(c)	название компетентного органа, выдавшего карточку (может быть напечатано на стр. 2)		
(d)	номер, отличный от номера, указанного в позиции 5, для административных целей (факультативно)		
5. (a)	номер водительского удостоверения (на дату выдачи карточки водителя)	-	-
5. b)	номер карточки		
6.	фотография водителя	фотография контролера (факультативно)	-
7.	подпись водителя	подпись держателя (факультативно)	
8.	обычное место жительства или почтовый адрес держателя (факультативно)	почтовый адрес контрольного органа	почтовый адрес предприятия или мастерской

176 даты записываются в формате "дд/мг/гггг" или дд.мм.гггг" (день, месяц, год).

На обратной стороне содержится:

177 разъяснение пронумерованных позиций, содержащихся на лицевой стороне карточки;

178 с письменного согласия держателя в каждом конкретном случае в карточку может включаться информация, которая не относится к работе с карточкой; такая дополнительная информация не должна никоим образом изменять метод использования этого образца в качестве карточки тахографа.



(Перевод содержания вышеупомянутых образцов приводится ниже)

ОБРАЗЕЦ КАРТОЧЕК ТАХОГРАФА

ЛИЦЕВАЯ СТОРОНА *ОБРАТНАЯ СТОРОНА*

Карточка водителя Договаривающая сторона:

1. Фамилия 2. Имя (имена) 3. Дата рождения
4a. Дата начала действия карточки
4b. Дата истечения административного срока действия карточки
4c. Компетентный орган, выдавший карточку
(4d) Не предназначена для административных целей на национальном уровне
5a. Номер водительского удостоверения 5b. Номер карточки
6. Фотография
7. Подпись (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

Карточка водителя Договаривающая сторона:

1. Контрольный орган 2. Фамилия 3. Имя (имена)
4a. Дата начала действия карточки
4b. Дата истечения административного срока действия карточки
4c. Компетентный орган, выдавший карточку
(4d) Не предназначена для административных целей на национальном уровне
5b. Номер карточки
6. Фотография
7. Подпись; (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

Карточка водителя Договаривающая сторона:

1. Название мастерской 2. Фамилия 3. Имя (имена)
4a. Дата начала действия карточки
4b. Дата истечения административного срока действия карточки
4c. Компетентный орган, выдавший карточку
(4d) Не предназначена для административных целей на национальном уровне
5b. Номер карточки
7. Подпись (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

Карточка водителя

Договаривающая сторона:

1. Название предприятия 2. Фамилия 3. Имя (имена)
4a. Дата начала действия карточки
4b. Дата истечения административного срока действия карточки
4c. Компетентный орган, выдавший карточку
(4d) Не предназначена для административных целей на национальном уровне
5b. Номер карточки
7. Подпись (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

179 Текст карточек тахографа печатается на фоне следующего цвета:

- карточка водителя: белый,
  карточка контролера: голубой,
- карточка мастерской: красный,
- карточка предприятия: желтый.

180 Карточки тахографа должны содержать как минимум следующие элементы защиты карточки от подделки и фальсификации:

- защитный фон в виде тонкого и радужного узора из пересекающихся линий,
- в районе фотографии - накладка защитного фона на фотографию,
- как минимум одна двухцветная линия, нанесенная способом микропечати.

181 По согласованию с секретариатом ЕЭК ООН Договаривающиеся стороны могут включать цвета или маркировку, например национальные символы и элементы защиты без ущерба для других положений настоящего добавления.

2. Защита

Система защиты имеет целью предохранить целостность и аутентичность данных, передаваемых между карточками и контрольным устройством, предохранение целостности и аутентичности данных, загружаемых с карточки, предоставление возможности производить некоторые операции по записи данных на карточку только контрольным устройством, исключение любой возможности фальсификации

данных, хранящихся в карточках, предотвращение фальсификации и обнаружение любой попытки такого рода.

182 В целях обеспечения защиты системы карточки тахографа должны удовлетворять требованиям, предъявляемым к защите, которые предусмотрены общими контрольными показателями защиты карточки тахографа (подраздел 10).

183 Карточки тахографа должны считываться другими устройствами, например персональными компьютерами.

3. Стандарты

184 Карточки тахографа должны соответствовать следующим стандартам:

- ISO/IEC 7810: Карточки идентификационные - физические характеристики,
- ISO/IEC 7816: Карточки идентификационные - карточки на интегральных схемах с контактами,
- Часть 1: Физические характеристики,
- Часть 2: Размеры и расположение контактов,
- Часть 3: Электронные сигналы и протоколы передачи данных,
- Часть 4: Межотраслевые команды обмена данными,
- Часть 8: Межотраслевые команды обеспечения защиты,
- ISO/IEC 10373: Карточки идентификационные - методы проверки.

4. Спецификации на окружающие условия и электромагнитную совместимость

185 Карточки тахографа должны быть способны правильно работать во всех климатических условиях, которые обычно встречаются на территории Договаривающихся сторон как минимум в диапазоне температур от -25°C до +70°C с нерегулярными пиковыми значениями до +85°C; при этом термин "нерегулярные" означает не более 4 часов каждый раз и не более 100 раз в течение всего срока использования карточки.

186 Карточки тахографа должны быть способны работать нормально в условиях влажности в диапазоне от 10% до 90%.

187 Карточки тахографа должны быть способны правильно работать в течение пяти лет, если они используются с соблюдением указанных спецификаций на окружающие условия и электромагнитную совместимость.

188 В процессе работы карточки тахографа должны соответствовать Правилам ЕЭК № 10[11], касающимся электромагнитной совместимости, и должны быть защищены от электростатических разрядов.

5. Хранение данных

Для целей настоящего пункта

- время регистрируется с точностью до одной минуты, если не предусмотрено иное,
- показания счетчика пробега регистрируются с точностью до 1 км,
- скорость регистрируется с точностью до 1 км/ч.

Функции, команды и логические структуры карточек тахографа, соответствующие требованиям, предъявляемым к хранению данных, указываются в подразделе 2.

189 В настоящем пункте определяется минимальный объем памяти хранения различных файлов данных соответствующих приложений. Карточки тахографа должны быть способны передавать контрольному устройству данные о фактическом объеме памяти хранения данных этих файлов.

Любые дополнительные данные, которые могут храниться на карточках тахографа, связанные с иными приложениями, предусмотренными в соответствующих случаях карточкой, хранятся в соответствии с Европейскими положениями[12], касающимися

---

[11] Исходным текстом в ЕС является директива Комиссии 95/54/ЕС от 31 октября 1995 года, предусматривающая приведение директивы Совета 72/245/ЕС о сближении законодательства государств-членов, регламентирующего подавление радиопомех, производимых двигателями с искровым зажиганием, установленными на автотранспортных средствах, в соответствие с техническим прогрессом (OJ No. L 266, 08/11/1995).

[12] Защита физических лиц в части обработки личных данных и беспрепятственной передачи таких данных соответствует положениям директивы Совета № 95/46/ЕС от 24 октября 1995 года с внесенными в них последними поправками (OJ No. L 281, 23/11/1995).

защиты физических лиц в части обработки личных данных и беспрепятственной передачи таких данных.

5.1 Идентификация карточки и данные о защите

5.1.1 Идентификация приложений

190 Карточки тахографа должны быть способны хранить следующие идентификационные данные приложений:

- идентификационные данные приложения тахографа,
- идентификационные данные типа карточки тахографа.

5.1.2 Идентификация микропроцессора

191 Карточки тахографа должны быть способны хранить следующие идентификационные данные интегральной схемы (ИС):

- серийный номер ИС,
- исходные заводские данные ИС.

5.1.3 Идентификация карточки на интегральной схеме

192 Карточки тахографа должны быть способны хранить следующие идентификационные данные карточки на интегральной схеме:

- серийный номер карточки (включая исходные заводские данные),
- номер официального утверждения типа карточки,
- идентификатор учреждения, персонализирующего карточку (ИД),
- ИД монтажного предприятия,
- идентификатор ИС.

5.1.4 Элементы защиты

193 Карточки тахографа должны быть способны хранить следующие элементы данных, касающихся защиты:

- европейский открытый ключ,
- сертификат Договаривающейся стороны,

- сертификат карточки,
- закрытый ключ карточки.

5.2 Карточка водителя

5.2.1 Идентификация карточки

194 Карточка водителя должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшая Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,
- дата начала действия карточки, дата истечения срока действия карточки.

5.2.2 Идентификация держателю карточки

195 Карточка водителя должна быть способна хранить следующие идентификационные данные держателя карточки:

- фамилия держателя,
- имя (имена) держателя,
- дата рождения,
- предпочитаемый язык.

5.2.3 Информация о водительском удостоверении

196 Карточка водителя должна быть способна хранить следующие данные о водительском удостоверении:

- выдавшая Договаривающаяся сторона, название выдавшего компетентного органа,
- номер водительского удостоверения (на дату выдачи карточки).

5.2.4 Данные об используемом транспортном средстве

197 Карточка водителя должна быть способна хранить за каждый календарный день, в течение которого используется эта карточка, и за каждый период использования данного транспортного средства в течение указанного дня (период использования

включает все последовательные циклы ввода/извлечения данной карточки на транспортном средстве) следующие данные:

- дата и время первого использования транспортного средства (т.е. первый ввод карточки за этот период использования транспортного средства или 00:00 часов, если в этот момент данный период использования продолжается),

- показание счетчика пробега транспортного средства в это время,

- дата и время последнего использования транспортного средства (т.е. последнее извлечение карточки в течение этого периода использования транспортного средства или 23 ч. 59 м., если в этот момент использование продолжается),

- показания счетчика пробега транспортного средства в это время,

- номер регистрации транспортного средства (VRN) и Договаривающаяся сторона регистрации данного транспортного средства.

198 Карточка водителя должна быть способна хранить как минимум 84 такие записи.

5.2.5 Данные о деятельности водителя

199 Карточка водителя должна быть способна хранить за каждый календарный день, в течение которого используется данная карточка или в течение которого водитель внес вручную данные о своей деятельности, следующие данные:

- дата,

- счетчик ежедневного присутствия (показания которого увеличиваются на одну единицу за каждый календарный день),

- общее расстояние, пройденное водителем на транспортном средстве в течение этого дня,

- статус водителя на 00:00 часов,

- во всех случаях когда водитель меняет вид деятельности и/или статус управления и/или вставляет или извлекает свою карточку:

- статус управления (CREW, SINGLE) (ЭКИПАЖ, ОДИН),

- считывающее устройство (DRIVER, CO-DRIVER) (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ),

- положение карточки (INSERTED, NOT INSERTED) (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА),

- виды деятельности (DRIVING, AVAILABILITY, WORK, BREAK/REST) (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ),

- время изменения.

200 Блок памяти карточки водителя должен быть способен хранить данные о деятельности водителя как минимум за последние 28 дней (показатель усредненной деятельности водителя определяется в качестве 93 изменений видов деятельности в день).

201 Данные, перечисленные в позициях 197 и 199, должны храниться таким образом, чтобы данные о видах деятельности можно было извлечь из памяти в хронологическом порядке их ввода, даже в случае нестыковки времени.

5.2.6 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы

202 Карточка водителя должна быть способна хранить следующие данные, касающиеся мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, введенные водителем:

- дата и время ввода (или дата/время, относящиеся к вводу этих данных, если этот ввод производится вручную),
- тип ввода (начало или конец, условия ввода),
- страна или район въезда,
- показания счетчика пробега транспортного средства.

203 Блок памяти карточки водителя должен быть способен хранить как минимум 42 пары таких записей.

5.2.7 Данные о событиях

Для целей настоящего подпункта данные о времени должны регистрироваться с точностью до одной секунды.

204 Карточка водителя должна быть способна хранить данные, касающиеся соответствующих событий, обнаруженных контрольным устройством со вставленной в него карточкой:

- нестыковка времени (в тех случаях когда причиной этого события является данная карточка),
- ввод карточки в процессе управления (в тех случаях когда причиной этого события является данная карточка),
- последний сеанс использования карточки, который был завершен неправильно (в тех случаях когда причиной этого события является данная карточка),
- прекращение электропитания,
- ошибка данных о движении,
- попытки нарушения защиты.

205 Карточка водителя должна быть способна хранить следующие данные об этих событиях:

- код события,
- дата и время начала события (или ввода карточки, если это событие в данный момент продолжается),
- дата и время конца события (или извлечения карточки, если в данный момент это событие продолжается),
- регистрационный номер транспортного средства (VRN) и Договаривающаяся сторона регистрации транспортного средства, к которому относится это событие.

Примечание: В случае события "Нестыковка времени":

- дата и время начала события должны соответствовать дате и времени извлечения карточки из предыдущего транспортного средства,

- дата и время завершения события должны соответствовать дате и времени ввода карточки в транспортное средство, используемое в данный момент,

- данные о транспортном средстве должны соответствовать используемому транспортному средству, к которому относится данное событие.

Примечание: В случае события "последний сеанс использования карточки завершен неправильно":

- дата и время начала события должны соответствовать дате и времени ввода карточки применительно к неправильно завершенному сеансу ее использования,

- дата и время завершения события должны соответствовать дате и времени ввода карточки, относящегося к сеансу ее использования, в ходе которого было обнаружено данное событие (текущий сеанс),

- данные о транспортном средстве должны соответствовать транспортному средству, на котором сеанс использования карточки был завершен неправильно.

206 Карточка водителя должна быть способна хранить данные о шести самых последних событиях каждого типа (т.е. 36 событий).

5.2.8 Данные о неисправностях

Для целей этого подпункта время регистрируется с точностью до одной секунды.

207 Карточка водителя должна быть способна хранить данные, касающиеся следующих неисправностей, обнаруженных устройством с введенной в него карточкой:

- сбой в работе карточки (в том случае если причиной события является карточка),

- сбой в работе контрольного устройства.

208 Карточка водителя должна быть способна хранить следующие данные об этих неисправностях:

- код неисправности,

- дата и время начала неисправности (или ввода карточки, если на данный момент времени неисправность сохраняется),

- дата и время прекращения неисправности (или извлечения карточки, если в данный момент времени неисправность сохраняется),

- регистрационный номер транспортного средства (VRN) и страна регистрации транспортного средства, на котором произошла данная неисправность.

209 Карточка водителя должна быть способна хранить данные о 12 самых последних неисправностях каждого типа (т.е. 24 неисправности).

5.2.9 Данные о проверочных операциях

210 Карточка водителя должна быть способна хранить следующие данные, касающиеся проверочных операций:

- дата и время проверки,

- номер контрольной карточки и название выдавшей ее Договаривающейся стороны,

- тип проверки (вывод на дисплей и/или на печать, и/или загрузка данных с бортового устройства, и/или загрузка данных с карточки (см. примечание)),

- период, за который загружаются данные, - в случае загрузки,

- регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации транспортного средства, на котором производилась проверка.

Примечание: Требования, предъявляемые к защите, предполагают, что факт загрузки данных с карточки будет регистрироваться только в том случае, если он производится с помощью контрольного устройства.

211 Карточка водителя должна быть способна хранить одну такую запись.

5.2.10 Данные о сеансе использования карточки

212 Карточка водителя должна быть способна хранить данные, касающиеся транспортного средства, на котором был начат сеанс ее использования:

- дата и время начала сеанса (т.е. ввода карточки) с точностью до одной секунды,

- регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации.

5.2.11 Данные об особых ситуациях

212a Карточка водителя должна быть способна хранить следующие данные, касающиеся особых ситуаций, введенных в то время, когда карточка была вставлена в контрольное устройство (независимо от считывающего устройства):

- дата и время начала ввода,

- тип особой ситуации.

212b Карточка водителя должна быть способна хранить 56 таких записей.

5.3 Карточка мастерской

5.3.1 Элементы защиты

213 Карточка мастерской должна быть способна хранить персональный идентификационный номер (PIN-код).

214 Карточка мастерской должна быть способна хранить криптографические ключи, необходимые для подсоединения датчиков движения к бортовым устройствам.

5.3.2 Идентификация карточки

215 Карточка мастерской должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшая ее Договаривающаяся сторона, название выдавшего ее компетентного органа, дата выдачи,
- дата начала действия карточки, дата истечения срока действия карточки.

5.3.3 Идентификация держателя карточки

216 Карточка мастерской должна быть способна хранить следующие идентификационные данные о держателе карточки:

- название мастерской,
- адрес мастерской,
- фамилия держателя,
- имя (имена) держателя,
- предпочитаемый язык.

5.3.4 Данные об используемом транспортном средстве

217 Карточка мастерской должна быть способна хранить записанные данные об используемых транспортных средствах таким же образом, как и карточка водителя.

218 Карточка мастерской должна быть способна хранить как минимум четыре таких записи.

5.3.5 Данные о деятельности водителя

219 Карточка мастерской должна быть способна хранить данные о деятельности водителя таким же образом, как и карточка водителя.

220 Карточка мастерской должна быть способна хранить данные о деятельности водителя как минимум за один день усредненной деятельности водителя.

5.3.6 Данные о начале и/или завершении ежедневных периодов работы

221 Карточка мастерской должна быть способна хранить записанные данные о начале и/или завершении ежедневных периодов работы таким же образом, как и карточка водителя.

222 Карточка мастерской должна быть способна хранить как минимум три пары таких записей.

5.3.7 Данные о событиях и неисправностях

223 Карточка мастерской должна быть способна хранить записанные данные о событиях и неисправностях таким же образом, как и карточка водителя.

224 Карточка мастерской должна быть способна хранить данные о трех самых последних событиях каждого типа (т.е. 18 событий) и о шести самых последних неисправностях каждого типа (т.е. 12 неисправностей).

5.3.8 Данные о проверочных операциях

225 Карточка мастерской должна быть способна хранить записанные данные о проверочных операциях таким же образом, как и карточка водителя.

5.3.9 Данные о калибровке и корректировке времени

226 Карточка мастерской должна быть способна хранить записанные данные о калибровке и/или корректировке времени, произведенной в то время, когда карточка была вставлена в контрольное устройство.

227 Каждая запись калибровки должна быть способна хранить следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция),
- идентификация транспортного средства,
- обновленные или подтвержденные параметры (w, k, l, размер шин, регулировка устройства ограничения скорости, показания счетчика пробега (новые и прежние показания), дата и время (новые и прежние показания)),

- идентификация контрольного устройства (номер деталей бортового устройства (БУ), серийный номер бортового устройства (БУ), серийный номер датчика движения).

228 Карточка мастерской должна быть способна хранить как минимум 88 таких записей.

229 Карточка мастерской должна иметь счетчик, указывающий число калибровок, произведенных на карточке.

230 Карточка мастерской должна иметь счетчик, указывающий общее число калибровок, произведенных с момента последней загрузки данных.

5.3.10 Данные об особых ситуациях

230a Карточка мастерской должна быть способна хранить данные, касающиеся особых ситуаций, таким же образом, как и карточка водителя. Карточка мастерской должна быть способна хранить две такие записи.

5.4 Карточка контролера

5.4.1 Идентификация карточки

231 Карточка мастерской должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,

- выдавшая ее Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,

- дата начала действия карточки, дата истечения срока действия карточки (в соответствующем случае).

5.4.2 Идентификация держателя карточки

232 Карточка контролера должна быть в состоянии хранить следующие идентификационные данные держателя карточки:

- название контрольного органа,
- адрес контрольного органа,
- фамилия держателя,
- имя (имена) держателя,
- предпочитаемый язык.

5.4.3 Данные о проверочных операциях

233 Карточка контролера должна быть способна хранить следующие данные о проверочных операциях:

- дата и время проверки,
- тип проверки (вывод на дисплей и/или на печать и/или загрузка данных с бортового устройства и/или загрузка с карточки),
- период, за который загружаются данные (в соответствующих случаях),
- регистрационный номер транспортного средства (VRN) компетентный орган Договаривающейся стороны, зарегистрировавший проверенное транспортное средство,
- номер проверенной карточки водителя и выдавшая ее Договаривающаяся сторона.

234 Карточка контролера должна быть способна хранить как минимум 230 таких записей.

5.5 Карточка предприятия

5.5.1 Идентификация карточки

235 Карточка предприятия должна быть способна хранить идентификационные данные карточки:

- номер карточки,
- выдавшая ее Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,

- дата начала действия карточки, дата истечения срока действия карточки (в соответствующем случае).

5.5.2 Идентификация держателя карточки

236 Карточка предприятия должна быть способна хранить следующие идентификационные данные держателя карточки:

- название предприятия,
- адрес предприятия.

5.5.3 Данные о действиях предприятия

237 Карточка предприятия должна быть способна хранить следующие данные о действиях предприятия:

- дата и время соответствующего действия,
- тип действия (блокировка и/или разблокировка бортового устройства и/или загрузка данных с бортового устройства и/или загрузка данных с карточки),
- период, за который загружаются данные (в соответствующем случае),
- регистрационный номер транспортного средства (VRN) и компетентный орган Договаривающейся стороны, зарегистрировавшей транспортное средство,
- номер карточки и название выдавшей ее Договаривающейся стороны (в случае загрузки данных с карточки).

238 Карточка предприятия должна быть способна хранить как минимум 230 таких записей.

V. УСТАНОВКА КОНТРОЛЬНОГО УСТРОЙСТВА

1. Установка

239 Новые контрольные устройства поставляются механикам и изготовителям транспортного средства неактивированными со всеми параметрами калибровки, перечисленными в главе III.20, выставленными на соответствующие и действующие значения по умолчанию. В тех случаях, когда какое-либо конкретное значение не соответствует заданному, буквенные параметры отображаются в виде строк из вопросительных знаков "?", а числовые параметры устанавливаются на ноль "0".

240 До активации контрольное устройство должно обеспечивать доступ к функции калибровки, даже если в режим калибровки оно не установлено.

241 До активации контрольное устройство не должно ни регистрировать, ни хранить данные, указанные в пунктах III.12.3-III.12.9 и III.12.12-III.12.14, включительно.

242 В процессе установки изготовители транспортных средств предварительно устанавливают все известные параметры.

243 Изготовители транспортных средств или механики должны активировать установленное контрольное устройство до выезда транспортного средства из цеха, в котором производилась установка.

244 Активация контрольного устройства должна производиться автоматически в результате первого ввода карточки предприятия в любое из считывающих устройств карточки.

245 Конкретные операции по подсоединению датчика движения и бортового устройства, если таковые требуются, должны производиться автоматически до или во время активации.

246 После активации контрольное устройство должно полностью обеспечивать контроль за доступом к функциям и соответствующим данным.

247 Функции регистрации и хранения контрольного устройства после его активации должны быть полностью работоспособными.

248 После установки производится калибровка. Первая калибровка должна включать ввод регистрационного номера транспортного средства (VRN) и должна производиться не позже, чем через две недели после установки или присвоения регистрационного номера транспортного средства, в зависимости от того, какое из этих событий наступает позже.

248a Контрольное устройство должно быть установлено в транспортном средстве таким образом, чтобы водитель имел доступ ко всем необходимым функциям со своего места.

2. Установочная табличка

249 После проверки установленного контрольного устройства на него, внутри или сзади, должна устанавливаться четко видимая и легко доступная установочная табличка. После каждой инспекции, проведенной уполномоченным механиком или мастерской, на месте прежней таблички устанавливается новая.

250 На табличке должны содержаться как минимум следующие данные:

- название, адрес или фирменный знак уполномоченного механика или предприятия,
- характеристический коэффициент транспортного средства в форме "w = imp/km"... ("w = ... имп./км"),
- постоянная контрольного устройства в форме "k = ... imp/km" ("k = имп./км")
- эффективная окружность шин колес в форме "l = ... mm" ("l = мм"),
- размер шин,
- дата определения характеристического коэффициента транспортного средства и измерение эффективной окружности шин колес,
- опознавательный номер транспортного средства.

3. Наложение пломб

251 Пломбы накладываются на следующие детали:

- любое соединение, которое в случае его нарушения приведет к необнаруживаемым изменениям или к необнаруживаемой потере данных;

- установочную табличку, если только она не прикреплена таким образом, что ее нельзя снять, не повредив нанесенную на ней маркировку.

252 Указанные выше пломбы могут быть сняты:

- в случае аварийной ситуации,

- в целях установки, регулировки или ремонта устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения, при условии, что контрольное устройство продолжает функционировать надежно и правильно и пломбируется уполномоченным механиком или предприятием (в соответствии с главой VI) сразу же после установки устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения или в течение семи дней в других случаях.

253 Каждый случай нарушения этих пломб должен быть предметом письменного уведомления компетентного органа с указанием причин, по которым были произведены такие действия.

VI. ПРОВЕРКА, ИНСПЕКЦИЯ И РЕМОНТ

Требования, регламентирующие обстоятельства, в которых могут быть сняты пломбы, как указано в пункте 5 статьи 9 приложения к настоящему Соглашению, определяются в части 3 главы V настоящего добавления.

1. Утверждение механиков или мастерских

Договаривающаяся сторона утверждает, регулярно контролирует и аттестует организации, которым поручена:

- установка,
- проверка,
- инспекция,
- ремонт.

На основании пункта 1 статьи 9 приложения к настоящему Соглашению карточки мастерской выдаются только механикам и/или мастерским, которые уполномочены производить активацию и/или калибровку контрольного устройства в соответствии с настоящим добавлением и, за исключением должным образом обоснованных случаев:

- которые не имеют права на карточку предприятия,
- и иная профессиональная деятельность которых не может поставить под угрозу общую защиту системы, определенную в подразделе 10.

2. Проверка новых или отремонтированных приборов

254 Каждое отдельное устройство, будь то новое или отремонтированное, должно проверяться на предмет его надлежащего функционирования и точности его показаний и записей в пределах, изложенных в главе III.2.1 и III.2.2, посредством наложения пломб в соответствии с главой V.3 и в соответствии с параметрами калибровки.

3. Инспекция после установки

255 Во время установки на транспортное средство весь сборочный узел, включая контрольное устройство, должен соответствовать положениям, регламентирующим максимальные допуски, указанные в главе III.2.1 и III.2.2.

4. Периодические инспекции

256 Периодические инспекции оборудования, установленного на транспортных средствах, должны производиться после любого ремонта такого оборудования или после любого изменения характеристического коэффициента транспортного средства или эффективной окружности шин или в том случае, если часы, показывающие время UTC, спешат или отстают более чем на 20 минут, или в случае изменения регистрационного номера транспортного средства (VRN) не реже одного раза в два года (24 месяца) после последней инспекции.

257 Эти инспекции включают следующие проверки, имеющие целью убедиться в том, что:

- контрольное устройство работает нормально, включая функцию хранения данных на карточках тахографа,
- положения главы III.2.1 и III.2.2 о максимальных допусках при установке соблюдаются должным образом,
- на контрольном устройстве проставлен знак официального утверждения типа,
- установочная табличка имеется,
- пломбы на устройстве и других частях оборудования не нарушены,
- размер шин и фактическая окружность шин колес соответствуют нормам.

258 Эти инспекции включают калибровку.

5. Измерение погрешностей

259 Измерение погрешностей в процессе установки и в ходе эксплуатации производится в следующих условиях, которые должны рассматриваться в качестве обычных условий испытания:

- транспортное средство в снаряженном состоянии без груза,
- давление в шинах соответствует инструкциям изготовителя,
- износ шин в пределах, допускаемых национальным законодательством,
- движение транспортного средства,
- транспортное средство движется вперед на своем двигателе по прямой линии по ровной дороге на скорости 50±5 км/ч. Измеряемое расстояние должно составлять не менее 1 000 метров,

– для проведения этого испытания могут также использоваться альтернативные методы, например использование соответствующего испытательного стенда при условии обеспечения сопоставимой точности.

6. Ремонт

260 Мастерские должны иметь возможность загружать данные с контрольного устройства для их передачи соответствующему транспортному предприятию.

261 Утвержденные мастерские должны выдавать транспортным предприятиям свидетельство, подтверждающее невозможность загрузки данных в том случае, когда неисправность контрольного устройства не позволяет загрузить ранее записанные данные даже после ремонта, произведенного данной мастерской. Мастерские хранят копию каждого выданного свидетельства в течение как минимум одного года.

VII. ВЫДАЧА КАРТОЧЕК

Порядок выдачи карточек, установленный Договаривающимися сторонами, должен соответствовать следующим предписаниям.

262 В случае первой выдачи карточки тахографа соответствующему заявителю номер карточки должен иметь порядковый индекс (в случае применимости), индекс замены и индекс возобновления, установленные на "0".

263 В случае всех неиндивидуальных карточек тахографа, выданных одному контрольному органу или одной мастерской или одному транспортному предприятию, первые 13 цифр номеров карточек должны быть одинаковыми, но порядковый индекс должен быть иным.

264 Карточка тахографа, выданная в порядке замены существующей карточки тахографа, должна иметь тот же номер, что и номер замененной карточки, за исключением индекса замены, который увеличивается на 1 (в порядке 0, ..., 9, A, ..., Z).

265 Карточка тахографа, выданная в порядке замены существующей карточки тахографа, должна иметь ту же дату истечения срока действия, что и замененная карточка.

266 Карточка тахографа, выданная в порядке возобновления существующей карточки тахографа, должна иметь тот же номер карточки, что и возобновленная карточка, за исключением индекса замены, который устанавливается на "0", и индекса возобновления, который увеличивается на 1 (в порядке 0, ..., 9, A, ..., Z).

267 Обмен существующей карточки тахографа в целях изменения административной даты производится в соответствии с правилами возобновления, если это происходит в той же Договаривающейся стороне или в соответствии с правилами первой выдачи карточки, если это происходит в другой Договаривающейся стороне.

268 В случае неиндивидуальных карточек мастерской или контрольных карточек в позиции "card holder surname" (фамилия держателя карточки), проставляется название мастерской или контрольного органа.

VIII. ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА КОНТРОЛЬНОГО УСТРОЙСТВА И КАРТОЧЕК ТАХОГРАФА

1. Общие положения

Для целей настоящей главы слова "control device" (контрольное устройство) означает контрольное устройство или его компоненты. Официальное утверждение типа электропроводки, связывающей датчик движения с бортовым устройством, не требуется. Бумага, используемая контрольным устройством, рассматривается в качестве одного из компонентов контрольного устройства.

269 Контрольное устройство представляется на официальное утверждение в сборе вместе со всеми комплектующими дополнительными устройствами.

270 Официальное утверждение типа контрольного устройства и карточек тахографа должна включать соответствующую проверку защиты, функциональную проверку и проверку на эксплуатационную совместимость. Положительные результаты каждой из этих проверок должны подтверждаться соответствующим сертификатом.

271 Компетентные органы Договаривающейся стороны, предоставляющие официальное утверждение типа, выдают свидетельство об официальном утверждении типа контрольного устройства или карточки тахографа, представленных на официальное утверждение типа, в соответствии со статьей 2 приложения к ЕСТР только при наличии:

- сертификата защиты,
- сертификата функциональности,
- сертификата эксплуатационной совместимости.

272 Любое изменение программного обеспечения или аппаратного оборудования или характера материалов, использованных для его изготовления, должно в предварительном порядке доводиться до сведения компетентного органа, который предоставил официальное утверждение оборудования по типу конструкции. Этот орган должен подтвердить изготовителю факт распространения официального утверждения данного типа или потребовать обновления или подтверждения соответствующего сертификата функциональности, сертификата защиты и/или сертификата эксплуатационной совместимости.

273 Процедуры совершенствования программного обеспечения контрольного устройства непосредственно на месте должны утверждаться компетентным органом, выдавшим

официальное утверждение типа контрольного устройства. Усовершенствованная версия программного обеспечения не должна приводить к изменению или стиранию любых данных о деятельности водителя, хранящихся в блоке памяти контрольного устройства. Усовершенствование программного обеспечения может производиться только под ответственность изготовителя данного устройства.

2. Сертификат защиты

274 Сертификат защиты выдается в соответствии с положениями подраздела 10 настоящего добавления.

3. Сертификат функциональности

275 Каждый претендент на получение официального утверждения типа направляет компетентному органу Договаривающейся стороны, предоставляющему официальное утверждение типа, все материалы и документацию, которые этот компетентный орган считают необходимыми.

276 Сертификат функциональности выдается изготовителю только по итогам всех требуемых успешно проведенных функциональных проверок, предусмотренных в подразделе 9.

277 Сертификат функциональности выдается компетентным органом, предоставляющим официальное утверждение типа. В этом сертификате должен содержаться, помимо названия его владельца и идентификационных данных модели, подробный перечень произведенных проверок и полученных результатов.

4. Сертификат эксплуатационной совместимости

278 Проверки на эксплуатационную совместимость проводятся одной и той же компетентной лабораторией, признанной на международном уровне.

279 Эта лаборатория регистрирует заявки на проведение проверок на эксплуатационную совместимость, представленные изготовителями, в хронологическом порядке их поступления.

280 Заявки официально регистрируются только в случае предоставления в распоряжение лаборатории:

- всего комплекта материалов и документов, необходимых для проведения таких проверок на предмет эксплуатационной совместимости,
- соответствующего сертификата защиты,
- соответствующего сертификата функциональности.

Дата регистрации заявки доводится до сведения изготовителя.

281 Проверки на эксплуатационную совместимость контрольного устройства или карточки тахографа, на которые не был выдан сертификат защиты или сертификат функциональности, лабораторией не проводятся.

282 Любой изготовитель, подавший заявку на проведение проверок на эксплуатационную совместимость, берет на себя обязательство передать на хранение лаборатории, уполномоченной проводить эти проверки, весь комплект материалов и документов, которые он предоставил для проведения этих проверок.

283 Проверки на эксплуатационную совместимость всех типов контрольных устройств или карточек тахографа:

- в случае которых официальное утверждение типа продолжает действовать или
- в случае которых официальное утверждение типа находится на рассмотрении и на которые действующие сертификаты эксплуатационной совместимости не выданы, проводятся в соответствии с положениями пункта 5 подраздела 9 настоящего добавления.

284 Сертификат эксплуатационной совместимости выдается лабораторией изготовителю только по итогам всех требуемых успешно проведенных проверок на эксплуатационную совместимость.

285 Если одно или более контрольных устройств или карточек тахографа не прошли проверки на эксплуатационную совместимость, как это предусмотрено требованием 283, то сертификат эксплуатационной совместимости не выдается до тех пор, пока изготовитель, представивший заявку, не произведет необходимые изменения и не проведет успешные проверки на эксплуатационную совместимость. Лаборатория определяет причину проблемы с помощью изготовителей, которых касается данное несоответствие требованиям к эксплуатационной совместимости, и стремится оказать изготовителю, подавшему заявку, помощь в поиске соответствующего технического решения. В том случае, если изготовитель модифицировал свое изделие, он обязан удостовериться в соответствующих

компетентных органах в том, что сертификат защиты и сертификат функциональности продолжают действовать.

286 Сертификат об эксплуатационной совместимости действует в течение шести месяцев. Если изготовитель не получил соответствующее свидетельство об официальном утверждении типа, его срок действия в конце этого периода истекает. Он препровождается изготовителем компетентному органу Договаривающейся стороны, предоставляющему официальное утверждение типа, который выдал сертификат функциональности.

287 Любой элемент, который может явиться причиной несоответствия требованиям к эксплуатационной совместимости, не должен использоваться в целях получения какой бы то ни было выгоды или приводить к созданию доминирующего положения.

5. Свидетельство об официальном утверждении типа

288 Орган Договаривающейся стороны, предоставляющий официальное утверждение типа, может выдавать свидетельство об официальном утверждении типа после того, как он получает в свое распоряжение все три требуемых сертификата.

289 Копия свидетельства об официальном утверждении типа направляется компетентным органом, предоставляющим официальное утверждение типа, лаборатории, уполномоченной проводить проверки на эксплуатационную совместимость, в момент его выдачи изготовителю.

290 Лаборатория, уполномоченная проводить проверки на эксплуатационную совместимость, должна вести открытый вебсайт, на котором должен содержаться обновленный перечень образцов контрольных устройств или карточек тахографа:

- в отношении которых была зарегистрирована заявка на проведение проверок на эксплуатационную совместимость,
- на которые был выдан сертификат эксплуатационной совместимости (даже временный),
- на которые было выдано свидетельство об официальном утверждении типа.

6. Зарезервировано

Эта часть (Исключительная процедура: первый сертификат эксплуатационной совместимости) к ЕСТР не относится.

ПОДРАЗДЕЛ I

СЛОВАРЬ ДАННЫХ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

I. Введение

В настоящем подразделе уточняются форматы данных, элементы данных и структуры данных, подлежащие использованию в контрольных устройствах и карточках тахографа.

1.1 Метод определения типов данных

Для определения типов данных в настоящем подразделе используется абстрактное описание синтаксиса версии 1 (ASN.1). Он позволяет определить простые и структурированные данные, не прибегая к помощи какого-либо конкретного синтаксиса передачи (правил кодирования), который зависит от приложения и операционной среды.

Правила присвоения названий типа ASN.1 соответствуют стандарту ISO/IEC 8824-1. Это предполагает, что:

- при возможности смысл соответствующего типа данных косвенно заложен в выбранных названиях,

- в том случае, если какой-либо тип данных состоит из других типов данных, то название этого типа данных и в этом случае представляет собой простую последовательность буквенных знаков, которая начинается с заглавной буквы; вместе с тем заглавные буквы используются и в названии с целью придать данным соответствующий смысл,

- в целом название типов данных соотносится к названию тех типов данных, с помощью которых они построены, с оборудованием, в которых хранятся данные, и с функцией, имеющей отношение к данным.

Если какой-либо тип ASN.1 уже определен в качестве того или иного стандарта и если он подходит для использования в контрольном устройстве, то в этом подразделе будет определен и этот тип ASN.1.

Для того чтобы можно было использовать несколько типов правил кодирования, некоторые типы ASN.1 в настоящем подразделе ограничиваются соответствующими идентификаторами диапазона значений. Идентификаторы диапазона значений определяются в пункте 3.

1.2 Источники

В настоящем подразделе используются следующие источники:

ISO 639	Код отображения названий языков. Издание первое: 1988 год.
EN 726-3	Системы карточек идентификационных - Телекоммуникационные карточки и терминалы на интегральной схеме (интегральных схемах) - Часть 3: Требования, не зависимые от вида приложения, которым должны удовлетворять карточки. Декабрь 1994 года
ISO 3779	Дорожные транспортные средства - Опознавательный номер транспортного средства (VIN) - Содержание и структура. Издание 3: 1083 год.
ISO/IEC 7816-5	Информационные технологии - Карточки идентификационные - Карточки на интегральной схеме (интегральных схемах) с контактами - Часть 5: Система нумерации и процедура регистрации идентификаторов приложений. Издание первое: 1994 год плюс поправка 1: 1996 год.
ISO/IEC 8824-1	Информационные технологии - Абстрактное описание синтаксиса версии 1 (ASN.1): Спецификация на базовое описание. Издание 2: 1998 год.
ISO/IEC 8825-2	Информационные технологии - Правила кодирования ASN.1: Спецификация на правила кодирования в сжатом формате (PER). Издание 2: 1998 год.
ISO/IEC 8859-1	Информационные технологии - 8-битовые однобайтовые наборы закодированных графических знаков - часть 1: Латинский алфавит № 1. Издание первое: 1998 год.
ISO/IEC 8859-7	Информационные технологии - 8-битовые однобайтовые наборы закодированных графических знаков - часть 7: Латинский/греческий алфавит. Издание первое: 1987 год.
ISO 16844-3	Дорожные транспортные средства - Системы тахографа - Интерфейс датчика движения. WD 3-20/05/99.

2. Определения типов данных

В случае любого из следующих типов данных значение по умолчанию содержания "unknown" ("нет данных") или "not applicable" ("не применимо") определяется посредством заполнения соответствующего элемента данных с помощью байтов 'FF'.

2.1 ActivityChangeInfo (данные об изменении вида деятельности)

Этот тип данных позволяет кодировать с помощью слова из двух байтов состояние считывающего устройства в 00:00 часов и статус водителя в 00:00 часов и/или изменения вида деятельности и/или изменения статуса управления и/или изменения положения карточки водителя или второго водителя. Этот тип данных относится к требованиям 084, 109a, 199 и 219.

ActivityChangeInfo ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))

Присвоение значения - выровненный байт: 'scpaatttttttttt'B (16 бит)

Для записи данных в блок памяти (или состояние считывающего устройства):

's'B Считывающее устройство:
'0'B: DRIVER (ВОДИТЕЛЬ),
'1'B: CO-DRIVER (ВТОРОЙ ВОДИТЕЛЬ),

'c'B Статус управления:
'0'B: SINGLE (ОДИН),
'1'B: CREW (ЭКИПАЖ),

'p'B Положение карточки водителя (или мастерской) в соответствующем считывающем устройстве:
'0'B: INSERTED, карточка вставлена,
'1'B: NOT INSERTED, карточка не вставлена (или карточка извлечена),

'aa'B Вид деятельности:
'00'B: BREAK/REST (ПЕРЕРЫВ/ОТДЫХ),
'01'B: AVAILABILITY (ГОТОВНОСТЬ),
'10'B: WORK (РАБОТА),
'11'B: DRIVING (УПРАВЛЕНИЕ),

‘ttttttttttt’B Время изменения: число минут начиная с 00:00 часов на данный день.

Для записи данных на карточку водителя (или мастерской) (и статуса водителя):

‘s’B Считывающее устройство (не применимо, если ‘p‘ = 1, за исключением случая, указанного ниже):
‘0’B: DRIVER (ВОДИТЕЛЬ),
‘1’B: CO-DRIVER (ВТОРОЙ ВОДИТЕЛЬ),

‘c’B Статус управления (случай ‘p‘ = 0) или Следующий вид деятельности (случай ‘p‘ = 1):

‘0’B: SINGLE (ОДИН),	‘0’B: UNKNOWN (НЕТ ДАННЫХ)
‘1’B: CREW (ЭКИПАЖ),	‘1’B: KNOWN (ЕСТЬ ДАННЫЕ) (= введено вручную)

‘p’B Положение карточки:
‘0’B: INSERTED, карточка вставлена в контрольное устройство,
‘1’B: NOT INSERTED, карточка не вставлена (или карточка извлечена),

‘aa’B Вид деятельности (неприменимо, если ‘p’=1 и ‘c’=0, за исключением случая, указанного ниже):

‘00’B: ПЕРЕРЫВ/ОТДЫХ,
‘01’B: ГОТОВНОСТЬ,
‘10’B: РАБОТА,
‘11’B: УПРАВЛЕНИЕ,

‘ttttttttttt’B Время изменения: число минут, начиная с 00:00 часов на данный день.

Примечание в случае ‘извлечения карточки’:

Когда карточка извлечена:

- ‘s’ этот знак применим и указывает на считывающее устройство, из которого извлечена карточка,
- ‘c’ должно быть установлено на 0,
- ‘p’ должно быть установлено на 1,

- ‘aa’ должно кодировать текущий вид деятельности, выбранный в указанное время.

В результате ручного ввода биты ‘c’ и ‘aa’ в составе слова (хранящееся в памяти карточки) позднее могут быть стерты и на их место записаны другие данные, отражающие факт этого ввода.

2.2. Address (адрес)

Адрес.

```
Address ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   codePage                    ЦЕЛОЕ ЧИСЛО (0..255),
   address                     ОКТЕТНАЯ СТРОКА (РАЗМЕР (35))
}
```

codePage указывает на часть стандарта ISO/IEC 8859, используемую для кодирования адреса,

address - закодированный адрес в соответствии с ISO/IEC 8859.

2.3 BCDString (строка BCD)

BCDString используется для отображения десятичного числа в двоичном коде (BCD). Этот тип данных используется для отображения одного десятичного знака в полуоктете (4 бита). BCDString определяется в соответствии со стандартом ISO/IEC 8824-1 (тип строки знаков).

```
BCDString ::= ЗНАКОВАЯ СТРОКА (С КОМПОНЕНТАМИ {
   идентификация (С КОМПОНЕНТАМИ {
   устанавливает ПРИСУТСТВИЕ }) })
```

BCDString использует для описания строки нотацию ‘hstring’. Крайняя левая шестнадцатиричная цифра представляет собой самый значимый полубайт первого байта. Для получения нескольких октетов после крайнего левого полуоктета первого октета включается соответствующее число нулевых полуоктетов.

Допустимые цифры: 0, 1, .. 9.

2.4 CalibrationPurpose (цель калибровки)

Данный код указывает причину регистрации набора параметров калибровки. Этот тип данных относится к требованиям 097 и 098.

CalibrationPurpose ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения:

'00'H	зарезервированное значение
'01'H	активация: регистрация известных параметров калибровки в момент включения БУ
'02'H	первая установка: первая калибровка БУ после его активации
'03'H	установка: первая калибровка БУ на данном транспортном средстве
'04' H	периодическая инспекция.

2.5 CardActivityDailyRecord (запись вида деятельности на карточке)

Информация, которая хранится на карточке, относится к деятельности водителя за конкретный календарный день. Этот тип данных относится к требованиям 199 и 219.

```
CardActivityDailyRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   activityPreviousRecordLength        ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange),
   activityRecordLength                ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange),
   activityRecordDate                  Реальное время,
   activityDailyPresenceCounter        Счетчик ежедневного присутствия,
   activityDayDistance                 Расстояние,
   activityChangeInfo                  УСТАНОВЛЕННЫЙ РАЗМЕР (1..1440)
                                       ЭЛЕМЕНТА ДАННЫХ ActivityChangeInfo
}
```

activityPreviousRecordLength - общая длина предыдущей ежедневной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи (см. пункт 3: CardActivityLengthRange). Когда эта запись становится самой старой ежедневной записью, значение activityPreviousRecordLength должно устанавливаться на ноль.

activityRecordLength - общая длина данной записи в байтах. Максимальное значение определяется длиной ОКТЕТНОЙ СТРОКИ, содержащей эти записи.

activityRecordDate - дата записи.

activityDailyPresenceCounter - счетчик ежедневного наличия карточки на данный день.

activityDayDistance - общее расстояние, пройденное за данный день.

activityChangeInfo - набор данных типа ActivityChangeInfo в отношении водителя на данный день. Он может содержать максимум 1 440 значений (изменение вида деятельности 1 раз в минуту). Этот набор данных всегда включает кодирование статуса водителя (activityChangeInfo) на 00:00 часов.

2.6 CardActivityLengthRange (длина записи о деятельности на карточке)

Число байтов на карточке водителя или мастерской, которые предусмотрены для хранения записей, касающихся деятельности водителя.

CardActivityLengthRange ::= ЦЕЛОЕ ЧИСЛО $(0..2^{16}-1)$

Присвоение значения: см. пункт 3.

2.7 CardApprovalNumber (номер официального утверждения карточки)

Эта позиция определяет номер официального утверждения типа карточки.

Card Approval Number:: = Строка IA5 (РАЗМЕР(8))

Присвоение значения: Не определено.

2.8 CardCertificate (сертификат карточки)

Сертификат открытого ключа карточки.

CardCertificate: = Сертификат

2.9 CardChipIdentification (идентификация микропроцессора карточки)

Информация, записанная на карточке, которая относится к идентификации интегральной схемы карточки (ИС) (требование 191).

CardChipIdentification: = ПОСЛЕДОВАТЕЛЬНОСТЬ {

icSerialNumber	ОКТЕТНАЯ СТРОКА (РАЗМЕР (4)),
icManufacturingReferences	ОКТЕТНАЯ СТРОКА (РАЗМЕР (4))

}

icSerialNumber - серийный номер ИС, определенный в стандарте EN 726-3.

icManufacturingReferences - идентификатор изготовителя ИС и производственные данные, определенные в стандарте EN 726-3.

2.10 CardConsecutiveIndex (порядковый индекс карточки)

Порядковый индекс карточки (определение h)).

CardConsecutiveIndex: = строка IA5 (РАЗМЕР (1))

Присвоенние значения: (см. главу VII настоящего добавления)

Порядок увеличения: '0 , ..., 9, A , ... , Z , a , ... , z'

2.11 CardControlActivityDataRecord (запись данных о проверочных операциях)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к последней проверке, которой подвергался водитель (требования 210 и 225).

CardControlActivityDataRecord: = ПОСЛЕДОВАТЕЛЬНОСТЬ {

controlType	тип проверки,
controlTime	реальное время,
controlCardNumber	полный номер карточки,
controlVehicleRegistration	идентификация регистрации транспортного средства,
controlDownloadPeriodBegin	реальное время,
controlDownloadPeriodEnd	реальное время

}

controlType - тип проверки.

controlTime - дата и время проверки.

controlCardNumber - полный номер карточки инспектора, который произвел проверку.

controlVehicleRegistration - регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации транспортного средства, в которой была произведена проверка.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** - период, за который загружаются данные, в случае загрузки.

2.12 CardCurrentUse (текущее использование карточки)

Информация о фактическом использовании карточки (требование 212).

```
CardCurrentUse: = ПОСЛЕДОВАТЕЛЬНОСТЬ {
      sessionOpenTime              реальное время,
      sessionOpenVehicle           идентификация регистрации транспортного средства
}
```

sessionOpenTime - время, когда карточка была вставлена в считывающее устройство применительно к данному виду использования. В случае извлечения карточки этот элемент данных устанавливается на ноль.

sessionOpenVehicle - идентификация используемого в настоящее время транспортного средства, регистрируемая в момент ввода карточки. В случае извлечения карточки этот элемент данных устанавливается на ноль.

2.13 CardDriverActivity (деятельность водителя)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к деятельности водителя (требования 199 и 219).

```
CardDriverActivity: = ПОСЛЕДОВАТЕЛЬНОСТЬ {
      activityPointerOldestDayRecord    ЦЕЛОЕ ЧИСЛО (0.. CardActivityLengthRange-1),
      activityPointerNewestRecord       ЦЕЛОЕ ЧИСЛО (0.. CardActivityLengthRange-1),
      activityDailyRecords              ОКТЕТНАЯ СТРОКА
                                        (РАЗМЕР(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord - указание на начало блока памяти (число байтов с начала строки) для хранения самой старой ежедневной записи в строке activityDailyRecords. Максимальное значение определяется длиной строки.

activityPointerNewestRecord - указание на начало блока памяти (число байтов с начала строки) для хранения самой последней ежедневной записи в строке activityDailyRecords. Максимальное значение определяется длиной строки.

activityDailyRecords - место, имеющееся для хранения данных о деятельности водителя (структура данных: CardActivityDailyRecord) за каждый календарный день, в течение которого использовалась карточка.

Присвоение значения: данная октетная строка периодически заполняется записями типа CardActivityDailyRecord. При первом использовании хранение данных производится с начала первого байта строки. Все новые записи включаются в конце предыдущей. Когда вся строка заполняется, процесс хранения продолжается с первого байта строки, независимо от наличия разрыва в том или ином элементе данных. До включения в строку данных о новом виде деятельности (посредством расширения текущей позиции activityDailyRecord или включения новой позиции activityDailyRecord), которые записываются вместо прежних данных о деятельности; указатель activityPointerOldestDayRecord должен быть обновлен с целью отразить новое место хранения самой старой полной ежедневной записи, а указатель activityPreviousRecordLength этой (новой) самой старой полной ежедневной записи должен быть установлен на ноль.

2.14 CardDrivingLicenceInformation (информация о водительском удостоверении)

Информация, записанная на карточке водителя, которая относится к данным о водительском удостоверении держателя карточки (требование 196).

```
CardDrivingLicenceInformation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    drivingLicenceIssuingAuthority          название,
    drivingLicenceIssuingNation             числовой код страны,
    drivingLicenceNumber                    строка IA5 (РАЗМЕР (16))
}
```

drivingLicenceIssuingAuthority - орган, ответственный за выдачу водительского удостоверения.

drivingLicenceIssuingNation - национальная принадлежность органа, выдавшего водительское удостоверение.

drivingLicenceNumber - номер водительского удостоверения.

2.15 CardEventData (данные о событиях)

Информация, записанная на карточке водителя или мастерской, которая относится к событиям, связанным с держателем карточки (требования 204 и 223).

```
CardEventData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(6) {
    cardEventRecords            УСТАНОВЛЕННЫЙ РАЗМЕР(NoOfEventsPerType)
                                ЗАПИСИ CardEventRecord
}
```

CardEventData - последовательность записей cardEventRecords, записанная в порядке возрастания значения элемента EventFaultType (за исключением записей, касающихся нарушения защиты, которые группируются в последнем массиве данных данной последовательности).

cardEventRecords - набор записей о событиях данного типа (или категория событий, имеющих отношение к попыткам нарушения защиты).

2.16 CardEventRecord (запись о событиях)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к данному событию, связанному с держателем карточки (требования 205 и 223).

```
CardEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    eventType                   тип события/неисправности,
    eventBeginTime              реальное время,
    eventEndTime                реальное время,
    eventVehicleRegistration    идентификация регистрации транспортного средства
}
```

eventType - тип события.

eventBeginTime - дата и время начала события.

eventEndTime - дата и время завершения события.

eventVehicleRegistration - регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации транспортного средства, в которой произошло данное событие.

2.17 CardFaultData (данные о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к сбоям в работе, связанным с держателем карточки (требования 207 и 223).

```
CardFaultData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(2) {
    cardFaultRecords                УСТАНОВЛЕННЫЙ РАЗМЕР
                                    (NoOfFaultsPerType) ЗАПИСИ CardFaultRecord
}
```

CardFaultData - последовательность совокупности записей, отражающих неисправности контрольного устройства, за которой следует совокупность записей, отражающих сбои в работе карточек.

cardFaultRecords - совокупность записей о неисправностях, сгруппированных по данной категории неисправностей (контрольного устройства или карточки).

2.18 CardFaultRecord (запись о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к сбою в работе, связанному с держателем карточки (требования 208 и 223).

```
CardFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    faultType               тип события/сбоя в работе,
    faultBeginTime          реальное время,
    faultEndTime            реальное время,
    VehicleRegistration     идентификация регистрации транспортного средства
}
```

faultType - тип сбоя в работе.

faultBeginTime - дата и время начала сбоя в работе.

faultEndTime - дата и время конца сбоя в работе.

faultVehicleRegistration - VRN и название Договаривающейся стороны регистрации транспортного средства, в которой имел место сбой в работе.

2.19 CardIccIdentification (идентификация ИС карточки)

Информация, записанная на карточке, которая относится к идентификации интегральной схемы (ИС) карточки (требование 192).

```
CardIccIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    clockStop                ОКТЕТНАЯ СТРОКА (РАЗМЕР(1)),
    CardApprovalNumber       расширенный номер серии,
    cardApprovalNumber       номер официального утверждения карточки,
    cardPersonaliserID       ОКТЕТНАЯ СТРОКА (РАЗМЕР(1)),
    embedderIcAssemblerId    ОКТЕТНАЯ СТРОКА (РАЗМЕР(5)),
    icIdentifier             ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))
}
```

clockStop - режим остановки часов, определенных в стандарте EN 726-3.

cardExtendedSerialNumber - серийный номер карточки на интегральной схеме и исходный заводской номер карточки на интегральной схеме, определенный в стандарте EN 726-3 и более точно определяемый типом данных ExtendedSerialNumber.

cardApprovalNumber - номер официального утверждения типа карточки.

cardPersonaliserID - идентификатор учреждения, персонализирующего карточку, определенный в стандарте EN 726-3.

embedderIcAssemblerId - идентификатор монтажного/сборочного предприятия, определенный в стандарте EN 726-3.

icIdentifier - идентификатор ИС карточки и изготовитель ИС, определенный в стандарте EN 726-3.

2.20 CardIdentification (идентификация карточки)

Информация, записанная на карточке, которая имеет отношение к идентификации карточки (требования 194, 215, 231, 235).

```
CardIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
        CardIssuingMemberState          числовой код страны,
        cardNumber                      номер карточки,
        cardIssuingAuthorityName        название,
        cardIssueDate                   реальное время,
        cardValidityBegin               реальное время,
        cardExpiryDate                  реальное время
}
```

cardIssuingMemberState - код Договаривающейся стороны, выдавшей карточку.

cardNumber - номер карточки.

cardIssuingAuthorityName - название органа, выдавшего карточку.

cardIssueDate - дата выдачи карточки нынешнему держателю.

cardValidityBegin - первая дата действия карточки.

cardExpiryDate - дата истечения срока действия карточки.

2.21 CardNumber (номер карточки)

Номер карточки, содержащийся в определении (g).

```
CardNumber ::= ВЫБОР {
    ПОСЛЕДОВАТЕЛЬНОСТЬ {
        driverIdentification        строка IA5 (РАЗМЕР (14)),
        cardReplacementIndex        индекс замены карточки
        cardRenewalIndex            индекс обновления карточки
    },

    ПОСЛЕДОВАТЕЛЬНОСТЬ {
        ownerIdentification         строка IA5 (РАЗМЕР (13)),
        cardConsecutiveIndex        порядковый индекс карточки,
        cardReplacementIndex        индекс замены карточки,
        cardRenewalIndex            индекс обновления карточки
    }
}
```

driverIdentification - индивидуальная идентификация водителя Договаривающейся стороны.

ownerIdentification - индивидуальная идентификация предприятия или мастерской или контрольного органа в соответствующей Договаривающейся стороне.

cardConsecutiveIndex - порядковый индекс карточки.

cardReplacementIndex - индекс замены карточки.

cardRenewalIndex - индекс возобновления карточки.

Первая последовательность этого варианта позволяет кодировать номер карточки водителя, а вторая последовательность позволяет кодировать номера карточки мастерской, контролера и предприятия.

2.22 CardPlaceDailyWorkPeriod (ежедневный период работы и место)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к местам, в которых начинаются и/или заканчиваются ежедневные периоды работы (требования 202 и 221).

```
CardPlaceDailyWorkPeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    placePointerNewestRecord    ЦЕЛОЕ ЧИСЛО (0 .. NoOfCardPlaceRecords-1),
    placeRecords                УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)
                                ЗАПИСИ PlaceRecord
}
```

placePointerNewestRecord - индекс последней обновленной записи данных о месте.

Присвоение значения: Число, соответствующее числовому показателю записи данных о месте, которое начинается с '0' в случае первой регистрации записей, касающихся места, в структуре.

placeRecords - совокупность записей, содержащих информацию о введенных названиях мест.

2.23 CardPrivateKey (закрытый ключ карточки)

Закрытый ключ карточки.

CardPrivateKey ::= закрытая экспонента ключа RSA

2.24 CardPublicKey (открытый ключ карточки)

Открытый ключ карточки.

CardPublicKey ::= открытый ключ

2.25 CardRenewalIndex (индекс возобновления карточки)

Индекс возобновления карточки (определение i)).

CardRenewalIndex ::= строка IA5 (РАЗМЕР (1))

Присвоение значения: (см. главу VII настоящего добавления).
'0' Первая выдача.
Порядок увеличения: '0 , … , 9 , A , … , Z'

2.26 CardReplacementIndex (индекс замены карточки)

Индекс замены карточки (определение j)).

CardReplacementIndex ::= IA5Строка (РАЗМЕР (1))

Присвоение значения: (см. главу VII настоящего добавления).
'0' первая карточка.
Порядок увеличения: '0 , … , 9 , A , … , Z'

2.27 CardSlotNumber (номер считывающего устройства карточки)

Код, позволяющий проводить различие между двумя считывающими устройствами бортового устройства.

```
CardSlotNumber ::= ЦЕЛОЕ ЧИСЛО {
   driverSlot                    (0),
   co-driverSlot                 (1)
}
```

Присвоение значения: дополнительно не уточняется.

2.28 CardSlotsStatus (состояние считывающих устройств карточки)

Код, указывающий тип карточек, вставленных в два считывающих устройства бортового устройства.

CardSlotsStatus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значения – Выровненный октет: 'ccccdddd'B

'cccc'B идентификация типа карточки, вставленной в считывающее устройство второго водителя,
'dddd'B идентификация типа карточки, вставленной в считывающее устройство водителя,

со следующими идентификационными кодами:
'0000'B карточка не вставлена,
'0001'B не вставлена карточка водителя,
'0010'B вставлена карточка мастерской,
'0011'B вставлена карточка контролера,
'0100'B вставлена карточка предприятия.

2.29 CardStructureVersion (вариант структуры карточки)

Код, указывающий вариант структуры, использованной на карточке тахографа.

CardStructureVersion ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))

Присвоение значения: 'aabb'H:
'aa'H индекс изменения структуры,
'00h' для данной версии

'bb'H индекс изменений, касающийся использования элементов данных, определенных в структуре, заданной стартовым байтом, '00h' для данного варианта.

2.30 CardVehicleRecord (запись использования транспортного средства)

Информация, записанная на карточке водителя или предприятия, которая имеет отношение к периоду использования транспортного средства в течение соответствующего календарного дня (требования 197 и 217).

```
CardVehicleRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   vehicleOdometerBegin          счетчик пробега,
   vehicleOdometerEnd            счетчик пробега,
   vehicleFirstUse               реальное время,
   vehicleLastUse                реальное время,
   vehicleRegistration           идентификация регистрации транспортного
                                 средства,
   vuDataBlockCounter            счетчик массивов данных бортового
                                 устройства
}
```

vehicleOdometerBegin - показания счетчика пробега транспортного средства на начало периода использования транспортного средства.

vehicleOdometerEnd - показания счетчика пробега транспортного средства на конец периода использования транспортного средства.

vehicleFirstUse - дата и время начала периода использования транспортного средства.

vehicleLastUse - дата и время завершения периода использования транспортного средства.

vehicleRegistration - VRN и Договаривающаяся сторона регистрации транспортного средства.

vuDataBlockCounter - показания счетчика блока данных бортового устройства на момент последнего извлечения данных, касающихся периода использования транспортного средства.

2.31 CardVehiclesUsed (использованное транспортное средство)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к транспортным средствам, используемым держателем карточки (требования 197 и 217).

```
CardVehiclesUsed := ПОСЛЕДОВАТЕЛЬНОСТЬ {
   vehiclePointerNewestRecord        ЦЕЛОЕ ЧИСЛО (0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                УСТАНОВЛЕННЫЙ РАЗМЕР
                                     (NoOfCardVehicleRecords) ЗАПИСИ
                                     CardVehicleRecord
}
```

vehiclePointerNewestRecord - индекс последней обновленной записи, касающейся транспортного средства.

Присвоение значения: число, соответствующее числовому показателю записи, касающейся транспортного средства, которое начинается с '0' в случае первой регистрации записей, касающихся транспортного средства, в данной структуре.

cardVehicleRecords - совокупность записей, содержащих информацию об использованных транспортных средствах.

2.32 Certificate (сертификат)

Сертификат открытого ключа, выданный сертификационным органом.

Certificate ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (194))

Присвоение значения: цифровая подпись с частичным восстановлением содержания сертификата в соответствии с подразделом 11 (общие механизмы защиты): подпись (128 байтов) || остальная часть открытого ключа (58 байтов) || исходные данные сертификационного органа (8 байтов).

2.33 CertificateContent (содержание сертификата)

(Открытое) содержание сертификата открытого ключа в соответствии с общими механизмами защиты, изложенными в подразделе 11.

```
CertificateContent ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   certificateProfileIdentifier          ЦЕЛОЕ ЧИСЛО (0..255),
   certificationAuthorityReference       Идентификатор ключа,
   certificateHolderAuthorisation        Разрешение владельца сертификата,
   certificateEndOfValidity              Реальное время,
   certificateHolderReference            Идентификатор ключа,
   publicKey                             Открытый ключ
}
```

certificateProfileIdentifier - версия соответствующего сертификата.
Присвоение значения: '01h' для данного варианта.

certificationAuthorityReference - идентификатор сертификационного органа, выдавшего сертификат. Он также включает ссылку на открытый ключ данного сертификационного органа.

certificateHolderAuthorisation - идентификатор прав держателя сертификата.

certificateEndOfValidity - дата, когда истекает срок административного действия сертификата.

certificateHolderReference - идентификатор держателя сертификата. Он также включает ссылку на его открытый ключ.

publicKey - открытый ключ, подтверждающий данный сертификат.

2.34 CertificateHolderAuthorisation (разрешение держателя сертификата)

Идентификация прав держателя сертификата.

```
CertificateHolderAuthorisation::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   tachographApplicationID          ОКТЕТНАЯ СТРОКА (РАЗМЕР (6))
   equipmentType                    Тип оборудования
}
```

tachographApplicationID - идентификатор приложения для прикладной программы тахографа.
Присвоение значения: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Этот идентификатор является фирменным незарегистрированным идентификатором приложения в соответствии со стандартом ISO/IEC 7816-5.

equipmentType - идентификация типа оборудования, для которого предназначен этот сертификат.

Присвоение значения: в соответствии с типом данных EquipmentType . **0**, если сертификат выдан какой-либо Договаривающейся стороной.

2.35 CertificateRequestID (запрос на идентификацию сертификата)

Индивидуальная идентификация запроса сертификата. Она также может использоваться в качестве идентификатора открытого ключа бортового устройства, если серийный номер бортового устройства, для которого предназначен данный ключ, в момент создания сертификата не был известен.

CertificateRequestID::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

requestSerialNumber	ЦЕЛОЕ ЧИСЛО (0..2^{32}-1)
requestMonthYear	BCDString(РАЗМЕР (2))
crIdentifier	ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))
manufacturerCode	Код изготовителя

}

requestSerialNumber - порядковый номер запроса на сертификат, индивидуальный для данного изготовителя и относящийся к месяцу, указанному ниже.

requestMonthYear - идентификация месяца и года запроса на сертификат.
Присвоение значения: Код BCD месяца (две цифры) и года (две последние цифры).

crIdentifier: идентификатор, позволяющий проводить различие между запросом на сертификат и расширенным порядковым номером.

Присвоение значения: 'FFh'.

Код завода-изготовителя: цифровой код изготовителя, запрашивающего сертификат.

2.36 CertificationAuthorityKID (Сертификационный орган KID)

Идентификатор открытого ключа Сертификационного органа (Договаривающейся стороны или Европейского сертификационного органа)

CertificationAuthorityKID:= ПОСЛЕДОВАТЕЛЬНОСТЬ {

nationNumeric	Числовой код страны
nationAlpha	Буквенный код страны
keySerialNumber	ЦЕЛОЕ ЧИСЛО (0..255)
additionalInfo	ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))
caIdentifier	ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

}

nationNumeric - числовой код страны сертификационного органа.

nationAlpha - буквенно-числовой код страны сертификационного органа.

keySerialNumber - порядковый номер, позволяющий проводить различие между различными ключами сертификационного органа в случае изменения ключей.

additionalInfo - двухбайтовое поле для дополнительного кодирования (специфичное для сертификационного органа).

caIdentifier - идентификатор, позволяющий проводить различие между идентификатор ключа сертификационного органа и другими идентификаторами ключа.
Присвоение значения: '01h'.

2.37 CompanyActivityData (данные об операциях с карточкой предприятия)

Информация, записанная на карточке предприятия, которая имеет отношение к операциям, произведенным с карточкой (требование 237).

```
CompanyActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   companyPointerNewestRecord      ЦЕЛОЕ ЧИСЛО (0..NoOfCompanyActivityRecords-1),
   companyActivityRecords          УСТАНОВЛЕННЫЙ РАЗМЕР
                                   (NoOfCompanyActivityRecords)
      companyActivityRecord           ПОСЛЕДОВАТЕЛЬНОСТИ {
      companyActivityType               тип операций с карточкой предприятия
      companyActivityTime               реальное время,
      cardNumberInformation             полный номер карточки,
      vehicleRegistrationInformation    идентификация регистрации транспортного
                                        средства,
      downloadPeriodBegin               реальное время,
      downloadPeriodEnd                 реальное время
    }
}
```

companyPointerNewestRecord - индекс последней обновленной записи операции с карточкой предприятия.
Присвоение значения: число, соответствующее числовому идентификатору записи операций с карточкой предприятия, начинающееся с '0' в случае первой записи операции, произведенной предприятием в данной структуре.

companyActivityRecords - совокупность всех записей операций, произведенных предприятием.

companyActivityRecord - последовательность информации, относящейся к одной операции, произведенной предприятием.

companyActivityType - тип операции, произведенной предприятием.

companyActivityTime - дата и время операции, произведенной предприятием.

cardNumberInformation - номер карточки и, в соответствующих случаях, название Договаривающейся стороны, выдавшей карточку с загруженными с нее данными.

vehicleRegistrationInformation - VRN и страна регистрации транспортного средства, с которого были загружены данные или на которое была поставлена или снята блокировка.

downloadPeriodBegin и **downloadPeriodEnd** - период, за который были загружены в соответствующих случаях данные с БУ.

2.38 CompanyActivityType (тип операции, произведенной предприятием)

Код указывающей операции, произведенной предприятием с использованием карточки предприятия.

```
CompanyActivityType:= ЦЕЛОЕ ЧИСЛО {
   загрузка данных с карточки        (1),
   загрузка с БУ                     (2),
   блокировка БУ                     (3),
   снятие блокировки с БУ            (4)
}
```

2.39 CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)

Информация, записанная на карточке предприятия, которая имеет отношение к идентификации приложения карточки (требование 190).

```
CompanyCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   typeOfTachographCardId            тип оборудования,
   cardStructureVersion              вариант структуры карточки,
   noOfCompanyActivityRecords        число записей операций, произведенных
                                     компанией
}
```

typeOfTachographCardId - элемент данных, указывающий на применяемый тип карточки.

cardStructureVersion - элемент данных, указывающий на версию структуры, которая используется в карточке.

noOfCompanyActivityRecords - число записей операций, произведенных предприятием, которые могут храниться на карточке.

2.40 CompanyCardHolderIdentification (идентификация держателя карточки предприятия)

Информация, записанная на карточке предприятия, которая относится к идентификации держателя карточки (требование 236).

CompanyCardHolderIdentification ::=	ПОСЛЕДОВАТЕЛЬНОСТЬ {
companyName	название,
companyAddress	адрес,
cardHolderPreferredLanguage	язык
}	

companyName - название предприятия-держателя.

companyAddress - адрес предприятия-держателя а.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.41 ControlCardApplicationIdentification (идентификация приложения карточки контролера)

Информация, записанная на карточке контролера, которая имеет отношение к идентификации приложения карточки (требование 190).

ControlCardApplicationIdentification ::=	ПОСЛЕДОВАТЕЛЬНОСТЬ {
typeOfTachographCardId	тип оборудования,
cardStructureVersion	версия структуры карточки,
noOfControlActivityRecords	число записей проверочных операций
}	

typeOfTachographCardId - элемент данных, указывающий на используемый тип карточки.

cardStructureVersion - элемент данных, указывающий вариант структуры, применяемой на карточке.

noOfControlActivityRecords - число записей проверочных операций, которые могут храниться на карточке.

2.42 ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)

Информация, записанная на карточке контролера, которая имеет отношение к проверочной операции, произведенной с карточкой (требование 233).

ControlCardControlActivityData ::=	ПОСЛЕДОВАТЕЛЬНОСТЬ {
controlPointerNewestRecord	ЦЕЛОЕ ЧИСЛО (0.. NoOfControlActivityRecords-1),
controlActivityRecords	УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfControlActivityRecords)
controlActivityRecord	ПОСЛЕДОВАТЕЛЬНОСТИ {
controlType	тип проверки,
controlTime	реальное время,
controlledCardNumber	полное время карточки,
controlledVehicleRegistration	идентификация регистрации транспортного средства,
controlDownloadPeriodBegin	реальное время,
controlDownloadPeriodEnd	реальное время
}	
}	

controlPointerNewestRecord - индекс последней обновленной записи проверочной операции.

Присвоение значения: число, соответствующее числовому показателю записи проверочной операции, которая начинается с '0' в случае первой записи проверочной операции в данной структуре.

controlActivityRecords - совокупность всех записей проверочных операций.

controlActivityRecord - последовательность информации, связанной с одной проверкой.

controlType - тип проверки.

controlTime - дата и время проверки.

controlledCardNumber - номер карточки и название Договаривающейся Стороны, выдавшей карточку, которая подвергалась проверке.

controlledVehicleRegistration - VRN и название Договаривающейся Стороны регистрации транспортного средства, в которой производилась проверка.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** - период, за который в соответствующих случаях загружались данные.

2.43 ControlCardHolderIdentification (идентификация держателя карточки контролера)

Информация, записанная на карточке контролера, которая имеет отношение к идентификации держателя карточки (требование 232).

```
ControlCardHolderIdentification ::=     ПОСЛЕДОВАТЕЛЬНОСТЬ {
   controlBodyName                      название,
   controlBodyAddress                   адрес,
   cardHolderName                       фамилия держателя,
   cardHolderPreferredLanguage          язык
}
```

controlBodyName - название контрольного органа держателя карточки.

controlBodyAddress - адрес контрольного органа держателя карточки.

cardHolderName - фамилия и имя (имена) держателя контрольной карточки.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.44 ControlType (тип проверки)

Код, указывающий на операции, проведенные в ходе проверки. Этот тип данных имеет отношение к требованиям 102, 210 и 225.

```
ControlType ::= ОКТЕТНАЯ (РАЗМЕР (1))
```

Присвоение значения - выровненный октет: ‘cvpdxxxx’B (8 битов)

‘c’B загрузка данных с карточки:
- ‘0’B: во время данной проверочной операции загрузка данных с карточки не была произведена,
- ‘1’B: во время данной операции загрузка данных с карточки была произведена.

‘v’B загрузка данных с БУ:
- ‘0’B: во время данной проверочной операции загрузка данных с БУ не была произведена,
- ‘1’B: во время данной проверочной операции загрузка данных с БУ была произведена

‘p’B вывод на печать:
- ‘0’B: во время данной проверочной операции вывод данных на печать произведен не был,
- ‘1’B: во время данной проверочной операции вывод данных на печать был произведен

‘d’B вывод на дисплей:
- ‘0’B: во время данной проверочной операции вывод на дисплей не использовался,
- ‘1’B: во время данной проверочной операции использовался вывод на дисплей

‘xxxx’B - не использовался.

2.45 CurrentDateTime (текущая дата/время)

Текущая дата и время, отображаемые на контрольном устройстве.

CurrentDateTime ::= реальное время

Присвоение значения: дополнительно не указывается.

2.46 DailyPresenceCounter (счетчик ежедневного присутствия)

Показания счетчика, записанные на карточке водителя или предприятия, которые увеличиваются на единицу за каждый календарный день, в течение которого в БУ была вставлена карточка. Этот тип данных имеет отношение к требованиям 199 и 219.

DailyPresenceCounter ::= строка BCD (РАЗМЕР(2))

Присвоение значения: порядковый номер с максимальным значением = 9 999, который снова начинается с 0. В момент первой выдачи номера карточки это число устанавливается на 0.

2.47 Datef (формат даты)

Дата, отображенная в числовом формате, которая может сразу выводиться на печать.

Datef ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

год	строка BCD (РАЗМЕР(2)),
месяц	строка BCD (РАЗМЕР(1)),
день	строка BCD (РАЗМЕР(1))

}

Присвоение значения:

гггг	год
мм	месяц
дд	день

'00000000'H четкое указание на отсутствие даты.

2.48 Distance (расстояние)

Пройденное расстояние (результат расчета разницы между двумя показаниями счетчика пробега транспортного средства в километрах).

Distance ::= ЦЕЛОЕ ЧИСЛО $(0..2^{16}-1)$

Присвоение значения: двоичный код без знака. Значение в км в рабочем диапазоне от 0 до 9 999 км.

2.49 DriverCardApplicationIdentification (идентификация приложения карточки водителя)

Информация, записанная на карточке водителя, которая имеет отношение к идентификации приложения карточки (требование 190).

```
DriverCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    typeOfTachographCardId          тип оборудования,
    cardStructureVersion            вариант структуры карточки,
    noOfEventsPerType               число событий по типу,
    noOfFaultsPerType               число неисправностей по типу,
    activityStructureLength         диапазон длины записи вида деятельности
                                    на карточку,
    noOfCardVehicleRecords          число записей на карточке, относящихся к
                                    транспортному средству,
    noOfCardPlaceRecords            число записей на карточке, относящихся к месту
}
```

typeOfTachographCardId - элемент данных, указывающий тип используемой карточки.

cardStructureVersion - элемент данных, указывающий вариант структуры, использованной в карточке.

noOfEventsPerType - число событий по типу события, которое может быть записано на карточку.

noOfFaultsPerType - число неисправностей по типу неисправности, которое может быть записано на карточку.

activityStructureLength - элемент данных, указывающий число байтов, которые могут быть использованы для хранения записей, относящихся к виду деятельности.

noOfCardVehicleRecords - число записей, относящихся к транспортному средству, которое может быть записано на карточку.

noOfCardPlaceRecords - число мест, которое может быть записано на карточку.

2.50 DriverCardHolderIdentification (идентификация держателя карточки водителя)

Информация, записанная на карточке водителя, которая имеет отношение к идентификации держателя карточки (требование 195).

```
DriverCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    cardHolderName                фамилия держателя,
    cardHolderBirthDate           формат даты,
    cardHolderPreferredLanguage   язык
}
```

cardHolderName - фамилия и имя (имена) держателя карточки водителя.

cardHolderBirthDate - дата рождения держателя карточки водителя.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.51 EntryTypeDailyWorkPeriod (тип ввода данных о ежедневных периодах работы)

Код, позволяющий провести различие между началом и концом ввода данных о месте ежедневного периода работы и условиями ввода.

```
EntryTypeDailyWorkPeriod ::= ЦЕЛОЕ ЧИСЛО {
    начало, относительное время = время ввода карточки или время ввода данных  (0),
    конец, относительное время = время извлечения карточки или время
    ввода данных                                                               (1),
    начало, относительное время ручного ввода данных (время начала работы)     (2),
    конец, относительное время ручного ввода данных (конец рабочего периода)   (3),
    начало, относительное время, зафиксированное БУ                            (4),
    конец, относительное время, зафиксированное БУ                             (5)
}
```

Присвоение значения: в соответствии со стандартом ISO/IEC8824-1.

2.52 EquipmentType (тип оборудования)

Код, позволяющий провести различие между различными типами оборудования в связи с использованием тахографа.

EquipmentType ::= ЦЕЛОЕ ЧИСЛО (0..255)
-- зарезервировано (0),
-- карточка водителя (1),
-- карточка мастерской (2),
-- карточка контролера (3),
-- карточка предприятия (4),
-- карточка завода-изготовителя (5),
-- бортовое устройство (6),
-- датчик движения (7),
-- RFU (зарезервировано для будущего использования)(8..255)

Присвоение значения: в соответствии со стандартом ISO/IEC8824-1.

Значение 0 зарезервировано для целей указания Договаривающейся стороны или Европы в поле данных CHA сертификатов.

2.53 EuropeanPublicKey (европейский открытый ключ)

Европейский открытый ключ.

EuropeanPublicKey ::= открытый ключ

2.54 EventFaultType (тип неисправности)

Код, отображающий события или неисправность.

EventFaultType ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значений:

'0x'H	общие события,
'00'H	дополнительно не уточняется,
'01'H	ввод недействительной карточки,
'02'H	несовместимость карточек,

‘03’H	нестыковка времени,
‘04’H	управление без соответствующей карточки,
‘05’H	ввод карточки в процессе управления,
‘06’H	последний сеанс использования карточки завершен неправильно,
‘07’H	превышение скорости,
‘08’H	прекращение электропитания,
'09’H	ошибка данных о движении,
‘0A’H to ‘0F’H	RFU,
‘1x’H	события, связанные с попыткой нарушения защиты бортового устройства,
‘10’H	дополнительно не уточняется,
‘11’H	сбой в аутентификации датчика движения,
‘12’H	сбой в аутентификации карточки тахографа,
‘13’H	несанкционированная замена датчика движения,
‘14’H	ошибка, указывающая на нарушение целостности при вводе данных на карточку
‘15’H	ошибка, указывающая на нарушение целостности данных пользователя, записанных в блоке памяти,
‘16’H	внутренняя ошибка при передаче данных,
‘17’H	несанкционированное вскрытие корпуса,
‘18’H	нарушение целостности аппаратного оборудования,
‘19’H to ‘1F’H	RFU,
‘2x’H	события, связанные с попыткой нарушения защиты датчика,
‘20’H	дополнительно не уточняется,
‘21’H	сбой в аутентификации,
‘22’H	ошибка, указывающая на нарушение целостности сохраненных данных,
‘23’H	внутренняя ошибка при передаче данных,
‘24’H	несанкционированное вскрытие корпуса,
‘25’H	нарушение целостности аппаратного оборудования,
‘26’H to ‘2F’H	RFU,
‘3x’H	неисправность контрольного устройства,
‘30’H	дополнительно не уточняется,
‘31’H	внутренняя неисправность БУ,
‘32’H	неисправность принтера,
‘33’H	неисправность дисплея,

‘34’H	ошибка при загрузке,
‘35’H	неисправность датчика,
‘36’H to ‘3F’H	RFU,
‘4x’H	сбой в работе карточки,
‘40’H	дополнительно не уточняется,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	по усмотрению изготовителя.

2.55 EventFaultRecordPurpose (цель регистрации события или неисправности)

Код, указывающий на причину регистрации события или неисправности.

EventFaultRecordPurpose: = ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значений:

‘00’H	одно из 10 самых последних (недавних) событий или неисправностей
‘01’H	самое длинное событие, происшедшее в один из последних 10 дней
‘02’H	одно из пяти наиболее продолжительных событий, происшедших за последние 365 дней
‘03’H	последнее событие за один из последних 10 дней
‘04’H	самое серьезное событие за один из последних 10 дней
‘05’H	одно из пяти самых серьезных событий, происшедших за последние 365 дней
‘06’H	первое событие или первая неисправность, имевшие место после последней калибровки
'07'H	текущее/продолжающееся событие или неисправность
‘08’H - ‘7F’H	RFU
‘80’H - ‘FF’H	по усмотрению изготовителя

2.56 ExtendedSerialNumber (расширенный номер серии)

Индивидуальная идентификация оборудования. Она может использоваться в качестве идентификатора открытого ключа оборудования.

ExtendedSerialNumber: = ПОСЛЕДОВАТЕЛЬНОСТЬ {

serialNumber	ЦЕЛОЕ ЧИСЛО (0..2^{32}-1)
monthYear	строка BCD (РАЗМЕР(2))
type	ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
manufacturerCode	код изготовителя

}

serialNumber - серийный номер оборудования, индивидуальный для данного изготовителя, типа оборудования и месяца, указанного ниже.

monthYear - идентификация месяца и года изготовления (или присвоение порядкового номера).

Присвоение значения: кодирование BCD месяца (две цифры) и года (две последние цифры).

type - идентификатор типа оборудования.

Присвоение значения: по усмотрению изготовителя с зарезервированным значением 'FFh'.

manufacturerCode: числовой код изготовителя оборудования.

2.57 FullCardNumber (полный номер карточки)

Код, полностью идентифицирующий карточку тахографа.

FullCardNumber: = ПОСЛЕДОВАТЕЛЬНОСТЬ {

cardType	тип оборудования,
cardIssuingMemberState	числовой код страны,
cardNumber	номер карточки

}

cardType - тип карточки тахографа.

cardIssuingMemberState - код Договаривающейся стороны, выдавшей карточку.

cardNumber - номер карточки.

2.58 HighResOdometer (показания счетчика пробега)

Показания счетчика пробега транспортного средства: общее расстояние, пройденное транспортным средством за период его эксплуатации.

HighResOdometer: = ЦЕЛОЕ ЧИСЛО (0..2^{32}-1)

Присвоение значения: двоичный код без знака. Значение с точностью до 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.59 HighResTripDistance (расстояние, пройденное за рейс)

Расстояние, пройденное за весь или часть рейса.

HighResTripDistance: = ЦЕЛОЕ ЧИСЛО (0..2^{32}-1)

Присвоение значения: двоичный код без знака. Значение с точностью до 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.60 HolderName (фамилия держателя)

Фамилия и имя (имена) держателя карточки.

```
HolderName: = ПОСЛЕДОВАТЕЛЬНОСТЬ {
      holderSurname                фамилия,
      holderFirstNames             имя
}
```

holderSurname - фамилия держателя. Эта фамилия не включает никаких дополнительных указаний.

Присвоение значения: когда карточка не именная, позиция holderSurname содержит ту же информацию, что и companyName (название предприятия), или workshopName (название мастерской) или controlBodyName (название контрольного органа).

holderFirstNames - имя (имена) и инициалы держателя.

2.61 K-ConstantOfRecordingEquipment (постоянная К записывающего оборудования)

Постоянная контрольного устройства (определение m)).

K-ConstantOfRecordingEquipment: = ЦЕЛОЕ ЧИСЛО ($0..2^{16}$-1)

Присвоение значения: импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

2.62 KeyIdentifier (идентификатор ключа)

Индивидуальный идентификатор открытого ключа, используемого для назначения и выбора ключа. Он также определяет держателя ключа.

```
KeyIdentifier: = ВЫБОР {
    extendedSerialNumber        расширенный номер серии,
    certificateRequestID        идентификатор запроса на сертификат,
    certificationAuthorityKID   сертификационный орган KID
}
```

Первый вариант выбора позволяет назначить открытый ключ бортового устройства или карточки тахографа.

Второй вариант выбора позволяет назначить открытый ключ бортового устройства (в том случае если в момент создания сертификата серийный номер бортового устройства неизвестен).

Третий вариант выбора позволяет назначить открытый ключ Договаривающейся стороны.

2.63 L-TyreCircumference (окружность шины L)

Эффективная окружность шин колес (определение u)).

L-TyreCircumference: = ЦЕЛОЕ ЧИСЛО ($0..2^{16}$-1)

Присвоение значения: двоичный код без знака, значение с точностью 1/8 мм в рабочем диапазоне от 0 до 8 031 мм.

2.64 Language (язык)

Код, идентифицирующий язык.

Language: = Строка IA5 (РАЗМЕР (2))

Присвоение значения: код в виде двух строчных букв в соответствии со стандартом ISO 639.

2.65 LastCardDownload (последняя дата загрузки с карточки)

Дата и время, записанные на карточке водителя, последней загрузки данных с карточки (для иных целей, кроме контроля). Эта дата может обновляться БУ или любым считывающим устройством.

LastCardDownload: = Реальное время

Присвоение значения: дополнительно не уточняется.

2.66 ManualInputFlag (метка ручного ввода)

Код, позволяющий определить, ввел ли держателя карточки данные о деятельности водителя вручную в момент ввода карточки или нет (требование 081).

ManualInputFlag: = ЦЕЛОЕ ЧИСЛО {

noEntry	(0)
manualEntries	(1)

}

Присвоение значения: дополнительно не уточняется.

2.67 ManufacturerCode (код изготовителя)

Код, идентифицирующий изготовителя[13].

---

[13] Обновленный список кодов, позволяющих идентифицировать заводы-изготовители, размещен на вебсайте Европейского сертификационного органа по адресу: http://dtc.jrc.ec.europa.eu/text/cm.html.

ManufacturerCode: = ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения :

‘00’H	Информации нет
‘01’H	Значение зарезервировано
‘02’H .. ‘0F’H	Зарезервировано для будущего использования
‘10’H	ACTIA
‘11’H .. ‘17’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘A’
‘18’H .. ‘1F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘B’
‘20’H .. ‘27’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘C’
‘28’H .. ‘2F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘D’
‘30’H .. ‘37’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘E’
‘38’H .. ‘3F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘F’
‘40’H	Giesecke & Devrient GmbH
‘41’H	GEM plus
‘42’H .. ‘47’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘G’
‘48’H .. ‘4F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘H’
‘50’H .. ‘57’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘I’
‘58’H .. ‘5F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘J’
‘60’H .. ‘67’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘K’
‘68’H .. ‘6F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘L’
‘70’H .. ‘77’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘M’
‘78’H .. ‘7F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘N’
‘80’H	OSCARD

‘81’H .. ‘87’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘O’
‘88’H .. ‘8F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘P’
‘90’H .. ‘97’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘Q’
‘98’H .. ‘9F’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘R’
‘A0’H	SETEC
‘A1’H	SIEMENS VDO
‘A2’H	STONERIDGE
‘A3’H.. ‘A7’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘S’
‘AA’H	TACHOCONTROL
’AB’H .. ‘AF’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘T’
‘B0’H .. ‘B7’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘U’
‘B8’H .. ‘BF’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘V’
‘C0’H .. ‘C7’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘W’
‘C8’H .. ‘CF’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘X’
‘D0’H .. ‘D7’H	Зарезервировано для заводов-изготовителей, название которых начинается с буквы ‘Y’
‘D8’H .. ‘DF’H	Зарезервировано для изготовителей, название которых начинается с буквы ‘Z’

2.68 MemberStateCertificate (сертификат государства-члена)

Сертификат открытого ключа Договаривающейся стороны, выданный Европейским сертификационным органом.

MemberStateCertificate: = Сертификат

2.69 MemberStatePublicKey (открытый ключ государства-члена)

Открытый ключ Договаривающейся стороны.

MemberStatePublicKey: = Открытый ключ

2.70 Name (название)

Название.

```
Название := ПОСЛЕДОВАТЕЛЬНОСТЬ {
   codePage                              ЦЕЛОЕ ЧИСЛО (0..255),
   name                                  ОКТЕТНАЯ СТРОКА (РАЗМЕР(35))
}
```

codePage - элемент данных, указывающий на раздел стандарта ISO/IEC 8859, использованный для кодирования названия,

name - название, закодированное в соответствии со стандартом ISO/IEC 8859-codePage.

2.71 NationAlpha (буквенный код страны)

Буквенное обозначение страны в соответствии с обычным принципом кодирования стран (отличительные знаки), которое наносится на заднюю часть транспортных средств (либо отдельно от номерного знака, либо включенного в номерной знак) и/или упомянутое в зеленых карточках, выдаваемых страховыми компаниями.

NationAlpha ::= строка IA5 (РАЗМЕР(3))

Присвоение значения:

' '	Информации нет,
'A '	Австрия,
'AL '	Албания,
'AND'	Андорра,
'ARM'	Армения,
'AZ '	Азербайджан,
'B '	Бельгия,
'BG '	Болгария,
'BIH'	Босния и Герцеговина,
'BY '	Беларусь,

‘CH ’	Швейцария,
‘CY ’	Кипр,
‘CZ ’	Чешская Республика,
‘D ’	Германия,
‘DK ’	Дания,
‘E ’	Испания,
‘EST’	Эстония,
‘F ’	Франция,
‘FIN’	Финляндия,
‘FL ’	Лихтенштейн,
‘FR ’	Фарерские Острова
‘UK ’	Соединенное Королевство, Олдерни, Гернси, Джерси, Остров Мэн, Гибралтар,
‘GE ’	Грузия,
‘GR ’	Греция,
‘H ’	Венгрия,
‘HR’	Хорватия,
‘I ’	Италия,
‘IRL’	Ирландия,
‘IS ’	Исландия,
‘KZ ’	Казахстан,
‘L ’	Люксембург,
‘LT ’	Литва,
‘LV ’	Латвия,
‘M ’	Мальта,
‘MC ’	Монако,
‘MD ’	Республика Молдова,
‘MK ’	Бывшая югославская Республика Македония,
‘N ’	Норвегия,
‘NL ’	Нидерланды,
‘P ’	Португалия,
‘PL ’	Польша,
‘RO ’	Румыния,
‘RSM’	Сан-Марино,
‘RUS’	Российская Федерация,
‘S ’	Швеция,
‘SK ’	Словакия,
‘SLO’	Словения,
‘SRB’	Сербия,

'TM '	Туркменистан
'TR '	Турция,
'UA '	Украина,
'V '	Ватикан,
'UNK'	Нет данных,
'EC '	Европейское сообщество,
'EUR'	Остальная часть Европы,
'WLD'	Остальная часть мира.

2.72 NationNumeric (числовой код страны)

Числовое обозначение страны.

NationNumeric ::= ЦЕЛОЕ ЧИСЛО (0 .. 255)

Присвоение значения:

-- Информации нет	(00)H,
-- Австрия	(01)H,
-- Албания	(02)H,
-- Андорра	(03)H,
-- Армения	(04)H,
-- Азербайджан	(05)H,
-- Бельгия	(06)H,
-- Болгария	(07)H,
-- Босния и Герцеговина	(08)H,
-- Беларусь	(09)H,
-- Швейцария	(0A)H,
-- Кипр	(0B)H,
-- Чешская Республика	(0C)H,
-- Германия	(0D)H,
-- Дания	(0E)H,
-- Испания	(0F)H,
-- Эстония	(10)H,
-- Франция	(11)H,
-- Финляндия	(12)H,
-- Лихтенштейн	(13)H,
-- Фарерские Острова	(14)H,
-- Соединенное Королевство	(15)H,

-- Грузия (16)H,
-- Греция (17)H,
-- Венгрия (18)H,
-- Хорватия (19)H,
-- Италия (1A)H,
-- Ирландия (1B)H,
-- Исландия (1C)H,
-- Казахстан (1D)H,
-- Люксембург (1E)H,
-- Литва (1F)H,
-- Латвия (20)H,
-- Мальта (21)H,
-- Монако (22)H,
-- Республика Молдова (23)H,
-- Бывшая югославская Республика Македония (24)H,
-- Норвегия (25)H,
-- Нидерланды (26)H,
-- Португалия (27)H,
-- Польша (28)H,
-- Румыния (29)H,
-- Сан-Марино (2A)H,
-- Российская Федерация (2B)H,
-- Швеция (2C)H,
-- Словакия (2D)H,
-- Словения (2E)H,
-- Туркменистан (2F)H,
-- Турция (30)H,
-- Украина (31)H,
-- Ватикан (32)H,
-- Сербия (33)H,
-- RFU (зарезервировано для будущего использования) (34 .. FC)H,
-- Европейское сообщество (FD)H,
-- Остальная часть Европы (FE)H,
-- Остальная часть мира (FF)H

2.73 NoOfCalibrationRecords (число записей калибровки)

Число записей калибровки, которое может храниться на карточке.

NoOfCalibrationRecords: = ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.74 NoOfCalibrationsSinceDownload (число калибровок после загрузки)

Счетчик, указывающий число калибровок, произведенных с карточкой мастерской после последней загрузки данных с этой карточки (требование 230).

NoOfCalibrationsSinceDownload ::= ЦЕЛОЕ ЧИСЛО (0..2^{16}-1),

Присвоение значения: Дополнительно не уточняется.

2.75 NoOfCardPlaceRecords (число записей, касающихся мест, мест на карточке)

Число записей с указанием мест, которое может храниться на карточке водителя или мастерской.

NoOfCardPlaceRecords ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.76 NoOfCardVehicleRecords (число записей, касающихся транспортных средств на карточке)

Число записей с указанием использованных транспортных средств, которое может храниться на карточке водителя или мастерской.

NoOfCardVehicleRecords: = ЦЕЛОЕ ЧИСЛО (0.. 2^{16}-1)

Присвоение значения: см. пункт 3.

2.77 NoOfCompanyActivityRecords (число записей, касающихся операций предприятия)

Число записей, касающихся операций предприятия, которое может храниться на карточке предприятия.

NoOfCompanyActivityRecords ::= ЦЕЛОЕ ЧИСЛО (0.. 2^{16}-1)

Присвоение значения: см. пункт 3.

2.78 NoOfControlActivityRecords (число записей, касающихся проверочных операций)

Число, касающихся проверочных операций, которое может храниться на карточке контролера.

NoOfControlActivityRecords ::= ЦЕЛОЕ ЧИСЛО (0.. 2^{16}-1)

Присвоение значения: см. пункт 3.

2.79 NoOfEventsPerType (число событий по типу)

Число событий по типу события, которое может храниться на карточке.

NoOfEventsPerType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.80 NoOfFaultsPerType (число неисправностей по типу)

Число неисправностей по типу неисправности, которое может храниться на карточке.

NoOfFaultsPerType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.81 OdometerValueMidnight (показания счетчика пробега в полночь)

Показания счетчика пробега транспортного средства в полночь на данный день (требование 090).

OdometerValueMidnight ::= Показания счетчика

Присвоение значения: дополнительно не уточняется.

2.82 OdometerShort (показания счетчика)

Показания счетчика пробега транспортного средства в краткой форме.

OdometerShort ::= ЦЕЛОЕ ЧИСЛО $(0..2^{24}-1)$

Присвоение значения: двоичный код без знака. Значение в км в рабочем диапазоне от 0 до 9 999 999 км.

2.83 OverspeedNumber (число превышений скорости)

Число превышений скорости с момента последнего контроля за превышением скорости.

OverspeedNumber ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: 0 означает, что после последнего контроля за превышением скорости случаев превышения скорости не было, 1 означает, что после последнего контроля за превышением скорости был один случай превышения скорости...
255 означает, что после последнего контроля за превышением скорости было 255 или больше случаев превышения скорости.

2.84 PlaceRecord (запись, касающаяся места)

Информация, касающаяся места, в котором начинается или заканчивается ежедневный период работы (требования 087, 202, 221).

PlaceRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

entryTime	реальное время,
entryTypeDailyWorkPeriod	тип данных о ежедневном периоде работы,
dailyWorkPeriodCountry	числовой код страны,

```
    dailyWorkPeriodRegion              числовой код региона,
    vehicleOdometerValue               показания счетчика пробега
}
```

entryTime - дата и время ввода данных.

entryTypeDailyWorkPeriod - тип ввода.

dailyWorkPeriodCountry - страна въезда.

dailyWorkPeriodRegion - район въезда.

vehicleOdometerValue - показания счетчика пробега в момент ввода данных о месте въезда.

2.85 PreviousVehicleInfo (информация о предыдущем транспортном средстве)

Информация, касающаяся транспортного средства, использованного водителем ранее, в момент ввода его карточки в бортовое устройство (требование 081).

```
PreviousVehicleInfo ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    vehicleRegistrationIdentification  идентификация регистрации транспортного
                                       средства,
    cardWithdrawalTime                 реальное время
}
```

vehicleRegistrationIdentification - VRN и Договаривающаяся сторона регистрации транспортного средства.

cardWithdrawalTime - дата и время извлечения карточки.

2.86 PublicKey (открытый ключ)

Открытый ключ RSA.

```
PublicKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    rsaKeyModulus                      модуль ключа RSA,
    rsaKeyPublicExponent               открытая экспонента ключа RSA
}
```

rsaKeyModulus - модуль парного ключа.

rsaKeyPublicExponent - открытая экспонента парного ключа.

2.87 RegionAlpha (буквенный код региона)

Буквенное обозначение региона в конкретной стране.

RegionAlpha ::= СТРОКА IA5 (РАЗМЕР (3))

Присвоение значения:

‘ ’	информации нет,
Испания:	
‘AN ’	Андалусия,
‘AR ’	Арагон,
‘AST’	Астурия,
‘C ’	Кантабрия,
‘CAT’	Каталония,
‘CL ’	Кастилия-Леон,
‘CM ’	Кастилия-ла-Манча,
‘CV’	Валенсия,
‘EXT’	Эстремадура,
‘G ’	Галисия,
‘IB ’	Балеарские острова,
‘IC ’	Канарские острова,
‘LR ’	Ла-Риоха,
‘M ’	Мадрид,
‘MU ’	Мурсия,
‘NA ’	Наварра,
‘PV ’	Страна Басков

2.88 RegionNumeric (числовой код района)

Числовое обозначение района в конкретной стране.

RegionNumeric ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значения:

'00'H	данных нет,
Испания:	
'01'H	Андалусия,
'02'H	Арагон,
'03'H	Астурия,
'04'H	Кантабрия,
'05'H	Каталония,
'06'H	Кастилия-Леон,
'07'H	Кастилия-ла-Манча,
'08'H	Валенсия,
'09'H	Эстремадура,
'0A'H	Галисия,
'0B'H	Балеарские острова,
'0C'H	Канарские острова,
'0D'H	Ла-Риоха,
'0E'H	Мадрид,
'0F'H	Мурсия,
'10'H	Наварра,
'11'H	Страна Басков

2.89 RSAKeyModulus (модуль ключа RSA)

Модуль парного ключа RSA.

RSAKeyModulus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (128))

Присвоение значения: не определено.

2.90 RSAKeyPrivateExponent (закрытая экспонента ключа RSA)

(закрытая экспонента парного ключа RSA.

RSAKeyPrivateExponent ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (128))

Присвоение значения: не определено.

2.91 RSA KeyPrivateExponent (открытая экспонента ключа RSA)

Открытая экспонента ключа RSA.

RSAKeyPublicExponent ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))

Присвоение значения: не определено.

2.92 SensorApprovalNumber (номер официального утверждения датчика)

Номер официального утверждения типа датчика.

SensorApprovalNumber ::= строка IA5 (РАЗМЕР(8))

Присвоение значения: не определено.

2.93 SensorIdentification (идентификация датчика)

Информация, записанная в датчике движения, которая имеет отношение к идентификации датчика движения (требование 077).

```
SensorIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   sensorSerialNumber              серийный номер датчика,
   sensorApprovalNumber            номер официального утверждения датчика,
   sensorSCIdentifier              идентификатор компонента защиты датчика,
   sensorOSIdentifier              идентификатор операционной системы датчика
}
```

sensorSerialNumber - расширенный серийный номер датчика движения (включая номера детелей и код изготовителя).

sensorApprovalNumber - номер официального утверждения датчика движения.

sensorSCIdentifier - идентификатор компонента защиты датчика движения.

sensorOSIdentifier - идентификатор операционной системы датчика движения.

2.94 SensorInstallation (установка датчика)

Информация, записанная в датчике движения, которая имеет отношение к установке датчика движения (требование 099).

```
SensorInstallation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   sensorPairingDateFirst          дата подсоединения датчика,
   firstVuApprovalNumber           номер официального утверждения БУ,
   firstVuSerialNumber             серийный номер БУ,
   sensorPairingDateCurrent        дата подсоединения датчика,
   currentVuApprovalNumber         номер официального утверждения БУ,
   currentVUSerialNumber           серийный номер БУ
}
```

sensorPairingDateFirst - дата первого подсоединения датчика движения к бортовому устройству.

firstVuApprovalNumber - номер официального утверждения первого бортового устройства, подсоединенного к датчику движения.

firstVuSerialNumber - серийный номер первого бортового устройства, подсоединенного к датчику движения.

sensorPairingDateCurrent - дата текущего подсоединения датчика движения к бортовому устройству.

currentVuApprovalNumber - официальный номер бортового устройства, подсоединенного в данный момент к датчику движения.

currentVUSerialNumber - серийный номер бортового устройства, подсоединенного в данный момент к датчику движения.

2.95 SensorInstallationSecData (данные о защите датчика)

Информация, записанная на карточке мастерской, которая имеет отношение к данным о защите, необходимым для подсоединения датчиков движения к бортовым устройствам (требование 214).

SensorInstallationSecData ::= сеанс трехкратного шифрования ключа по системе DES

Присвоение значения: в соответствии со стандартом ISO 16844-3.

2.96 SensorOSIdentifier (идентификатор датчика ОС)

Идентификатор операционной системы датчика движения.

SensorOSIdentifier ::= Строка IA5 (РАЗМЕР (2))

Присвоение значения: по усмотрению изготовителя.

2.97 SensorPaired (подсоединенный датчик)

Информация, записанная в бортовом устройстве, которая имеет отношение к идентификации датчика движения, подсоединенного к бортовому устройству (требование 079).

```
SensorPaired ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   sensorSerialNumber                серийный номер датчика,
   sensorApprovalNumber              номер официального утверждения датчика,
   sensorPairingDateFirst            дата подсоединения датчика
}
```

sensorSerialNumber - серийный номер датчика движения, подсоединенного в данный момент к бортовому устройству.

sensorApprovalNumber - номер официального утверждения датчика движения, подсоединенного в данный момент к бортовому устройству.

sensorPairingDateFirst - дата первого подсоединения к бортовому устройству датчика движения, подсоединенного к бортовому устройству в данный момент.

2.98 SensorPairingDate (дата подсоединения датчика)

Дата подсоединения датчика движения к бортовому устройству.

SensorPairingDate ::= Реальное время.

Присвоение значения: не определено.

2.99 SensorSerialNumber (серийный номер датчика)

Серийный номер датчика движения.

SensorSerialNumber ::= Расширенный серийный номер

2.100 SensorSCIdentifier (идентификатор защиты датчика)

Идентификатор компонента защиты датчика движения.

SensorSCIdentifier ::= Страна IA5 (РАЗМЕР (8))

Присвоение значения: по усмотрению изготовителя компонента.

2.101 Signature (подпись)

Цифровая подпись.

Signature ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: в соответствии с общими механизмами защиты, определенными в подразделе 11.

2.102 SimilarEventsNumber (число аналогичных событий)

Число аналогичных событий за один конкретный день (требование 094).

SimilarEventsNumber ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: 0 не используется, 1 означает, что в данный день имело место и было зарегистрировано только одно событие этого типа, 2 означает, что в этот день имели место 2 события (из которых было зарегистрировано только одно), ...255 означает, что в данный день произошло 255 или более событий этого типа.

2.103 SpecificConditionType (тип особой ситуации)

Код, позволяющий идентифицировать ту или иную особую ситуацию (требования 050b, 105a, 212a и 230a).

SpecificConditionType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения:
'00'H RFU (зарезервировано для будущего использования)
'01'H неприменимо – начало
'02'H неприменимо - конец
'03'H Переезд на пароме /поезде
'04'H .. 'FF'HRFU

2.104 SpecificConditionRecord (запись особой ситуации)

Информация, записанная на карточке водителя, карточке предприятия и в бортовом устройстве, которая имеет отношение к особой ситуации (требования 105a, 212a и 230a).

```
SpecificConditionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   entryTime                    реальное время,
   specificConditionType        тип особой ситуации
}
```

entryTime - дата и время ввода данных.

specificConditionType - код, позволяющий идентифицировать особую ситуацию.

2.105 Speed (скорость)

Скорость транспортного средства (км/ч).

Speed ::= ЦЕЛОЕ ЧИСЛО (0,255)

Присвоение значения: км в час в рабочем диапазоне от 0 до 220 км/ч.

2.106 SpeedAuthorised (разрешенная скорость)

Максимальная разрешенная скорость транспортного средства (определение bb)).

SpeedAuthorised ::= Скорость

2.107 SpeedAverage (средняя скорость)

Средняя скорость за предварительно определенный промежуток времени (км/ч).

SpeedAverage ::= Скорость

2.108 SpeedMax (максимальная скорость)

Максимальная скорость за предварительно определенный промежуток времени.

SpeedMax ::= Скорость

2.109 TDesSessionKey (ключ сеанса)

Трехкратное шифрование ключа сеанса в системе DES.

```
TDesSessionKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   tDesKeyA                    ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))
   tDesKeyB                    ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))
}
```

Присвоение значения: дополнительно не уточняется.

2.110 TimeReal (реальное время)

Код совмещенного поля данных даты и времени, в котором дата и время выражаются в секундах, начиная с 00 ч. 00 м. 00 с. 1 января 1970 года (среднее время по Гринвичу).

TimeReal{INTEGER:TimeRealRange} ::= ЦЕЛОЕ ЧИСЛО (0..TimeRealRange)

Присвоение значения – Выровненный байт: число секунд начиная с полночи 1 января 1970 года (среднее время по Гринвичу).

Максимально возможное отображение даты/времени - 2106 год.

2.111 TyreSize (размер шин)

Обозначение размера шин.

TyreSize ::= Сторона IA5 (РАЗМЕР (15))

Присвоение значения: в соответствии с Правилами ЕЭК №°54[14].

2.112 VehicleIdentificationNumber (идентификационный номер транспортного средства)

Идентификационный номер транспортного средства (VIN), указывающий на транспортное средство в целом; обычно это серийный номер шасси или номер рамы.

VehicleIdentificationNumber ::= Сторона IA5 (РАЗМЕР (17))

Присвоение значения: в соответствии с определением в стандарте ИСО 3779.

2.113 VehicleRegistrationIdentification (идентификация регистрации транспортного средства)

Идентификация транспортного средства, индивидуальная для Европы (VRN и Договаривающаяся сторона)

```
VehicleRegistrationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   vehicleRegistrationNation          числовой код страны,
   vehicleRegistrationNumber          номер регистрации транспортного средства
}
```

vehicleRegistrationNation - страна, в которой зарегистрировано транспортное средство.

vehicleRegistrationNumber - номер регистрации транспортного средства (VRN).

2.114 VehicleRegistrationNumber (номер регистрации транспортного средства)

Номер регистрации транспортного средства (VRN). Номер регистрации присваивается компетентным органом, регистрирующим транспортное средство.

---

[14] Исходным текстом является директива ЕС 92/23/ЕЕС, касающаяся шин автотранспортных средств и их прицепов и их установки, от 31 марта 1992 года (OJ No L 129, 14/05/1992).

```
VehicleRegistrationNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   codePage                    ЦЕЛОЕ ЧИСЛО (0,255),
   vehicleRegNumber            ОКТЕТНАЯ СТРОКА (РАЗМЕР(13))
}
```

codePage - элемент данных, указывающих на раздел стандарта ISO/IEC 8859, использованный для кодирования регистрационного номера транспортного средства,

vehicleRegNumber - VRN, закодированный в соответствии со стандартом ISO/IEC 8859-codePage.

Присвоение значения: по усмотрению страны.

2.115 VuActivityDailyData (данные об изменении деятельности в БУ)

Информация, записанная в БУ, которая имеет отношение к изменению деятельности и/или изменению статуса управления и/или изменению состояния карточки за данный календарный день (требование 084) и к состоянию считывающих устройств на 00:00 часов в указанный день.

```
VuActivityDailyData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfActivityChanges         ЦЕЛОЕ ЧИСЛО (0.1440),
   activityChangeInfos         УСТАНОВЛЕННЫЙ РАЗМЕР
                               (noOfActivityChanges) ПАРАМЕТРА
                               ActivityChangeInfo
}
```

noOfActivityChanges - число слов позиции ActivityChangeInfo в совокупности данных activityChangeInfos.

activityChangeInfos - совокупность слов позиции ActivityChangeInfo, записанных в БУ за данный день. Она всегда включает два слова ActivityChangeInfo, указывающих на состояние считывающих устройств в 00:00 часов в указанный день.

2.116 VuApprovalNumber (номер официального утверждения БУ)

Номер официального утверждения типа бортового устройства

```
VuApprovalNumber ::= Сторона IA5 (РАЗМЕР (8))
```

Присвоенное значение: не определено.

2.117 VuCalibrationData (дата калибровки БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к калибровке контрольного устройства (требование 098).

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfVuCalibrationRecords          ЦЕЛОЕ ЧИСЛО (0,255),
   vuCalibrationRecords              УСТАНОВЛЕННЫЙ РАЗМЕР
                                     (noOfVuCalibrationRecords) ПАРАМЕТРА
                                     VuCalibrationRecord
}
```

noOfVuCalibrationRecords - число записей, содержащееся в совокупности vuCalibrationRecords.

vuCalibrationRecords - совокупность записей калибровки.

2.118 VuCalibrationRecord (запись калибровки БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к калибровке контрольного устройства (требование 098).

```
VuCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   calibrationPurpose                цель калибровки,
   workshopName                      название,
   workshopAddress                   адрес,
   workshopCardNumber                полный номер карточки,
   workshopCardExpiryDate            реальное время,
   vehicleIdentificationNumber       идентификационный номер транспортного
                                     средства,
   vehicleRegistrationIdentification идентификация регистрации транспортного
                                     средства,
   wVehicleCharacteristicConstant    характеристическая постоянная
                                     транспортного средства W,
   kConstantOfRecordingEquipment     постоянная записывающего оборудования K,
   lTyreCircumference                окружность шины L,
```

tyreSize	размер шины,
authorisedSpeed	разрешенная скорость,
oldOdometerValue	показания счетчика пробега,
newOdometerValue	показания счетчика пробега,
oldTimeValue	реальное время,
newTimeValue	реальное время,
nextCalibrationDate	реальное время

}

calibrationPurpose - цель калибровки.

workshopName, workshopAddress - название и адрес мастерской.

workshopCardNumber - идентификатор карточки мастерской, использованной во время калибровки.

workshopCardExpiryDate - дата истечения срока действия карточки.

vehicleIdentificationNumber - VIN (опознавательный номер транспортного средства).

vehicleRegistrationIdentification - VRN (регистрационный номер транспортного средства) и Договаривающаяся сторона регистрации.

wVehicleCharacteristicConstant - характеристический коэффициент транспортного средства.

kConstantOfRecordingEquipment - постоянная контрольного устройства.

lTyreCircumference - эффективная окружность шин колес.

tyreSize - обозначение размера шин, установленных на транспортном средстве.

authorisedSpeed - разрешенная скорость транспортного средства.

oldOdometerValue, newOdometerValue - прежние и новые показания счетчика пробега.

oldTimeValue, newTimeValue - прежние и новые значения даты и времени.

nextCalibrationDate - дата следующей калибровки типа, указанной в позиции CalibrationPurpose, которая должна быть произведена уполномоченным инспекционным органом.

2.119 VuCardIWData (данные о вводе и извлечении карточки)

Информация, записанная в бортовом устройстве, которая имеет отношение к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (требование 081).

```
VuCardIWData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfIWRecords                    ЦЕЛОЕ ЧИСЛО(0..2^16-1),
   vuCardIWRecords                  УСТАНОВЛЕННЫЙ РАЗМЕР(noOfIWRecords)
                                    ПАРАМЕТРА VuCardIWRecord
}
```

noOfIWRecords - число записей в совокупности vuCardIWRecords.

vuCardIWRecords - совокупность записей, относящихся к циклам ввода и извлечения карточек.

2.120 VuCardIWRecord (запись данных о вводе и извлечении карточки)

Информация, записанная в бортовом устройстве, которая имеет отношение к циклу ввода карточки водителя или карточки мастерской в бортовое устройство и их извлечения (требование 081).

```
VuCardIWRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   cardHolderName                   фамилия держателя,
   fullCardNumber                   полный номер карточки,
   cardExpiryDate                   реальное время,
   cardInsertionTime                реальное время,
   vehicleOdometerValueAtInsertion  показания счетчика пробега,
   cardSlotNumber                   номер считывающего устройства,
   cardWithdrawalTime               реальное время,
   vehicleOdometerValueAtWithdrawal показания счетчика пробега,
   previousVehicleInfo              информация о предыдущем транспортном
                                    средстве
   manualInputFlag                  отметка, указывающая на ручной ввод данных
}
```

cardHolderName - фамилия и имя держателя карточки водителя или мастерской, записанные в карточке.

fullCardNumber - тип карточки, выдавшая ее Договаривающаяся сторона и номер карточки, записанные в карточке.

cardExpiryDate - дата истечения срока действия карточки, записанная в карточке.

cardInsertionTime - дата и время ввода карточки.

vehicleOdometerValueAtInsertion - показания счетчика пробега транспортного средства в момент ввода карточки.

cardSlotNumber - считывающее устройство, в которое вставлена карточка.

cardWithdrawalTime - дата и время извлечения карточки.

vehicleOdometerValueAtWithdrawal - показания счетчика пробега транспортного средства в момент извлечения карточки.

previousVehicleInfo - информация о предыдущем транспортном средстве, использованном водителем, записанная в карточке.

manualInputFlag - метка, позволяющая определить, ввел ли держатель карточки в момент ее ввода данные о деятельности водителя вручную.

2.121 VuCertificate (сертификат БУ)

Сертификат открытого ключа бортового устройства.

VuCertificate ::= сертификат

2.122 VuCompanyLocksData (дата блокировки БУ предприятием)

Информация, записанная в бортовом устройстве, которая относится к блокировкам, установленным предприятием (требование 104).

```
VuCompanyLocksData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfLocks                    ЦЕЛОЕ ЧИСЛО(0..20),
   vuCompanyLocksRecords        УСТАНОВЛЕННЫЙ РАЗМЕР(noOfLocks)
                                ПАРАМЕТРА VuCompanyLocksRecord
}
```

noOfLocks - число блокировок, перечисленных в файле vuCompanyLocksRecords.

vuCompanyLocksRecords - совокупность записей о блокировках, установленных предприятием.

2.123 VuCompanyLocksRecord (запись блокировки БУ предприятием)

Информация, записанная в бортовом устройстве, которая относится к одной блокировке, произведенной предприятием (требование 104).

```
VuCompanyLocksRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   lockInTime                   реальное время,
   lockOutTime                  реальное время,
   companyName                  название,
   companyAddress               адрес,
   companyCardNumber            полный номер  карточки
}
```

lockInTime, lockOutTime - дата и время блокировки и снятия блокировки.

companyName, companyAddress - название и адрес предприятия, которое произвело блокировку.

companyCardNumber - номер, идентифицирующий карточку, использованную для блокировки.

2.124 VuControlActivityData (дата операций по проверке БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к проверкам данного БУ (требование 102).

```
VuControlActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfControls                    ЦЕЛОЕ ЧИСЛО(0..20),
   vuControlActivityRecords        УСТАНОВЛЕННЫЙ РАЗМЕР(noOfControls)
                                   ПАРАМЕТРА VuControlActivityRecord
}
```

noOfControls - число проверок, перечисленных в файле vuControlActivityRecords.

vuControlActivityRecords - совокупность записей о проверочных операциях.

2.125 VuControlActivityRecord (запись операций по проверке БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к проверке данного БУ (требование 102).

```
VuControlActivityRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   controlType                     тип проверки,
   controlTime                     реальное время,
   controlCardNumber               полный номер карточки,
   downloadPeriodBeginTime         реальное время,
   downloadPeriodEndTime           реальное время
}
```

controlType - тип проверки.

controlTime - дата и время проверки.

controlCardNumber - идентификатор карточки контролера, использованной для проверки.

downloadPeriodBeginTime - время начала периода, за который загружаются данные (в случае загрузки).

downloadPeriodEndTime - время конца периода, за который загружаются данные (в случае загрузки).

2.126 VuDataBlockCounter (счетчик блока данных БУ)

Счетчик, записанный на карточке, который позволяет определять последовательную нумерацию циклов ввода и извлечения карточки в бортовых устройствах.

VuDataBlockCounter ::= строка BCD (РАЗМЕР (2))

Присвоение значения: последовательная нумерация с максимальным значением 9 999, которая снова начинается с 0.

2.127 VuDetailedSpeedBlock (блок данных о скорости в БУ)

Информация, записанная в бортовом устройстве, которое относится к скорости транспортного средства за минуту, в течение которой транспортное средство находится в процессе движения (требование 093).

```
VuDetailedSpeedBlock ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   speedBlockBeginDate    реальное время,
   speedsPerSecond        РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ (60) параметра Speed
}
```

speedBlockBeginDate - дата и время первого значения скорости в блоке данных.

speedsPerSecond хронологическая последовательность измеряемых скоростей за каждую секунду в течение минуты, которая начинает отсчитываться с момента реального времени, отраженного в позиции speedBlockBeginDate (включительно).

2.128 VuDetailedSpeedData (данные о скорости в БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к изменению скорости транспортного средства.

```
VuDetailedSpeedData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfSpeedBlocks                ЦЕЛОЕ ЧИСЛО (0,2^16-1),
   vuDetailedSpeedBlocks          УСТАНОВЛЕННЫЙ РАЗМЕР
                                  (noOfSpeedBlocks) параметра
                                  VuDetailedSpeedBlock
}
```

noOfSpeedBlocks - число блоков скорости в совокупности vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks - совокупность блоков данных об изменении скорости.

2.129 VuDownloadablePeriod (период загрузки данных в БУ)

Самая ранняя и самая последняя дата, на которую хранятся в бортовом устройстве данные о деятельности водителя (требования 081, 084 или 087).

```
VuDownloadablePeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   minDownloadableTime
   maxDownloadableTime                    реальное время
}
```

minDownloadableTime - самая ранняя дата и время ввода карточки, въезда на данную территорию или изменения вида деятельности, которые хранятся в блоке памяти бортового устройства.

maxDownloadableTime - самая последняя дата и время извлечения карточки, въезда на данную территорию или изменения вида деятельности, которые хранятся в блоке памяти бортового устройства.

2.130 VuDownloadActivityData (информация о загрузке данных в БУ)

Информация, записанная в бортовом устройстве, которая указывает на время последней загрузки (требование 105).

```
VuDownloadActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   downloadingTime                        реальное время,
   fullCardNumber                         полный номер карточки,
   companyOrWorkshopName                  название
}
```

downloadingTime - дата и время загрузки.

fullCardNumber - идентификатор использованной карточки, разрешающий загрузку.

companyOrWorkshopName - название предприятия или мастерской.

2.131 VuEventData (данные о событиях в БУ)

Информация, записанная в бортовом устройстве, указывающая на события (требование 094, за исключением случая превышения скорости).

```
VuEventData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfVuEvents                    ЦЕЛОЕ ЧИСЛО (0,255),
   vuEventRecords                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuEvents)
                                   параметра VuEventRecord
}
```

noOfVuEvents - число событий, перечисленных в массиве данных vuEventRecords.

vuEventRecords - совокупность записей данных о событиях.

2.132 VuEventRecord (записи событий в БУ)

Информация, записанная в бортовом устройстве, указывающая на соответствующее событие (требование 094, за исключением случая превышения скорости).

```
VuEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   eventType                       тип события/неисправности,
   eventRecordPurpose              причина регистрации события/неисправности,
   eventBeginTime                  реальное время,
   eventEndTime                    реальное время,
   cardNumberDriverSlotBegin       полный номер карточки,
   cardNumberCodriverSlotBegin     полный номер карточки,
   cardNumberDriverSlotEnd         полный номер карточки,
   cardNumberCodriverSlotEnd       полный номер карточки,
   similarEventsNumber             число аналогичных событий
}
```

eventType - тип события.

eventRecordPurpose - цель регистрации данного события.

eventBeginTime - дата и время начала события.

eventEndTime - дата и время конца события.

cardNumberDriverSlotBegin - идентификатор вставленной карточки в считывающее устройство водителя в начале события.

cardNumberCodriverSlotBegin - идентификатор вставленной карточки в считывающее устройство второго водителя в начале события.

cardNumberDriverSlotEnd - идентификатор вставленной карточки в считывающее устройство водителя в конце события.

cardNumberCodriverSlotEnd - идентификатор вставленной карточки в считывающее устройство второго водителя в конце события.

similarEventsNumber - число аналогичных событий в указанный день.

Эта последовательность может быть использована для всех событий, помимо случаев превышения скорости.

2.133 VuFaultData (данные о неисправностях в БУ)

Информация, записанная в бортовом устройстве, указывающая на неисправности (требование 096).

```
VuFaultData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfVuFaults                    ЦЕЛОЕ ЧИСЛО (0,255),
   vuFaultRecords                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuFaults)
                                   параметра VuFaultRecord
}
```

noOfVuFaults - число неисправностей, перечисленных в массиве данных vuFaultRecords.

vuFaultRecords - совокупность записей о неисправностях.

2.134 VuFaultRecord (записи о неисправностях в БУ)

Информация, записанная в бортовом устройстве, которое указывает на неисправность (требование 096).

```
VuFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   faultType                       тип неисправности,
   faultRecordPurpose              цель регистрации неисправности,
   faultBeginTime                  реальное время,
   faultEndTime                    реальное время,
   cardNumberDriverSlotBegin       полный номер карточки,
```

```
   cardNumberCodriverSlotBegin          полный номер карточки,
   cardNumberDriverSlotEnd              полный номер карточки,
   cardNumberCodriverSlotEnd            полный номер карточки
}
```

faultType - тип неисправности контрольного устройства.

faultRecordPurpose - цель регистрации данной неисправности.

faultBeginTime - дата и время начала неисправности.

faultEndTime - дата и время конца неисправности.

cardNumberDriverSlotBegin - идентификатор карточки, вставленной в считывающее устройство водителя в начале неисправности.

cardNumberCodriverSlotBegin - идентификатор карточки, вставленной в считывающее устройство второго водителя в начале неисправности.

cardNumberDriverSlotEnd - идентификатор карточки, вставленной в считывающее устройство водителя в конце неисправности.

cardNumberCodriverSlotEnd - идентификатор карточки, вставленной в считывающее устройство второго водителя в конце неисправности.

2.135 VuIdentification (идентификация БУ)

Информация, записанная в бортовом устройстве, которая указывает на идентификацию бортового устройства (требование 075).

```
VuIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   vuManufacturerName                   название изготовителя БУ,
   vuManufacturerAddress                адрес изготовителя БУ,
   vuPartNumber                         номер детали БУ,
   vuSerialNumber                       серийный номер БУ,
   vuSoftwareIdentification             идентификация программного обеспечения БУ,
   vuManufacturingDate                  дата изготовления БУ,
   vuApprovalNumber                     номер официального утверждения БУ
}
```

vuManufacturerName - название изготовителя бортового устройства.

vuManufacturerAddress - адрес изготовителя бортового устройства.

vuPartNumber - номер детали бортового устройства.

vuSerialNumber - серийный номер бортового устройства.

vuSoftwareIdentification - идентификатор программного обеспечения, использованного в бортовом устройстве.

vuManufacturingDate - дата изготовления бортового устройства.

vuApprovalNumber - номер официального утверждения бортового устройства.

2.136 VuManufacturerAddress (адрес изготовителя БУ)

Адрес изготовителя бортового устройства.

VuManufacturerAddress ::= адрес.

Присвоение значения: не определено.

2.137 (название изготовителя БУ)

Название изготовителя бортового устройства.

VuManufacturerName ::= название

Присвоение значения: дата изготовления бортового устройства.

2.138 VuManufacturingDate (дата изготовления БУ)

Дата изготовления бортового устройства.

VuManufacturingDate ::= реальное время

Присвоение значения: не определено.

2.139 VuOverSpeedingControlData (данные о контроле за превышением скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости после последнего контроля за превышением скорости (требование 095).

```
VuOverSpeedingControlData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   lastOverspeedControlTime          реальное время,
   firstOverspeedSince               реальное время,
   numberOfOverspeedSince            число превышений скорости
}
```

lastOverspeedControlTime - дата и время последнего контроля за превышением скорости.

firstOverspeedSince - дата и время первого превышения скорости после указанного контроля за превышением скорости.

numberOfOverspeedSince - число случаев превышения скорости после последнего контроля за превышением скорости.

2.140 VuOverSpeedingEventData (данные о случаях превышения скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости (требование 094).

```
VuOverSpeedingEventData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfVuOverSpeedingEvents       ЦЕЛОЕ ЧИСЛО(0..255),
   vuOverSpeedingEventRecords     УСТАНОВЛЕННЫЙ
                                  РАЗМЕР(noOfVuOverSpeedingEvents) ПАРАМЕТРА
                                  VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents - число случаев, перечисленных в массиве данных vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords - массив данных, содержащий записи случаев превышения скорости.

2.141 VuOverSpeedingEventRecord (записи случаев превышения скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости (требование 094).

```
VuOverSpeedingEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   eventType                    тип события/неисправности,
   eventRecordPurpose           цель регистрации события/неисправности,
   eventBeginTime               реальное время,
   eventEndTime                 реальное время,
   maxSpeedValue                максимальная скорость,
   averageSpeedValue            средняя скорость,
   cardNumberDriverSlotBegin    полный номер карточки,
   similarEventsNumber          число аналогичных событий
}
```

eventType - тип события.

eventRecordPurpose - цель регистрации данного события.

eventBeginTime - дата и время начала события.

eventEndTime - дата и время завершения события.

maxSpeedValue - максимальная скорость, измеренная во время события.

averageSpeedValue - среднее арифметическое скорости, измеренной во время события.

cardNumberDriverSlotBegin - идентификатор карточки, вставленной в считывающее устройство водителя в начале события.

similarEventsNumber - число аналогичных событий в указанный день.

2.142 VuPartNumber (номер детали БУ)

Номер детали бортового устройства.

VuPartNumber ::= Строка IA5(РАЗМЕР(16))

Присвоение значения: по усмотрению изготовителя БУ.

2.143 VuPlaceDailyWorkPeriodData (данные о месте/ежедневном периоде работы в БУ)

Информация, записанная в бортовом устройстве, которая указывает на места, в которых водители начинают или завершают ежедневные периоды работы (требование 087).

```
VuPlaceDailyWorkPeriodData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   noOfPlaceRecords                 ЦЕЛОЕ ЧИСЛО(0..255),
   vuPlaceDailyWorkPeriodRecords    УСТАНОВЛЕННЫЙ РАЗМЕР
                                    (noOfPlaceRecords) ПАРАМЕТРА
                                    VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords - число записей, перечисленных в массиве данных vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords - массив записей с указанием мест.

2.144 VuPlaceDailyWorkPeriodRecord (записи о месте/ежедневном периоде работы в БУ)

Информация, записанная в бортовом устройстве, которая указывает на место, в котором водитель начинает или заканчивает ежедневный период работы (требование 087).

```
VuPlaceDailyWorkPeriodRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   fullCardNumber                   полный номер карточки,
   placeRecord                      запись данных о месте
}
```

fullCardNumber - тип карточки водителя, Договаривающаяся сторона, выдавшая карточку и номер карточки.

placeRecord - запись, содержащая информацию о месте въезда.

2.145 VuPrivateKey (закрытый ключ БУ)

Закрытый ключ бортового устройства.

VuPrivateKey ::= Закрытая экспонента ключа RSA

2.146 VuPublicKey (открытый ключ БУ)

Открытый ключ бортового устройства

VuPublicKey ::= открытый ключ

2.147 VuSerialNumber (серийный номер БУ)

Серийный номер бортового устройства (требование 075).

VuSerialNumber ::= расширенный серийный номер

2.148 VuSoftInstallationDate (дата установки программы БУ)

Дата установки варианта программного обеспечения бортового устройства.

VuSoftInstallationDate ::= реальное время

Присвоение значения: не определено.

2.149 VuSoftwareIdentification (идентификация программы БУ)

Информация, записанная в бортовом устройстве, которая указывает на установленное программное обеспечение.

```
VuSoftwareIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
        vuSoftwareVersion                       вариант программы БУ,
        vuSoftInstallationDate                  дата установки программы БУ
}
```

vuSoftwareVersion - номер версии программного обеспечения бортового устройства.

vuSoftInstallationDate - дата установки версии программного обеспечения.

2.150 VuSoftwareVersion (версия программы БУ)

Вариант программного обеспечения бортового устройства.

VuSoftwareVersion ::= IA5Размер(РАЗМЕР(4))

Присвоение значения: не определено.

2.151 VuSpecificConditionData (данные об особых ситуациях в БУ)

Информация, записанная в бортовом устройстве, которая указывает на особые ситуации.

```
VuSpecificConditionData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
        noOfSpecificConditionRecords        ЦЕЛОЕ ЧИСЛО(0..216-1)
        specificConditionRecords            УСТАНОВЛЕННЫЙ РАЗМЕР
                                            (noOfSpecificConditionRecords)
                                            ПАРАМЕТРА SpecificConditionRecord
}
```

noOfSpecificConditionRecords - число записей, перечисленных в массиве данных specificConditionRecords.

specificConditionRecords - массив данных, содержащих записи об особых ситуациях.

2.152 VuTimeAdjustmentData (данные о корректировке времени в БУ)

Информация, записанная в бортовом устройстве, которая указывает на корректировки времени, произведенные вне программы регулярной калибровки (требование 101)

```
VuTimeAdjustmentData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ    {
        noOfVuTimeAdjRecords                ЦЕЛОЕ ЧИСЛО(0..6),
        vuTimeAdjustmentRecords             УСТАНОВЛЕННЫЙ РАЗМЕР
                                            (noOfVuTimeAdjRecords) ПАРАМЕТРА
                                            VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords - число записей в массиве данных TimeAdjustmentRecords.

vuTimeAdjustmentRecords - массив данных с записями о корректировке времени.

2.153 VuTimeAdjustmentRecord (записи корректировки времени в БУ)

Информация, записанная в бортовом устройстве, указывающая на корректировку времени, произведенную вне программы регулярной калибровки (требование 101)

VuTimeAdjustmentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    newTimeValue реальное время,
    workshopName название,
    workshopAddress адрес,
    workshopCardNumber полный номер карточки
}

oldTimeValue, newTimeValue - прежнее и новое значения даты и времени.

workshopName, workshopAddress - название и адрес мастерской.

workshopCardNumber - идентификатор карточки мастерской, использованной для корректировки времени.

2.154 W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства

Характеристический коэффициент транспортного средства (определение k)).

W-VehicleCharacteristicConstant ::= ЦЕЛОЕ ЧИСЛО $(0..2^{16}-1)$)

Присвоение значения: Импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

2.155 WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)

Информация, записанная в карточке мастерской, которая указывает на идентификацию приложения карточки (требование 190).

WorkshopCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    typeOfTachographCardId тип оборудования
    cardStructureVersion вариант структуры карточки

noOfEventsPerType	число событий по типу
noOfFaultsPerType	число неисправностей по типу
activityStructureLength	диапазон длины записи, касающейся деятельности
noOfCardVehicleRecords	число записей, касающихся транспортного средства
noOfCardPlaceRecords	число записей, касающихся мест
noOfCalibrationRecords	число записей калибровок

}

typeOfTachographCardId - данные, указывающие на тип использованной карточки.

cardStructureVersion - данные, указывающие вариант структуры, использованной в карточке.

noOfEventsPerType - число событий по типу события, которое может храниться на карточке.

noOfFaultsPerType - число неисправностей по типу неисправности, которое может храниться на карточке

activityStructureLength - число имеющихся байтов памяти для хранения записей, касающихся деятельности.

noOfCardVehicleRecords - число записей, касающихся транспортного средства, которое может храниться на карточке.

noOfCardPlaceRecords - число мест, которое может храниться на карточке.

noOfCalibrationRecords - число записей калибровки, которое может храниться на карточке.

2.156 WorkshopCardCalibrationData (данные о калибровке на карточке мастерской)

Информация, записанная на карточке мастерской, указывающая на операцию, произведенную мастерской с карточкой (требования 227 и 229).

```
WorkshopCardCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
        calibrationTotalNumber              ЦЕЛОЕ ЧИСЛО (0 .. 2^16-1),
        calibrationPointerNewestRecord      ЦЕЛОЕ ЧИСЛО(0 .. NoOfCalibrationRecords-1),
        calibrationRecords                  УСТАНОВЛЕННЫЙ РАЗМЕР
                                            (NoOfCalibrationRecords) ПАРАМЕТРА
                                            WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber - общее число калибровок, произведенных с карточкой.

calibrationPointerNewestRecord - индекс последней обновленной записи калибровки.

Присвоение значения: число, соответствующее численному показателю записи калибровки, которое начинается с '0' в случае первой записи калибровки в структуре.

calibrationRecords - массив данных с записями, содержащими данные о калибровке и/или корректировке времени.

2.157 WorkshopCardCalibrationRecord (записи калибровки на карточке мастерской)

Информация, записанная на карточке мастерской, которая указывает на калибровку, произведенную с карточкой (требование 227).

```
WorkshopCardCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
   calibrationPurpose                   цель калибровки,
   vehicleIdentificationNumber          номер идентификации транспортного средства,
   vehicleRegistration                  идентификация регистрации транспортного
                                        средства,
   wVehicleCharacteristicConstant       характеристическая постоянная транспортного
                                        средства W,
   kConstantOfRecordingEquipment        постоянная записывающего оборудования K
   lTyreCircumference                   окружность шин L,
   tyreSize                             размер шин,
   authorisedSpeed                      разрешенная скорость,
   oldOdometerValue                     показания счетчика пробега,
   newOdometerValue                     показания счетчика пробега,
   oldTimeValue                         реальное время,
   newTimeValue                         реальное время,
   nextCalibrationDate                  реальное время,
```

vuPartNumber	номер детали БУ,
vuSerialNumber	серийный номер БУ,
sensorSerialNumber	серийный номер датчика

}

calibrationPurpose - цель калибровки.

vehicleIdentificationNumber - опознавательный номер транспортного средства (VIN).

vehicleRegistration - VIN и Договаривающаяся сторона регистрации.

wVehicleCharacteristicConstant - характеристический коэффициент транспортного средства.

kConstantOfRecordingEquipment - постоянная контрольного устройства.

lTyreCircumference - эффективная окружность шин колес.

tyreSize - обозначение размеров шин, установленных на транспортном средстве.

authorisedSpeed - максимальная разрешенная скорость транспортного средства.

oldOdometerValue, newOdometerValue - прежние и новые показания счетчика пробега.

oldTimeValue, newTimeValue - прежние и новые значения даты и времени.

nextCalibrationDate - дата следующей калибровки типа, указанного в файле CalibrationPurpose, которая должна осуществляться уполномоченным инспекционным органом.

vuPartNumber, **vuSerialNumber** и **sensorSerialNumber** - элементы данных, идентифицирующие контрольное устройство.

2.158 WorkshopCardHolderIdentification (идентификация держателя карточки мастерской)

Информация, записанная в карточке мастерской, указывающая на идентификацию держателя карточки (требование 216).

WorkshopCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

workshopName	название,
workshopAddress	адрес,
cardHolderName	фамилия держателя,
cardHolderPreferredLanguage	язык

}

workshopName - название мастерской держателя карточки.

workshopAddress - адрес мастерской держателя карточки.

cardHolderName - фамилия и имя (имена) держателя (например, фамилия механика).

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.159 WorkshopCardPIN (PIN-код карточки мастерской)

Персональный идентификационный номер карточки мастерской (требование 213).

WorkshopCardPIN ::= Строка IA5 (РАЗМЕР(8))

Присвоение значения: Известный номер PIN держателя карточки, за которым следует серия байтов 'FF' (до восьми байтов).

3. Определение диапазонов значений и размеров

Определение значений переменных, используемых для определений, содержащихся в пункте 2.

TimeRealRange ::= 2^{32}-1

3.1 Определения для карточки водителя:

Название переменной	мин.	макс.
CardActivityLengthRange	5 544 байта (28 дней, 93 изменения вида деятельности в день)	13 776 байтов (28 дней, 240 изменений вида деятельности в день)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 Определения для карточки мастерской:

Название переменной	мин.	макс.
CardActivityLengthRange	198 байтов (1 день, 93 изменения вида деятельности)	492 байта (1 день, 240 изменений вида деятельности)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 Определения для карточки контролера:

Название переменной	мин.	макс.
NoOfControlActivityRecords	230	520

3.4 Определения для карточки предприятия:

Название переменной	мин.	макс.
NoOfCompanyActivityRecords	230	520

4. Наборы знаков

В строках IA5 используются знаки ASCII, определенные в стандарте ISO/IEC 8824-1. Для удобочитаемости и простоты присвоенные значения приводятся ниже. В случае разночтений вместо этой информационной записки следует использовать стандарт ISO/IEC 8824-1.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

В других строках знаков (адрес, название, номер регистрации транспортного средства) используются, кроме того, знаки, определенные кодами 192-255 стандарта ISO/IEC 8859-1 (Набор латинских знаков типа 1) или ISO/IEC 8859-7 (Набор греческих знаков).

5. Кодирование

В случае кодирования с помощью правил кодирования ASN.1 все определенные типы данных кодируются в соответствии со стандартом ISO/IEC 8825-2 (согласованный вариант).

ПОДРАЗДЕЛ II
СПЕЦИФИКАЦИИ НА КАРТОЧКИ ТАХОГРАФА

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

1. Введение

1.1 Сокращения

Для целей настоящего подраздела используются следующие сокращения.

AC	Условия доступа
AID	Идентификатор приложения
ALW	Всегда
APDU	Элемент данных протокола приложения (структура команды)
ATR	Ответ на перезагрузку
AUT	Подтверждено
C6, C7	Контакты N° 6 и 7 карточки в соответствии с описанием в стандарте ISO/IEC 7816-2
cc	тактовые циклы (тц)
CHV	Информация для проверки идентификационных данных держателя карточки
CLA	Байт класса команды APDU
DF	Каталог: DF может содержать другие файлы (EF или DF)
EF	Элементарный файл
ENC	Зашифровано: доступ возможен только с использованием закодированных данных
etu	Элементарная единица времени (эев)
IC	Интегральная схема (ИС)
ICC	Карточка на интегральной схеме (КИС)
ID	Идентификатор
IFD	Интерфейс
IFS	Размер поля данных
IFSC	Размер поля данных на карточке
IFSD	Размер зоны данных (предназначенных для терминалов)
INS	Командный байт APDU
Lc	Длина вводимых данных для команды APDU
Le	Длина ожидаемых данных (выходные данные команды)
MF	Главный файл (корневой DF)
P1-P2	Параметрические байты
NAD	Узловой адрес, используемый в протоколе T=1
NEV	Никогда
PIN	Персональный идентификационный номер
PRO SM	Криптозащищенное сообщение
PTS	Выбор протокола передачи

RFU Зарезервировано для будущего использования
RST Перезагрузка (карточки)
SM Криптозащищенный обмен сообщениями
SW1-SW2 Байты состояния
TS Начальный знак ATR
VPP Напряжение программирования
XXh Значение XX в шестнадцатиричном исчислении
|| Символ связи 03||04=0304

1.2 Источники

В настоящем подразделе использованы следующие источники:

EN 726-3 Системы идентификационных карточек - Карточки и терминалы на интегральных схемах для передачи данных - Часть 3: применение независимых требований к карточке. Декабрь 1994 года.

ISO/IEC 7816-2 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 2: Размеры и расположение контактов. Издание первое: 1999 год.

ISO/IEC 7816-3 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 3: Электронные сигналы и протокол передачи данных. Издание 2: 1997 год.

ISO/IEC 7816-4 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 4: Межотраслевые команды обмена данных. Издание первое: 1995 год + поправка 1: 1997 год.

ISO/IEC 7816-6 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 6: Межотраслевые элементы данных. Издание первое: 1996 год + поправка 1: 1998 год.

ISO/IEC 7816-8 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 8: Межотраслевые команды, связанные с защитой. Издание первое: 1999 год.

ISO/IEC 9797 Информационные технологии - методы защиты - механизм обеспечения целостности данных с использованием функции криптографической проверки на основе алгоритма блочного шифрования. Издание 2: 1994 год.

2. Электрические и физические характеристики

TCS_200 Все электрические сигналы должны соответствовать стандарту ISO/IEC 7816-3, если не указано иное.

TCS_201 Расположение и размеры контактов карточки должны соответствовать стандарту ISO/IEC 7816-2.

2.1 Напряжение питания и потребление тока

TCS_202 Карточка должна работать в соответствии со спецификациями на предельные значения потребления, указанные в стандарте ISO/IEC 7816-3.

TCS_203 Карточка должна работать при Vcc = 3 В (± 0,3В) или при Vcc = 5В (± 0,5В).

Выбор напряжения производится в соответствии со стандартом ISO/IEC 7816-3.

2.2 Программирующее напряжение V_{pp}

TCS_204 Карточка не должна предусматривать наличие программирующего напряжения на выводе С6. Предполагается, что вывод С6 к интерфейсу не подсоединяется. На контакт С6 может подаваться напряжение V_{cc} с карточки, однако он не должен подсоединяться на массу. В любом случае это напряжение не должно интерпретироваться.

2.3 Формирование и частота тактовых сигналов

TCS_205 Карточка должна работать в диапазоне частот а 1-5 МГц в течение одного сеанса использования карточки. Тактовая частота может меняться в пределах ± 2%. Тактовая частота генерируется бортовым устройством, а не самой карточкой. Рабочий цикл может варьироваться в пределах 40-60%.

TCS_206 В соответствии с параметрами, заложенными в файле карточки EF_{ICC}, внешние часы могут останавливаться. Первый байт основного файла EF_{ICC} кодирует параметры режима остановки часов (более подробно см. стандарт EN 726-3):

Нулевой бит	**Единичный бит**		
бит 3	**бит 2**	**бит 1**	
0	0	1	Остановка часов разрешена, предпочитаемый уровень разряда отсутствует
0	1	1	Остановка часов разрешена, предпочитаемый уровень - высокий
1	0	1	Остановка часов разрешена, предпочитаемый уровень - низкий
0	0	0	Остановка часов не разрешена
0	1	0	Остановка часов разрешена только на высоком уровне
1	0	0	Остановка часов разрешена только на низком уровне

Биты 4-8 не используются.

2.4 Контакт "вход-выход"

TCS_207 Контакт C7 "вход-выход" используется для получения данных от интерфейса и передачи данных на интерфейсе. Во время работы в режиме передачи может находиться либо только карточка, либо интерфейс. В том случае, если оба устройства работают в режиме передачи, карточка повреждена не будет. Если передача данных с карточки не производится, она переключается в режим приема.

2.5 Состояние карточки

TCS_208 В случае подачи на карточку напряжения, она может находиться в двух состояниях:

- в рабочем состоянии при выполнении команд или обмене данными с цифровым блоком,

- в нерабочем состоянии в остальное время; в этом состоянии все данные на карточке сохраняются.

3. Аппаратное оборудование и передача данных

3.1 Введение

В настоящем пункте излагаются минимальные требования к функциям карточек тахографа и БУ в целях обеспечения правильной работы и эксплуатационной совместимости.

Карточки тахографа в максимальной степени соответствуют применимым нормам стандарта ISO/IEC (прежде всего ISO/IEC 7816). Однако в целях уточнения некоторых ограниченных видов использования или различий, в случае их наличия, характеристики всех команд и протоколов указываются полностью. Указанные команды полностью соответствуют упомянутым выше стандартам, если не оговорено иное.

3.2 Протокол передачи данных

TCS_300 Протокол передачи данных соответствует стандарту ISO/IEC 7816-3. В частности, БУ должно распознавать сигналы продления времени ожидания, передаваемые карточкой.

3.2.1 Протоколы

TCS_301 Карточка должна поддерживать протокол **T=0** и протокол **T=1**.

TCS_302 **T=0** - протокол по умолчанию, поэтому для изменения протокола на **T=1** нужна команда **PTS** (выбор протокола передачи).

TCS_303 Устройства должны поддерживать **прямой режим** в обоих протоколах. В этой связи для карточки прямой режим обязателен.

TCS_304 Байт **Information Field Size Card** должен быть отображен в ATR в виде AT3. Это значение должно составлять как минимум: 'F0h' (240 байт).

К протоколу применяются следующие ограничения.

TCS_305 **T=0**

- Интерфейс должен принимать ответ на входе и выходе после нарастания сигнала на RST начиная с 400 тц.

- Интерфейс должен быть способен считывать знаки, отделенные во времени на 12 эев.

- Интерфейс должен распознавать ошибочные знаки и их повторение, если они разделены во времени на 13 эев. В случае обнаружения ошибочного знака контакт "вход-выход" должен отражать сигнал ошибки в интервале 1-2 эев. Устройство должно реагировать на задержку продолжительностью 1 эев.

- Интерфейс должен принимать ATR (ответ на перезагрузку) размером 33 байта (TS+ 32)

- Если в ATR есть знак TC1, то для знаков, передаваемых интерфейсом, должно быть предусмотрено дополнительное время хранения, хотя временной интервал между знаками, посылаемыми карточкой, может и в этом случае составлять 12 эев. Это также применимо к знаку ACK, посылаемому карточкой после передачи знака P3 интерфейсом.

- Интерфейс должен принимать знак NUL, передаваемый карточкой.

- Интерфейс должен принимать дополнительный режим для ACK.

- Команда на получение ответа не может использоваться в режиме прямого вывода для получения данных, длина которых может превышать 255 байтов.

TCS_306 **T=1**

- Байт NAD не используется (NAD устанавливается на "00").

- S-блок "ABORT": не используется.

- Ошибка состояния S-блока VPP: не используется.

- Общая длина цепочки вывода данных для поля данных не должна превышать 255 байтов (для обеспечения совместимости с интерфейсом).

- Размер поля данных для интерфейса (IFSD) указывается IFD сразу же после ATR (ответ на сигнал перезагрузки): интерфейс передает запрос на указание размера информационного S-блока после ATR, после чего карточка должна передать обратно данные о размере S-блока интерфейса. Рекомендуемое значение для IFSD: 254 байта.

- Карточка не должна требовать корректировки IFS.

3.2.2 ATR (ответ на сигнал перезагрузки)

TCS_307 Устройство проверяет байты ATR в соответствии со стандартом ISO/IEC 7816-3. Проверка архивных знаков ATR не производится.

Пример базового двойного протокола ATR в соответствии со стандартом ISO/IEC 7816-3

Знак	Значение	Примечания
TS	"3Bh"	Указывает на прямое соглашение.
T0	"85h"	TD1 присуствует; 5 архивных байтов присутствуют.
TD1	"80h"	TD2 присутствует; T=0 подлежит использованию
TD2	"11h"	TA3 присутствует; T=1 подлежит использованию
TA3	"XXh" (at least "F0h")	Размер поля данных карточки (IFSC)
TH1 to TH5	"XXh"	Архивные знаки
TCK	"XXh"	Проверочный знак (исключительно OR)

TCS_308 После ответа на сигнал перезагрузки (ATR) выбирается по косвенным признакам основной файл (MF), который становится текущей директорией.

3.2.3 PTS (выбор протокола передачи)

TCS_309 Протоколом по умолчанию является T=0. Для перехода на протокол T=1 устройство должно передать на карточку сигнал PTS (также обозначаемый сокращением PPS).

TCS_310 Поскольку для карточки оба протокола T=0 и T=1 обязательны, базовый сигнал PTS для перехода с одного протокола на другой обязателен и для карточки.

PTS может использоваться, как указано в стандарте ISO/IEC 7816-3, для перехода на более высокие скорости передачи данных в бодах, чем скорость по умолчанию, предлагаемая в соответствующих случаях карточкой в ATR (байт (TA(1)).

Более высокие скорости передачи в бодах для карточки факультативны.

TCS_311 Если другая скорость передачи в бодах, помимо скорости по умолчанию, не поддерживается (или если не поддерживается выбранная скорость передачи в бодах), то карточка должна передать правильную команду PTS в соответствии со стандартом ISO/IEC 7816-3, опустив байт PPS1.

Примеры базовой команды PTS для выбора протокола указаны ниже:

Знак	Значение	Замечания
PPSS	"FFh"	Начальный знак.
PPS0	"00h" или "01h"	PPS1-PPS3 не присутствуют: "00h" для выбора T0, "01h" для выбора T1.
PK	"XXh"	Проверка знака: "XXh" = "FFh" если PPS0 = "00h", "XXh" = "FEh" если PPS0 = ""01h"".

3.3 Условия доступа (AC)

Условия доступа (AC) для команд UPDATE_BINARY и READ_BINARY определяется в каждом элементарном файле.

TCS_312 До открытия доступа к файлу с помощью этих команд должен удовлетворяться параметр AC для данного файла.

Определения имеющихся условий доступа указаны ниже:

- **ALW**: действие возможно во всех случаях и может быть выполнено без каких бы то ни было ограничений.
- **NEV**: действие невозможно ни в каких случаях.
- **AUT**: право, соответствующее успешной внешней аутентификации, должно быть открыто (производится с помощью команды EXTERNAL_AUTHENTICATE).
- **PRO SM**: команда должна передаваться с криптографической контрольной суммой в криптозащищенном виде (см. подраздел 11).
- **AUT** и **PRO SM** (комбинированные).

После обработки команды (UPDATE_BINARY и READ_BINARY) на карточке могут быть открыты следующие условия доступа:

	UPDATE_BINARY	READ_BINARY
ALW	Да	Да
NEV	Да	Да
AUT	Да	Да
PRO SM	Да	Нет
AUT и PRO SM	Да	Нет

Для команды READ_BINARY условие доступа PRO SM отсутствует. Это означает, что наличие криптографической контрольной суммы для команды READ необязательно ни в одном случае. Однако, используя значения 'ОС' для данного класса, можно использовать команду READ_BINARY в криптозащищенном виде, как описано в пункте 3.6.2.

3.4 Шифрование данных

В том случае, если надо обеспечить конфиденциальность данных, считываемых с того или иного файла, этот файл должен быть отмечен "Encrypted". Шифрование производится с использованием системы криптозащищенного обмена данными (см. подраздел 11).

3.5 Сводный перечень команд и кодов ошибок

Команды и структура файлов определяются стандартом ISO/IEC 7816-4 и соответствуют ему.

TCS_313 В настоящем разделе приводятся параметры следующих пар "команда-ответ APDU":

Команда	**INS**
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION : COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A

Команда	INS
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT : SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Слова состояния SW1 SW2 включаются в любое ответное сообщение и означают состояние обработки команды.

SW1	SW2	Значение
90	00	Нормальная обработка
61	XX	Нормальная обработка XX = число имеющихся байтов для ответа
62	81	Обработка предупреждения. Часть передаваемых обратно данных может быть повреждена
63	CX	Неправильный код CHV (PIN). Счетчик оставшихся попыток указывается с помощью "X"
64	00	Ошибка исполнения - состояние постоянной памяти не изменилось. Ошибка целостности
65	00	Ошибка исполнения - состояние постоянной памяти изменилось
65	81	Ошибка исполнения - состояние постоянной памяти изменилось - отказ памяти
66	88	Ошибка защиты: неправильная криптографическая контрольная сумма (во время криптозащищенного обмена сообщениями) или неправильный сертификат (во время проверки сертификата) или неправильная криптограмма (во время внешней аутентификации) или неправильная подпись (во время проверки подписи)
67	00	Неправильная длина (неправильные значения Lc или Le)
69	00	Запрещенная команда (отсутствие ответа в T=0)
69	82	Статус защиты неприемлем
69	83	Метод аутентификации заблокирован
69	85	Условия использования неприемлемы
69	86	Команда не разрешена (активный элементарный файл отсутствует)
69	87	Отсутствие предусмотренных криптозащищенных объектов данных

SW1	SW2	Значение
69	88	Неправильные криптозащищенные объекты данных
6A	82	Файл не найден
6A	86	Неправильные параметры P1-P2
6A	88	Исходные данные не найдены
6B	00	Неправильные параметры (выход за пределы элементарного файла)
6C	XX	Неправильная длина, SW2 указывает правильную длину. Поле данных не выдается
6D	00	Командный код не поддерживается или недействителен
6E	00	Класс не поддерживается
6F	00	Другие контрольные ошибки

3.6 Описание команд

В настоящей главе описываются параметры обязательных команд для карточек тахографа.

Дополнительные соответствующие данные, относящиеся к криптографическим операциям, даются в подразделе 11 "Общие механизмы защиты".

Все команды описываются независимо от используемого протокола (T=0 или T=1). Байты APDU: CLA, INS, P1, P2, Lc и Le указываются всегда. Если байты Lc или Le для данной команды не нужны, относящаяся к ней длина, значение и описание не заполнены.

TCS_315 Если запрашиваются оба байта длины (Lc и Le), то описываемая команда разделяется на две части; если IFD (интерфейс) использует протокол T=0 : IFD передает команду, описанную с помощью данных P3=Lc + данные, после чего направляет команду GET_RESPONSE (см. пункт 3.6.6) с P3=Le.

TCS_316 Если запрашиваются оба байта длины и если Le=0 (криптозащищенный обмен сообщениями):

- в случае использования протокола T=1 карточка выдает Le=0, передавая все имеющиеся выходные данные;

- в случае использования протокола T=0 IFD передает первую команду с P3=Lc + данные, карточка передает ответ (на это имплицитное значение Le=0) с помощью байтов состояния '**61La**', где La - число

байтов, имеющихся для ответа. После этого IFD генерирует команду GET REPONSE с P3 = La для чтения данных.

3.6.1 Select File (выбор файла)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда SELECT FILE используется:

- для выбора приложения DF (должен использоваться выбор с использованием названия);
- для выбора элементарного файла, соответствующего представленному файлу ID

3.6.1.1 Select File (AID) (Выбор по названию)

Эта команда позволяет выбрать приложение DF на карточке.

TCS_317 Эта команда может быть выполнена из любой точки структуры файла (после ATR и в любое время).

TCS_318 Выбор приложения приводит к перезагрузке текущей среды защиты. После выбора приложения используемый открытый ключ больше не выбирается, а ключ прежнего сеанса криптозащищенной передачи сообщений более недоступен. Условие доступа AUT также теряется.

TCS_319 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Выбор по названию (AID)
P2	1	'0Ch'	Ответ не требуется
Lc	1	'NNh'	Число байтов, переданных на карточку (длина AID) : '06h' для приложения тахографа
#6-#(5+NN)	NN	'XX..XXh'	AID : 'FF 54 41 43 48 4F' для приложения тахографа

Ответ на команду SELECT FILE не требуется (в случае T=1 Le отсутствует, а в случае T=0 запрос на ответ не передается).

TCS_320 **Ответное сообщение (запроса на ответ нет)**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.
- Если приложение, соответствующее AID, не найдено, состояние обработки выдается в виде '**6A82**'.
- При T=1, если присутствует байт Le, состояние выдается в виде '**6700**'.
- При T=0, если запрос на ответ поступает после команды SELECT FILE, состояние выдается в виде '**6900**'.
- Если выбранное приложение считается поврежденным (в атрибутах файла обнаружена ошибка целостности), состояние обработки выдается в виде '**6400**' или '**6581**'.

3.6.1.2 Выбор элементарного файла (EF) с использованием идентификатора файла

TCS_321 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Выбор EF по текущему каталогу DF
P2	1	'0Ch'	Ответ не требуется
Lc	1	'02h'	Число байтов, переданных на карточку
#6-#7	2	'XXXXh'	Идентификатор файла

Ответ на команду SELECT FILE не требуется (в случае T=1 байт Le отсутствует, а в случае T=0 запрос на ответ не передается).

TCS_322 **Ответное сообщение (ответ не запрашивается)**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.
- Если файл, соответствующий идентификатору, не найден, состояние обработки выдается в виде '**6A82**'.
- При T=1, если присутствует байт Le, состояние выдается в виде '**6700**'.
- При T=0, если запрос на ответ поступает после команды SELECT FILE, состояние выдается в виде '**6900**'.
- Если выбранное приложение считается поврежденным (в атрибутах файла обнаружена ошибка целостности), состояние обработки выдается в виде '**6400**' или '**6581**'.

3.6.2 Read binary (считывание данных)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда Read Binary используется для считывания данных с "прозрачного" файла.

Ответ карточки сводится к обратной передаче считанных данных, которые могут быть включены в структуру криптозащищенного обмена сообщениями.

TCS_323 Команда может быть выполнена только в том случае, если состояние защиты соответствует атрибутам защиты, определенным для элементарного файла и функции READ.

3.6.2.1 Команда, передаваемая в некриптозащищенном виде

Эта команда позволяет интерфейсу считывать данные с выбранного в данный момент файла EF в некриптозащищенном виде.

TCS_324 Считывание данных с файла с отметкой "Encrypted" с помощью этой команды невозможно.

TCS_325 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	Запрос на криптозащищенный обмен данными отсутствует
INS	1	'B0h'	
P1	1	'XXh'	Сдвиг байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Сдвиг байтов с начала файла: байт самого младшего разряда
Le	1	'XXh'	Ожидается указание длины данных. Число байтов, подлежащих извлечению

Примечание: бит 8 байта P1 должен быть равен 0.

TCS_326 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Считанные данные
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если выбран EF, состояние обработки выдается в виде **'6986'**.
- Если параметры контроля доступа к выбранному файле не удовлетворены, команда прерывается с выдачей **'6982'**.
- Если сдвиг не соответствует размеру EF (Сдвиг > размера EF), состояние обработки выдается в виде **'6B00'**.
- Если размер данных, подлежащих извлечению, не соответствует размеру EF (Сдвиг + Le > размера EF), состояние обработки выдается в виде **'6700'** или **'6Cxx'**, где 'xx' указывает точную длину.

- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл поврежден и не может быть восстановлен, и состояние обработки выдается в виде **'6400'** или **'6581'**.

- Если в записанных данных обнаруживается ошибка целостности, карточка возвращает затребованные данные, а состояние обработки выдаются в виде **'6281'**.

3.6.2.2 Команда, передаваемая в криптозащищенном виде

Эта команда позволяет интерфейсу считывать данные с выбранного в данный момент файла EF в криптозащищенном виде в целях проверки целостности полученных данных и защиты конфиденциальности данных в том случае, если EF содержит отметку "Encrypted".

TCS_327 **Командное сообщение**

Байт	**Длина**	**Значение**	**Описание**
CLA	1	'0Ch'	Запрос на криптозащищенный обмен данными
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (смещение байтов с начала файла): байт самого старшего разряда
P2	1	'XXh'	P2 (смещение байтов с начала файла): байт самого младшего разряда
Lc	1	'09h'	Длина вводимых данных в криптозащищенном виде
#6	1	'97h'	T_{LE}: метка, указывающая спецификацию ожидаемой длины
#7	1	'01h'	L_{LE}: длина ожидаемой длины
#8	1	'NNh'	Спецификация ожидаемой длины (изначальная длина Le): число байтов, подлежащих извлечению
#9	1	'8Eh'	T_{CC}: метка, указывающая криптографическую контрольную сумму
#10	1	'04h'	L_{CC}: длина следующей криптографической контрольной суммы
#11-#14	4	'XX..XXh'	Криптографическая сумма (4 байта самого старшего разряда)
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_328 **Ответ на сообщение, если файл EF не содержит отметку "Encrypted" и если входной формат криптозащищенного обмена данными правильный:**

Байт	Длина	Значение	Описание
#1	1	'81h'	T_{PV}: метка, указывающая значение обычных данных
#2	L	'NNh' или '81 NNh'	L_{PV}: длина переданных обратно данных (=изначальная длина Le). L равен 2 байтам, если L_{PV}>127 байтов
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Значения обычных данных
#(2+L+NN)	1	'8Eh'	T_{CC}: метка, указывающая криптографическую контрольную сумму
#(3+L+NN)	1	'04h'	L_{CC}: длина следующей криптографической контрольной суммы
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Криптографическая сумма (4 байта самого старшего разряда)
SW	2	'XXXXh'	Слова состояния (SW1, SW2)

TCS_329 **Ответ на сообщение, если файл EF содержит отметку "Encrypted" и если входной формат криптозащищенного обмена данными правильный:**

Байт	Длина	Значение	Описание
#1	1	'87h'	$T_{PI\,CG}$: Метка, указывающая на зашифрованные данные (криптограмма)
#2	L	'MMh' или '81 MMh'	$L_{PI\,CG}$: длина выданных зашифрованных данных (отличная от изначальной длины Le команды, что обусловлено заполнением). L равно 2 байтам, если $L_{PI\,CG}$ > 127 байтов.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Зашифрованные данные: показатель заполнения и криптограмма
#(2+L+MM)	1	'8Eh'	T_{CC}: Метка, указывающая на криптографическую контрольную сумму
#(3+L+MM)	1	'04h'	L_{CC}: Длина следующей криптографической контрольной суммы
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Криптографическая контрольная сумма (4 байта самого старшего разряда)
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

Возвращенные зашифрованные данные содержат первый байт, указывающий на использованный способ заполнения. В случае приложения тахографа показатель заполнения всегда принимает значение '01h', что указывает на соответствие использованного способа заполнения способу, предусмотренному в стандарте ISO/IEC 7816-4 (один байт, со значением '80h', за которым следует несколько нулевых байтов: ISO/IEC 9797, метод 2).

Данные о состояниях "нормальной" обработки, описанных в команде READ BINARY, передаваемой в некриптозащищенном виде (см. пункт 3.6.2.1), могут возвращаться с использованием структур ответного сообщения, описанного выше, с меткой "99h" (как указано в TCS 335).

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_330 **Ответное сообщение, если входной формат криптозащищенного обмена данными неправильный**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если ключ текущего сеанса отсутствует, состояние обработки выдается в виде '**6A88**'. Это происходит либо по той причине, что ключ сеанса еще не создан, или по той, что ключ сеанса больше недействителен (в этом случае интенфейс должен повторить процесс взаимной аутентификации в целях генерации нового ключа сеанса).

- Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена данными отсутствуют, состояние обработки выдается в виде '**6987**': эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.

- Если некоторые объекты неправильны, состояние обработки выдается в виде '**6988**': эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.

- Если проверка криптографической контрольной суммы показала неправильный результат, состояние обработки выдается в виде '**6688**'.

3.6.3 Update Binary (обновление данных)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Командное сообщение UPDATE BINARY начинает обновление (стирание + запись) битов, которые уже присутствуют в данных файла EF с помощью битов, содержащихся в команде APDU.

TCS_331 Эта команда может выполняться в том случае, если состояние защиты удовлетворяет атрибутам защиты, определенным для EF и функции UPDATE (если контроль доступа к безопасной функции UPDATE включает PRO SM, в команду должен быть включен элемент защиты данных).

3.6.3.1 Команда, передаваемая в некриптозащищенном виде

Эта команда позволяет интерфейсу записывать данные в выбранный в данный момент элементарный файл без проверки целостности полученных данных карточкой. Этот обычный режим допускается только в том случае, если соответствующий файл не содержит отметку "Encrypted".

TCS_332 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	Запрос на криптозащищенный обмен данными отсутствует
INS	1	'D6h'	
P1	1	'XXh'	Смещение байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Смещение байтов с начала файла: байт самого младшего разряда
Lc	1	'NNh'	Длина Lc данных, подлежащих обновлению. Число байтов, подлежащих записи
#6-#(5+NN)	NN	'XX..XXh'	Данные, подлежащие записи

Примечание: бит 8 байта P1 должен быть равен 0.

TCS_333 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.
- Если элементарный файл не выбран, состояние обработки выдается в виде '**6986**'.
- Если параметры контроля доступа к выбранному файлу не удовлетворены, передача команды прерывается и выдается в виде '**6982**'.
- Если сдвиг не соответствует размеру элементарного файла (сдвиг > размера EF), состояние обработки выдается в виде '**6B00**'.
- Если размер данных, подлежащих записи, не соответствует размеру элементарного файла (сдвиг + Lc > размера EF), состояние обработки выдается в виде '6700'.
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает файл поврежденным и невосстанавливаемым, и состояние обработки выдается в виде '**6400**' или '**6500**'.
- Если при записи произошел сбой, состояние обработки выдается в виде '6581'.

3.6.3.2 Команда, передаваемая в криптозащищенном виде

Эта команда позволяет интерфейсу записывать данные в элементарный файл, выбранный в данный момент, с проверкой целостности полученных данных карточкой. Поскольку требование конфиденциальности отсутствует, данные не шифруются.

TCS_334 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘0Ch’	Криптозащищенный обмен сообщениями. Запрос
INS	1	‘D6h’	INS
P1	1	‘XXh’	Сдвиг в байтах от начала файла: Байт самого старшего разряда
P2	1	‘XXh’	Сдвиг в байтах от начала файла: Байт самого младшего разряда
Lc	1	‘XXh’	Длина поля защищенных данных
#6	1	‘81h’	T_{PV}: Метка, указывающая на значение обычных данных
#7	L	‘NNh’ or ‘81 NNh’	L_{PV}: Длина переданных данных. L равно 2 байтам, если $L_{PV} > 127$ байтов
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Значение обычных данных (Данные, подлежащие записи)
#(7+L+NN)	1	‘8Eh’	T_{CC}: Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	‘04h’	L_{CC}: Длина следующей криптографической контрольной суммы
#(9+L+NN)-#(12+L+NN)	4	‘XX..XXh’	Криптографическая контрольная сумма (4 байта самого старшего разряда)
Le	1	‘00h’	Как указано в стандарте ISO/IEC 7816-4

TCS_335 **Ответное сообщение, если входной формат криптозащищенного обмена данными правильный**

Байт	Длина	Значение	Описание
#1	1	‘99h’	T_{SW}: Метка, указывающая на слова состояния (должна быть защищена с помощью криптографической суммы)
#2	1	‘02h’	L_{SW}: Длина переданных обратно слов состояния
#3-#4	2	‘XXXXh’	Слова состояния (SW1, SW2)
#5	1	‘8Eh’	T_{CC} : Метка, указывающая на слова состояния
#6	1	‘04h’	L_{CC}: Длина следующей криптографической контрольной суммы
#7-#10	4	‘XX..XXh’	Криптографическая контрольная сумма (4 байта самого старшего разряда)
SW	2	‘XXXXh’	Слова состояния (SW1, SW2)

Данные о состояниях "нормальной" обработки, описанные для команды UPDATE BINARY, передаваемой в некриптозащищенном виде (см. пункт 3.6.3.1), могут возвращаться с использованием структур ответного сообщения, описанного выше.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_336 **Ответное сообщение в случае ошибки в криптозащищенном обмене сообщениями**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если ключ текущего сеанса отсутствует, состояние обработки выдается в виде **'6A88'.**

- Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена сообщениями отсутствуют, состояние обработки выдается в виде **'6987'**: эта ошибка происходит в том случае, если отсутствует метка или если основная часть команды построена неправильно.

- Если некоторые объекты данных неправильны, состояние обработки выдается в виде **'6988'**: эта ошибка имеет место в том случае, если все требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.

- Если проверка криптографической контрольной суммы дала неправильные результаты, состояние обработки выдается в виде **'6688'**.

3.6.4 Get Challenge (получение запроса)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

Команда GET CHALLENGE предлагает карточке выдать запрос для его использования в процедуре, связанной с защитой, которая предусматривает передачу карточке криптограммы или некоторых зашифрованных данных.

TCS_337 Запрос, выданный карточкой, действителен только для следующей команды, которая использует запрос, переданный карточке.

TCS_338 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Длина ожидаемого запроса).

TCS_339 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#8	8	'XX..XXh'	Запрос
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если Le отличается от '08h', то состояние обработки выдается в виде **'6700'**.
- Если параметры P1-P2 неправильны, состояние обработки выдается в виде **'6A86'**.

3.6.5 Verify (проверка)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

Команда Verify инициирует сравнение на уровне карточки между переданными данными CHV (PIN) и исходными данными CHV, записанными на карточке.

Примечание: PIN, введенный пользователем, должен быть заполнен интерфейсом с правой стороны байтами 'FFh' до достижения длины 8 байтов.

TCS_340 Если команда проходит, права отображения CHV открываются и счетчик оставшихся попыток CHV выставляется на ноль.

TCS_341 Сравнение, которое дало неправильные результаты, регистрируется в карточке с целью ограничить число дальнейших попыток использования исходных данных CHV.

TCS_342 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (проверенные данные CHV известны по косвенным признакам)
Lc	1	'08h'	Длина переданного кода CHV
#6-#13	8	'XX..XXh'	CHV

TCS_343 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояние (SW1,SW2)

- Если команда не проходит, карточка выдает **'9000'**.
- Если исходные данные CHV не найдены, состояние обработки выдается в виде **'6A88'**.
- Если данные CHV заблокированы (счетчик оставшихся попыток CHV показывает ноль), состояние обработки выдается в виде **'6983'**. В этом состоянии данные CHV больше никогда не принимаются.
- Если сравнение дало неправильные результаты, показание счетчика оставшихся попыток уменьшается и статус обработки выдается в виде **'63CX'** (X > 0 и X равно показанию счетчика оставшихся попыток CHV. Если X = 'F', то показания счетчика попыток CHV больше 'F').

- Если исходные данные CHV считаются поврежденными, состояние обработки выдается в виде **'6400'** или **'6581'**.

3.6.6 Get Respons (получение ответа)

Эта команда соответствует стандарту ISO/IEC 7816-4.

Эта команда (необходимая и доступная только для протокола T = 0) используется для передачи подготовленных данных с карточки на интерфейс (случай, когда команда включает оба байта Lc и Le).

Команда GET_RESPONSE должна выдаваться сразу же после команды на подготовку данных, в противном случае данные потеряются. После выполнения команды GET_RESPONSE (за исключением случаев ошибки **'61xx'** или **'6Cxx'**, см. ниже) данные, подготовленные ранее, становятся недоступны.

TCS_344 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Число ожидаемых байтов

TCS_345 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Данные
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если данные карточкой подготовлены не были, состояние обработки выдается в виде **'6900'** или **'6F00'**.
- Если длина байта превышает число имеющихся байтов или если Le равно нулю, то состояние обработки выдается в виде **'6Cxx'**, где xx указывает на точное число имеющихся байтов. В этом случае подготовленные данные все еще доступны для следующей команды GET_RESPONSE.

- Если длина байта Le не равна нулю и меньше, чем число имеющихся байтов, то требуемые данные нормально передаются карточкой, а состояние обработки выдается в виде **'61xx'**, где 'xx' указывает число дополнительных байтов, все еще имеющихся для выполнения следующей команды GET_RESPONSE.

- Если команда не поддерживается (протокол T=1), карточка выдает **'6D00'**.

3.6.7 PSO: Verify Certificate (проверка сертификата)

Эта команда соответствует стандарту ISO/IEC 7816-8, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

Команда VERIFY CERTIFICATE используется карточкой для получения открытого ключа извне и проверки его действительности.

TCS_346 Если команда VERIFY CERTIFICATE проходит, открытый ключ записывается для будущего использования в среде защиты. Этот ключ должен прямо конфигурироваться для использования команд, связанных с защитой (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE) с помощью команды MSE (см. пункт 3.6.10), использующей идентификатор этого ключа.

TCS_347 В любом случае команда VERIFY CERTIFICATE использует открытый ключ, ранее выбранный командой MSE для открытия сертификата. Открытый ключ должен быть ключом одной из Договаривающихся сторон.

TCS_348 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции по защите
P1	1	'00h'	P1
P2	1	'AEh'	P2: закодированные данные к классу BER-TLV не относятся (конкатенация элементов данных)
Lc	1	'C2h'	Lc: длина сертификата, 194 байта
#6-#199	194	'XX..XXh'	Сертификат: конкатенация элементов данных (как указано в подразделе 11)

TCS_349 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если проверка сертификата дает неправильные результаты, состояние обработки выдается в виде **'6688'**. Процесс проверки и расшифровки сертификата описывается в подразделе 11.
- Если открытый ключ среды защиты отсутствует, выдается **'6A88'**.
- Если выбранный открытый ключ (используемый для расшифровки сертификата) считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.
- Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolderAuthorisation.equipmentType) отличается от '00' (т.е. не является ключом какой-либо Договаривающейся стороны), состояние обработки выдается в виде '**6985**'.

3.6.8 Internal Authenticate (внутренняя аутентификация)

Эта команда соответствует стандарту ISO/IEC 7816-4.

Используя команду INTERNAL AUTHENTICATE, интерфейс может произвести аутентификацию карточки.

Процесс аутентификации описывается в подразделе 11. Он включает следующие сообщения:

TCS_350 Команда INTERNAL AUTHENTICATE использует закрытый ключ (выбранный по косвенным признакам) для подтверждения данных аутентификации, включая K1 (первый элемент, указывающий на соответствие ключа сеанса) и RND1, и использует открытый ключ, выбранный в данный момент (на основании последней команды MSE) для шифрования подписи и создания маркера аутентификации (более подробно см. в подразделе 11).

TCS_351 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Длина данных, переданных на карточку
#6 - #13	8	'XX..XXh'	Запрос, использованный для аутентификации карточки
#14 -#21	8	'XX..XXh'	VU.CHR (см. подраздел 11)
Le	1	'80h'	Длина данных, ожидаемых от карточки

TCS_352 **Ответ на сообщение**

Байт	Длина	Значение	Описание
#1-#128	128	'XX..XXh'	Маркер аутентификации карточки (см. подраздел 11)
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если в среде защиты присутствует открытый ключ, состояние обработки дается в виде **'6A88'**.
- Если в среде защиты присутствует закрытый ключ, состояние обработки выдается в виде **'6A88'**.
- Если VU.CHR не соответствует данному идентификатору открытого ключа, состояние обработки выдается в виде **'6A88'**.
- Если выбранный закрытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

TCS_353 Если команда INTERNAL_AUTHENTICATE проходит, ключ текущего сеанса, если он существует, стирается и для создания нового ключа сеанса больше не доступен. Для создания нового ключа сеанса команда EXTERNAL_ AUTHENTICATE должна быть выполнена.

3.6.9 *External Authenticate (внешняя аутентификация)*

Эта команда соответствует стандарту ISO/IEC 7816-4.

Используя команду EXTERNAL AUTHENTICATE, карточка может произвести аутентификацию интерфейса.

Процесс аутентификации излагается в подразделе 11. Он включает следующие сообщения:

TCS_354 Команда GET CHALLENGE должна предшествовать непосредственно команде EXTERNAL_AUTHENTICATE. Карточка выдает запрос во внешнюю среду (RND3).

TCS_355 Для проверки криптограммы используется RND3 (запрос, выданный карточкой), закрытый ключ карточки (выбранный по косвенным признакам) и открытый ключ, выбранный ранее по команде MSE.

TCS_356 Карточка проверяет криптограмму и, если она правильная, открывается условие доступа AUT (на подтверждение).

TCS_357 Входная криптограмма передает второй элемент K2, указывающий на соответствие ключа сеанса.

TCS_358 **Командное сообщение**

Байт	**Длина**	**Значение**	**Описание**
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (открытый ключ, который должен использоваться, по косвенным признакам известен и был создан по команде MSE)
Lc	1	'80h'	Lc (длина данных, переданных на карточку)
#6-#133	128	'XX..XXh'	Криптограмма (см. подраздел 11)

TCS_359 **Ответ на сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова статуса (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если открытый ключ в среде защиты отсутствует, выдается **'6A88'**.
- Если CHA выбранного открытого ключа не соответствует соединению AID приложения тахографа и типа БУ, состояние обработки выдается в виде **'6F00'** (см. подраздел 11).
- Если в среде защиты закрытый ключ отсутствует, состояние обработки выдается в виде **'6A88'**.
- Если проверка криптограммы дала неправильные результаты, состояние обработки выдается в виде **'6688'**.
- Если этой команде не предшествует непосредственно команда GET CHALLENGE, состояние обработки выдается в виде **'6985'**.
- Если выбранный закрытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

TCS_360 Если команда EXTERNAL AUTHENTICATE проходит и если доступ к первой части ключа сеанса в результате выполненной перед этим команды INTERNAL AUTHENTICATE есть, ключ сеанса готов для выполнения будущих команд по процедуре криптозащищенного обмена сообщениями.

TCS_361 Если по предыдущей команде INTERNAL AUTHENTICATE первая часть ключа сеанса не доступна, вторая часть ключа сеанса, переданная интерфейсом, в карточке не регистрируется. Этот механизм обеспечивает осуществление процесса взаимной аутентификации в порядке, указанном в подразделе 11.

3.6.10 *Manage Security Environment (управление средой защиты)*

Эта команда используется для определения открытого ключа в целях аутентификации.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_362 Ключ, указанный в поле данных MSE, действителен для каждого файла DF тахографа.

TCS_363 Ключ, указанный в поле данных MSE, продолжает оставаться действующим открытым ключом до следующей правильной команды MSE.

TCS_364 Если указанный ключ в карточке еще не указан, среда защиты не меняется.

TCS_365 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: исходный ключ, действительный для всех криптографических операций
P2	1	'B6h'	P2 (исходные данные, касающиеся цифровой подписи)
Lc	1	'0Ah'	Lc: длина последующего поля данных
#6	1	'83h'	Метка, указывающая на открытый ключ в асимметричных случаях
#7	1	'08h'	Длина исходных данных ключа (идентификатор ключа)
#8-#15	08h	'XX..XXh'	Идентификатор ключа, определенный в подразделе 11

TCS_366 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.

- Если указанный ключ в карточке отсутствует, состояние обработки выдается в виде **'6A88'.**

- Если некоторые ожидаемые объекты данных в формате криптозащищенного обмена сообщениями отсутствуют, состояние обработки выдается в виде **'6987'.** Это может произойти, если отсутствует метка '83h'.

- Если некоторые объекты данных неправильны, состояние обработки выдается в виде **'6988'**. Это может произойти в том случае, если длина идентификатора ключа не соответствует '08h'.

- Если выбранный ключ считается поврежденным, состояние обработки выдается в виде **'6400'** и **'6581'**.

3.6.11 PSO: Hash (хеширование)

Эта команда используется для передачи карточке результата расчета хеширования некоторых данных. Она используется для проверки цифровых подписей. Значение хеширования хранится в памяти EEPROM для следующей команды на проверку цифровой подписи.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_367 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операций по защите
P1	1	'90h'	Возврат хеш-кода
P2	1	'A0h'	Метка: поле данных содержит объекты данных, относящиеся к хешированию
Lc	1	'16h'	Длина байта Lc последующего поля данных
#6	1	'90h'	Метка, указывающая на хеш-код
#7	1	'14h'	Длина хеш-кода
#8-#27	20	'XX..XXh'	Хеш-код

TCS_368 **Ответное на сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, состояние обработки выдается в виде **'6987'**. Это происходит в том случае, если одна из меток '90h' отсутствует.
- Если некоторые объекты данных неправильны, состояние обработки выдается в виде **'6988'**. Эта ошибка имеет место в том случае, если требуемая метка присутствует, но ее длина отличается от '14h'.

3.6.12 Perform Hash of File (хеширование файла)

Эта команда не соответствует стандарту ISO/IEC 7816-8. Поэтому байт CLA этой команды указывает на эксклюзивное использование команды PERFORM SECURITY OPERATION / HASH.

TCS_369 Команда PERFORM HASH FILE используется для хеширования зоны данных выбранного в данный момент транспарентного элементарного файла.

TCS_370 Результат операции хеширования регистрируется на карточке. Он может затем использоваться для получения цифровой подписи файла с использованием команды PSO-COMPUTE_DIGITAL_SIGNATURE. Этот результат остается доступным для команды COMPUTE DIGITAL SIGNATURE до следующей выполненной команды PERFORM HASH OF FILE.

TCS_371 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Выполнение операций по защите
P1	1	'90h'	Метка: хеширование
P2	1	'00h'	P2: хеширование данных выбранного в данный момент транспарентного файла

TCS_372 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает **'9000'**.
- Если приложение не выбрано, состояние обработки выдается в виде **'6985'**.
- Если выбранный элементарный файл считается поврежденным (ошибки в атрибутах файла или целостности записанных данных), состояние обработки выдается в виде **'6400'** или **'6581'**.
- Если выбранный файл является транспарентным файлом, состояние обработки выдается в виде **'6986'**.

3.6.13 PSO: Compute Digital Signature (расчет цифровой подписи)

Эта команда используется для расчета цифровой подписи ранее рассчитанного хеш-кода (см. ХЕШИРОВАНИЕ ФАЙЛА, пункт 3.6.12).

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_373 Закрытый ключ карточки используется для расчета цифровой подписи и известен карточке по косвенным признакам.

TCS_374 Карточка производит цифровую подпись с использованием метода заполнения, соответствующего PKCS1 (более подробно см. подраздел 11).

TCS_375 **Командное сообщение**

Байт	Длина	Значения	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Осуществление операции защиты
P1	1	'9Eh'	Цифровая подпись, подлежащая возврату
P2	1	'9Ah'	Метка: поле данных содержит данные, требующие подписи. Если поле данных не включено, то предполагается, что эти данные уже записаны на карточке (хеширование файла)
Le	1	'80h'	Длина ожидаемой подписи

TCS_376 **Ответное сообщение**

Байт	Длина	Значения	Описание
#1-#128	128	'XX..XXh'	Подпись ранее рассчитанного хеширования
SW	2	'XXXXh'	Слова состояний (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.
- Если выбранный закрытый ключ считается по косвенным признакам поврежденным, состояние обработки выдается в виде '**6400**' или '**6581**'.

3.6.14 PSO: Verify Digital Signature (проверка цифровой подписи)

Данная команда используется для проверки цифровой подписи, представленной в качестве входных данных в соответствии с параметром PKCS1 сообщения, хеш-код которой карточке известен. Алгоритм подписи известен карточке по косвенным признакам.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограниченно.

TCS_377 Команда Verify Digital Signature всегда использует открытый ключ, выбранный на основании предыдущей команды Manage Security Environment, а предыдущий хеш-код вносится командой PSO: Hash (хеширование).

TCS_378 **Командное сообщение**

Байт	Длина	Значения	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Осуществление операций защиты
P1	1	'00h'	
P2	1	'A8h'	Метка: поле данных содержит объекты данных, относящиеся к проверке
Lc	1	'83h'	Длина Lc последующего поля данных
#28	1	'9Eh'	Метка, указывающая на цифровую подпись
#29-#30	2	'8180h'	Длина цифровой подписи (128 байтов, закодированных в соответствии со стандартом ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Содержание цифровой подписи

TCS_379 **Ответное сообщение**

Байт	Длина	Значения	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- Если команда проходит, карточка выдает '**9000**'.
- Если проверка подписи дает неправильные результаты, состояние обработки выдается в виде **'6688'**. Процесс проверки описан в подразделе 11.
- Если открытый ключ не выбран, состояние обработки выдается в виде **'6A88'**.
- Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, состояние обработки выдается в виде **'6987'**. Это может произойти в том случае, если одна из требуемых меток отсутствует.
- Если хеш-кода для обработки команды нет (в результате предыдущей команды на хеширование), состояние обработки выдается в виде **'6985'**.
- Если некоторые объекты данных неправильные, состояние обработки выдается в виде **'6988'**. Это может произойти в том случае, если требуемая длина объектов данных неправильна.
- Если выбранный открытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

4. Структура карточек тахографа

В настоящем пункте уточняются структуры файлов карточек тахографа для хранения доступных данных.

В нем не указываются внутренние структуры, определяемые по усмотрению изготовителя, такие, как заголовки файлов, а также элементы хранения и обработки данных, необходимые только для внутреннего пользования, например, EuropeanPublicKey, CardPrivateKey, TDesSessionKey или WorkshopCardPin.

Полезный объем хранения данных на карточках тахографа должен составлять не менее 11 килобайт. Допускается использование большего объема. В таком случае структура карточки остается той же, однако число записей некоторых элементов структуры

увеличивается. В этом пункте указываются минимальные и максимальные значения этого количества записей.

4.1 Структура карточки водителя

TCS_400 После ее персонализации карточка водителя должна иметь следующую постоянную структуру файла и условия доступа к файлам:

		Условия доступа		
Файл	**ИД файла**	**Чтение**	**Обновление**	**Зашифрованный**
MF	3F00			
├─EF ICC	0002	ALW	NEV	Нет
├─EF IC	0005	ALW	NEV	Нет
└─DF Tachograph	0500			
├─EF Application Identification	0501	ALW	NEV	Нет
├─EF Card Certificate	C100	ALW	NEV	Нет
├─EF CA Certificate	C108	ALW	NEV	Нет
├─EF Identification	0520	ALW	NEV	Нет
├─EF Card Download	050E	ALW	ALW	Нет
├─EF Driving Licence Info	0521	ALW	NEV	Нет
├─EF Events Data	0502	ALW	PRO SM / AUT	Нет
├─EF Faults Data	0503	ALW	PRO SM / AUT	Нет
├─EF Driver Activity Data	0504	ALW	PRO SM / AUT	Нет
├─EF Vehicles Used	0505	ALW	PRO SM / AUT	Нет
├─EF Places	0506	ALW	PRO SM / AUT	Нет
├─EF Current Usage	0507	ALW	PRO SM / AUT	Нет
├─EF Control Activity Data	0508	ALW	PRO SM / AUT	Нет
└─EF Specific Conditions	0522	ALW	PRO SM / AUT	Нет

TCS_401 Все структуры элементарных файлов должны быть транспарентными.

TCS_402 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_403 Карточка водителя должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты) мин.	Размер (байты) макс.	Значения по умолчанию
ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
[illegible]		[illegible]	[illegible]	
EF Application Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving Licence Info		*53*	*53*	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events Data		*864*	*1728*	
CardEventData		864	1728	

└cardEventRecords	6	144	288	
└CardEventRecord	n_1	24	24	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults Data		*576*	*1152*	
└CardFaultData		576	1152	
└cardFaultRecords	2	288	576	
└CardFaultRecord	n_2	24	24	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 0..20}
EF Driver Activity Data		*5548*	*13780*	
└CardDriverActivity		5548	13780	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles Used		*2606*	*6202*	
└CardVehiclesUsed		2606	6202	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		2604	6200	
└CardVehicleRecord	n_3	31	31	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		841	1121	
├placePointerNewestRecord		1	1	{00}
└placeRecords		840	1120	
└PlaceRecord	n_4	10	10	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current Usage		*19*	*19*	
└CardCurrentUse		19	19	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control Activity Data		*46*	*46*	

└CardControlActivityDataRecord		46	46	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├CardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
└EF Specific Conditions		*280*	*280*	
└SpecificConditionRecord	56	5	5	
├entryTime		4	4	{00..00}
└SpecificConditionType		1	1	{00}

TCS_404 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки водители:

		мин.	**макс.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 байта (28 дней * 93 изменения вида деятельности)	13 776 байт (28 дней * 240 изменений вида деятельности)

4.2 Структура карточки мастерской

TCS_405 После персонализации карточка мастерской должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

		Условия доступа		
Файл	**ИД файла**	**Чтение**	**Обновление**	**Зашифрованный**
MF	3F00			
├EF ICC	0002	ALW	NEV	Нет
├EF IC	0005	ALW	NEV	Нет
└DF Tachograph	0500			
├EF Application Identification	0501	ALW	NEV	Нет
├EF Card Certificate	C100	ALW	NEV	Нет
├EF CA Certificate	C108	ALW	NEV	Нет
├EF Identification	0520	ALW	NEV	Нет

├EF Card Download	0509	ALW	ALW	Нет
├EF Calibration	050A	ALW	PRO SM / AUT	Нет
├EF Sensor Installation Data	050B	ALW	NEV	Да
├EF Events Data	0502	ALW	PRO SM / AUT	Нет
├EF Faults Data	0503	ALW	PRO SM / AUT	Нет
├EF Driver Activity Data	0504	ALW	PRO SM / AUT	Нет
├EF Vehicles Used	0505	ALW	PRO SM / AUT	Нет
├EF Places	0506	ALW	PRO SM / AUT	Нет
├EF Current Usage	0507	ALW	PRO SM / AUT	Нет
├EF Control Activity Data	0508	ALW	PRO SM / AUT	Нет
└EF Specific Conditions	0522	ALW	PRO SM / AUT	Нет

TCS_406 Все структуры элементарных файлов должны быть траспарентными.

TCS_407 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_408 Карточка мастерской должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты) мин.	Размер (байты) макс.	Значение по умолчанию
├EF ICC	*25*	*25*		
└CardIccIdentification	*25*	*25*		
├clockStop	1	1	{00}	
├cardExtendedSerialNumber	8	8	{00..00}	
├cardApprovalNumber	8	8	{20..20}	
├cardPersonaliserID	1	1	{00}	
├embedderIcAssemblerId	5	5	{00..00}	
└icIdentifier	2	2	{00 00}	
├EF IC	8	8		
└CardChipIdentification	8	8		
├icSerialNumber	4	4	{00..00}	
└icManufacturingReferences	4	4	{00..00}	
DF Tachograph	*11*	*2028*		
├EF Application Identification	*11*	*11*		
└WorkshopCardApplicationIdentification	*11*	*11*		
├typeOfTachographCardId	1	1	{00}	
├cardStructureVersion	2	2	{00 00}	
├noOfEventsPerType	1	1	{00}	
├noOfFaultsPerType	1	1	{00}	
├activityStructureLength	2	2	{00 00}	
├noOfCardVehicleRecords	2	2	{00 00}	
├noOfCardPlaceRecords	1	1	{00}	
└noOfCalibrationRecords	1	1	{00}	
├EF Card Certificate	*194*	*194*		
└CardCertificate	194	194	{00..00}	
├EF CA Certificate	*194*	*194*		
└MemberStateCertificate	194	194	{00..00}	

EF Identification		*211*	*211*	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		9243	26778	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		9240	26775	
WorkshopCardCalibrationRecord	n_5	105	105	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
EF Sensor Installation Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events Data		*432*	*432*	
CardEventData		432	432	
cardEventRecords	6	72	72	
CardEventRecord	n_1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

EF Faults Data		*288*	*288*	
CardFaultData		288	288	
cardFaultRecords	2	144	144	
CardFaultRecord	n_2	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver Activity Data		*202*	*496*	
CardDriverActivity		202	496	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles Used		*126*	*250*	
CardVehiclesUsed		126	250	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		124	248	
CardVehicleRecord	n_3	31	31	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		61	81	
placePointerNewestRecord		1	1	{00}
placeRecords		60	80	
PlaceRecord	n_4	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current Usage		*19*	*19*	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control Activity Data		*46*	*46*	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}

├controlVehicleRegistration				
│ ├vehicleRegistrationNation		1	1	{00}
│ └vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
└EF Specific Conditions		*10*	*10*	
└SpecificConditionRecord	2	5	5	
├entryTime		4	4	{00..00}
└SpecificConditionType		1	1	{00}

TCS_409 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки мастерской:

		мин.	**макс.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 байт (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)

4.3 Структура карточки контролера

TCS_410 После персонализации карточка контролера должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

		Условия доступа		
Файл	**ИД файла**	**Чтение**	**Обновление**	**Зашифрованный**
MF	3F00			
├EF ICC	0002	ALW	NEV	Нет
├EF IC	0005	ALW	NEV	Нет
└DF Tachograph	0500			
├EF Application Identification	0501	ALW	NEV	Нет
├EF Card Certificate	C100	ALW	NEV	Нет
├EF CA Certificate	C108	ALW	NEV	Нет
├EF Identification	0520	AUT	NEV	Нет
└EF Controller Activity Data	050C	ALW	PRO SM / AUT	Нет

TCS_411 Все структуры элементарных файлов должны быть траспарентными.

TCS_412 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_413 Карточка контролера должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты) мин.	Размер (байты) макс.	Значение по умолчанию
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		*1186*	*24226*	
EF Application Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller Activity Data		*10582*	*23922*	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n7	46	46	

├controlType	1	1	{00}
├controlTime	4	4	{00..00}
├controlledCardNumber			
│ ├cardType	1	1	{00}
│ ├CardIssuingMemberState	1	1	{00}
│ └cardNumber	16	16	{20..20}
├controlledVehicleRegistration			
│ ├vehicleRegistrationNation	1	1	{00}
│ └vehicleRegistrationNumber	14	14	{00, 20..20}
├controlDownloadPeriodBegin	4	4	{00..00}
└controlDownloadPeriodEnd	4	4	{00..00}

TCS_414 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки контролера:

		мин.	**макс.**
n_7	NoOfControlActivityRecords	230	520

4.4 Структура карточки предприятия

TCS_415 После персонализации карточка предприятия должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

		Условия доступа		
Файл	**ИД файла**	**Чтение**	**Обновление**	**Зашифрованный**
MF	3F00			
├EF ICC	0002	ALW	NEV	Нет
├EF IC	0005	ALW	NEV	Нет
└DF Tachograph	0500			
├EF Application Identification	0501	ALW	NEV	Нет
├EF Card Certificate	C100	ALW	NEV	Нет
├EF CA Certificate	C108	ALW	NEV	Нет
├EF Identification	0520	AUT	NEV	Нет
└EF Company_Activity_Data	050D	ALW	PRO SM/AUT	Нет

TCS_416 Все структуры элементарных файлов должны быть траспарентными.

TCS_417 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_418 Карточка предприятия должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты) мин.	Размер (байты) макс.	Значение по умолчанию
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		5114	24454	
EF Application Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company Activity Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n8	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_419 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки мастерской:

		мин.	**макс.**
n_8	NoOfCompanyActivityRecords	230	520

ПОДРАЗДЕЛ III

ПИКТОГРАММЫ

PIC_001 В контрольном устройстве могут использоваться следующие пиктограммы и их комбинации:

Основные пиктограммы

	Люди	**Действия**	**Режимы работы**
	Предприятие		Режим предприятия
	Контролер Контроль		Режим контроля
	Водитель Управление		Рабочий режим
	Мастерская/пункт техконтроля	Инспекция/калибровка	Режим калибровки
	Изготовитель		

	Виды деятельности	**Периоды времени**
	Готовность	Текущий период готовности
	Управление	Время непрерывного управления
	Отдых	Текущий период отдыха
	Работа	Текущий период работы
	Перерыв	Совокупная продолжительность перерывов
?	Нет данных	

	Аппаратура	**Функции**
1	Считывающее устройство для карточки водителя	
2	Считывающее устройство для карточки второго водителя	
	Карточка	
	Часы	
	Дисплей Индикация	
	Внешний носитель данных	Загрузка
	Источник питания	
	Печатающее устройство/распечатка	Печать
	Датчик	

Размер шин

Транспортное средство/бортовое устройство

Особые ситуации

OUT Неприменимо

Переезд на пароме/поезде

Разное

! События × Неисправности

Начало ежедневного периода работы Конец ежедневного периода работы

Географический пункт

M Ручной ввод данных о деятельности водителя

Защита

Скорость

Время

Σ Суммарные/сводные данные

Периодичность

24h Ежедневно

I Еженедельно

II За две недели

С … до …

Комбинации пиктограмм

Разное

Пункт контроля

Пункт начала ежедневного периода работы Пункт ежедневного периода работы

Время: с … Время: до …

С транспортного средства

OUT Начало ситуации "неприменимо" OUT Конец ситуации "неприменимо"

Карточки

Карточка водителя
Карточка предприятия
Карточка контролера
Карточка мастерской
Карточка не введена

Управление

Управление осуществляется экипажем
Время управления за одну неделю
Время управления за две недели

Распечатка данных

Распечатка сохраненных на карточке данных о деятельности водителя за сутки
Распечатка сохраненных в БУ данных о деятельности водителя за сутки
Распечатка сохраненных на карточке данных о событиях и неисправностях
Распечатка сохраненных в БУ данных о событиях и неисправностях
Распечатка технических данных
Распечатка данных о превышениях скорости

События

Ввод недействительной карточки
Несовместимость карточки
Нестыковка времени
Управление без соответствующей карточки
Ввод карточки во время управления
Ошибка при завершении последнего сеанса работы с карточкой
Превышение скорости
Прекращение электропитания
Ошибка в данных о движении
Нарушение защиты
Корректировка времени (в мастерской)
Контроль за превышениями скорости

Неисправности

×▪1 Сбой в работе карточки (считывающее устройство водителя)
×▪2 Сбой в работе карточки (считывающее устройство второго водителя)
×□ Сбой в работе дисплея
×↧ Сбой загрузки данных
×▼ Сбой в работе печатающего устройства
×Л Сбой в работе датчика
×Д Внутренние неполадки в БУ

Процедура ручного ввода данных

▮▶?▶▮ Продолжение того же ежедневного периода работы?
▶▮? Конец предыдущего периода работы?
▶▮●? Подтвердить или ввести пункт окончания рабочего периода
◷▮▶? Ввести время начала
●▮▶? Ввести пункт начала рабочего периода.

Примечание. В подразделе IV указаны дополнительные комбинации пиктограмм, используемые в качестве идентификаторов блоков или записей данных при распечатке.

ПОДРАЗДЕЛ IV

РАСПЕЧАТКА ДАННЫХ

СОДЕРЖАНИЕ

1. Общие положения

Каждая распечатка составляется из следующих друг за другом блоков различных данных, которые могут быть обозначены идентификаторами блоков.

Блок данных состоит из одной или нескольких записей, которые могут быть обозначены идентификаторами записей.

PRT_001 Если идентификатору записи непосредственно предшествует идентификатор блока данных, то идентификатор записи не печатается.

PRT_002 Если элемент данных отсутствует или не подлежит распечатке в силу режима доступа к данным, вместо него распечатывается серия пробелов.

PRT_003 Если содержание целой строки отсутствует или не нуждается в распечатке, эта строка опускается целиком.

PRT_004 Поля числовых данных печатаются с выравниванием по правому краю; в качестве символа, отделяющего разряды тысяч и миллионов, используется пробел; начальные нули не печатаются.

PRT_005 Поля строковых данных печатаются с выравниванием по левому краю и заполняются пробелами на всю оставшуюся длину элемента данных, а в соответствующих случаях (названия, фамилии, адреса) печатаются в форме, усеченной до размеров элемента данных.

2. Спецификации блоков данных

В тексте данной главы применяются следующие условные обозначения:

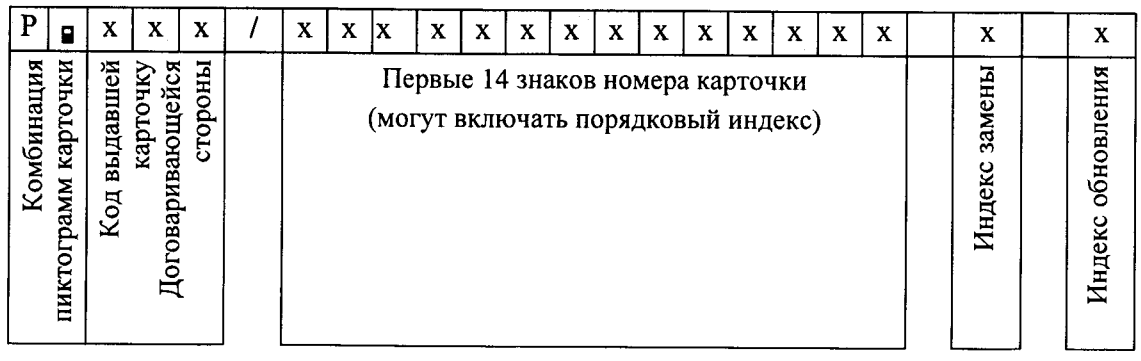
- **жирным шрифтом** обозначена информация, распечатываемая в текстовой форме (при распечатке используется обычный шрифт);

- обычным шрифтом указаны переменные параметры (поля для пиктограмм или виды данных), вместо которых распечатываются соответствующие пиктограммы или значения;

- к названиям переменных параметров добавлены символы подчеркивания, указывающие длину элемента данных, выделенного под соответствующий параметр;

- даты указываются в формате "дд/мм/гггг" (день-месяц-год). Допускается также использование формата "дд.мм.гггг";

- под термином "идентификационные данные карточки" понимается совокупность следующих компонентов: вид карточки, обозначаемый комбинацией соответствующих пиктограмм, код Договаривающейся стороны, выдавшей карточку, наклонная черта вправо и номер карточки с индексом замены и индексом обновления, отделенными пробелом:



PRT_006 При распечатке данные делятся на блоки и/или записи данных, перечисляемые ниже с указанием их значения и формата:

Номер блока или записи Значение	Формат данных
1. ***Дата и время распечатки документа***	▼ дд/мм/гггг чч:мм **(UTC)**
2. ***Вид распечатки***	
Идентификатор блока данных	----------▼----------
Комбинация пиктограмм, соответствующих данной распечатке (см. подраздел III), положение устройства ограничения скорости (только при распечатке данных о превышениях скорости)	Пикто **xxx км/ч**

3. ***Идентификационные данные держателя карточки***

Идентификатор блока данных. P = пиктограмма "люди"	----------P----------
Фамилия держателя карточки	P Фамилия_____
Имя (имена) держателя карточки (если имеются)	Имя_____
Идентификационные данные карточки	Идент._данные_карточки_____
Срок действия карточки (если он ограничен)	дд/мм/гггг

На карточки, не принадлежащие конкретным лицам, вместо фамилии держателя наносится название предприятия, мастерской или контрольного органа.

4. ***Идентификационные данные транспортного средства***

Идентификатор блока данных	----------A----------
VIN	A VIN_____
Договаривающаяся сторона регистрации транспортного средства и VRN	Гос/VRN_____

5. ***Идентификационные данные БУ***

Идентификатор блока данных	----------B----------
Название изготовителя БУ	B Изготовитель_БУ_____
Номер детали БУ	Номер_детали_БУ __

6. ***Последняя калибровка контрольного устройства***

Идентификатор блока данных	----------T----------
Название мастерской	T Фамилия_____
Идентификационные данные карточки мастерской	Идент._данные_карточки_____
Дата калибровки	T дд/мм/гггг

7. ***Последний контроль (проверка контролером)***

Идентификатор блока данных	----------▫----------
Идентификационные данные карточки контролера	Идент._данные_карточки_____
Дата, время и вид контроля	▫ дд/мм/гггг чч:мм пррр

Вид контроля: до четырех пиктограмм. Возможные виды контроля (по отдельности или в сочетании друг с другом):

▪: загрузка данных с карточки, ▾: загрузка данных с БУ, ▾: распечатка, ▫: вывод на дисплей.

8. ***Данные о деятельности водителя, сохраняемые на карточке в хронологической последовательности***

Идентификатор блока данных	----------▫----------
Проверяемая дата (календарный день, данные за который подлежат распечатке) + календарный счетчик вводов карточки	дд/мм/гггг ххх

8.1 *Период, в течение которого карточка находилась вне устройства*

8.1a Идентификатор записи (начало периода)	----------
8.1b *Период, за который нет данных.* Время начала и окончания, продолжительность	чч:мм чч:мм чччмм
8.1c *Данные о деятельности, введенные вручную.*	А чч:мм чч:мм чччмм *
Пиктограмма вида деятельности, время начала и окончания (включительно), продолжительность, периоды отдыха длительностью не менее одного часа помечаются звездочкой.	

8.2 *Ввод карточки в считывающее устройство S*

Идентификатор записи; S = пиктограмма считывающего устройства	---------S---------
Договаривающаяся сторона регистрации транспортного средства и его VRN	д Гос/VRN_____
Показания счетчика пробега на момент ввода карточки	x xxx xxx км

8.3 *Деятельность (между вводом и извлечением карточки)*

Пиктограмма вида деятельности, время начала и окончания (включительно), продолжительность, состав экипажа (пиктограмма "экипаж" при наличии экипажа (CREW), пробелы при наличии одиночного водителя (SINGLE)), периоды отдыха длительностью не менее одного часа помечаются звездочкой.	А чч:мм чч:мм ччмм

8.3a *Особые ситуации.* Время ввода данных, пиктограмма (или комбинация пиктограмм) особой ситуации.

чч:мм -----pppp-----

8.4 *Извлечение карточки*

Показания счетчика пробега и расстояние, пройденное с момента последнего ввода карточки, при котором были зафиксированы показания счетчика пробега.	x xxx xxx км; x xxx км

9. ***Данные о деятельности водителей, сохраненные в БУ отдельно для каждого считывающего устройства в хронологическом порядке***

Идентификатор блока данных	----------o----------
Проверяемая дата (календарные сутки, данные за которые подлежат распечатке)	дд/мм/гггг
Показания счетчика пробега на 00:00 часов и на 24:00 часа	x xxx xxx - x xxx xxx км

10. ***Данные о деятельности водителей со считывающего устройства S***

Идентификатор блока данных	----------S----------

10.1 *Период отсутствия карточки в считывающем устройстве S*

Идентификатор записи	----------
Карточка не введена	⊙■---
Показания счетчика пробега на начало периода	x xxx xxx **км**

10.2 *Ввод карточки*

Идентификатор записи о вводе карточки	----------
Фамилия водителя	⊙ Фамилия_____
Имя водителя	Имя_____
Идентификационные данные карточки водителя	Идент._данные_карточки_____
Срок действия карточки водителя	дд/мм/гггг
Договаривающаяся сторона регистрации предыдущего транспортного средства, которым управлял водитель, и его VRN	**Д**+Гос/VRN_____
Дата и время извлечения карточки из предыдущего транспортного средства	дд/мм/гггг чч:мм
Пустая строка	
Показания счетчика пробега на момент ввода карточки, метка ручного ввода данных о деятельности водителя (М - "да", пробел - "нет").	x xxx xxx **км** **М**

10.3 *Деятельность*

Пиктограмма вида деятельности, время начала и окончания (включительно), продолжительность, состав экипажа (пиктограмма "экипаж" при наличии экипажа (CREW), пробелы при наличии одиночного водителя (SINGLE)), периоды отдыха длительностью не менее одного часа помечаются звездочкой.	A чч:мм чч:мм ччмм ⊙⊙ *

10.3a *Особые ситуации.* Время ввода данных, пиктограмма (или комбинация пиктограмм) особой ситуации.

```
чч:мм -----pppp-----
```

10.4 *Извлечение карточки или окончание периода отсутствия карточки*

Показания счетчика пробега на момент извлечения карточки или окончания периода отсутствия карточки в устройстве и расстояние, пройденное с момента ввода карточки или с начала периода отсутствия карточки в устройстве.

```
x xxx xxx км; x xxx км
```

11. ***Суточная сводка***

Идентификатор блока данных

```
----------Σ-----------
```

11.1 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки водителя*

Идентификатор блока данных

```
1◙▮---
```

11.2 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки второго водителя*

Идентификатор блока данных

```
2◙▮---
```

11.3 *Суточная сводка данных БУ по каждому водителю*

Идентификатор записи

Фамилия водителя

Имя (имена) водителя

Идентификационные данные карточки водителя

```
------------------
Фамилия_____
Имя_____
Идент._данные_карточки_____
```

11.4 *Введенные данные о месте начала и/или окончания ежедневного периода работы*

пи = пиктограмма места начала / окончания, время, страна, район

Показания счетчика пробега

```
пи чч:мм Стр Рег

 x xxx xxx км
```

11.5 *Суммарные данные о деятельности водителя (с карточки)*

Общее время управления, пройденное расстояние	⊙ чччмм x xxx км
Общее время работы и готовности	✻ чччмм ⧈ чччмм
Общее время отдыха и отсутствия данных	⊢ чччмм ? чччмм
Суммарное время деятельности экипажа	⊙⊙ чччмм

11.6 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки водителя)*

Общее время управления, пройденное расстояние	⊙ чччмм x xxx км
Общее время работы и готовности	✻ чччмм ⧈ чччмм
Общее время отдыха	⊢ чччмм

11.7 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки второго водителя)*

Общее время работы и готовности	✻ чччмм ⧈ чччмм
Общее время отдыха	⊢ чччмм

11.8 *Суммарные данные о деятельности (каждого водителя по данным обоих считывающих устройств)*

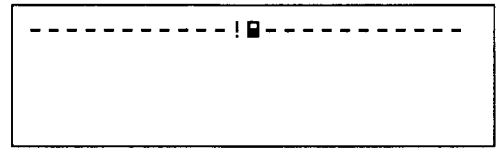
Общее время управления, пройденное расстояние	⊙ чччмм x xxx км
Общее время работы и готовности	✻ чччмм ⧈ чччмм
Общее время отдыха	⊢ чччмм
Суммарное время деятельности экипажа	⊙⊙ чччмм

При вводе команды на распечатку суточной сводки за текущий день имеющиеся данные за сутки суммируются по состоянию на момент распечатки.

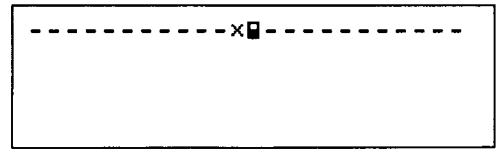
12. ***События и/или неисправности, зарегистрированные на карточке***

12.1 Идентификатор блока данных: последние 5 "событий и неисправностей", зарегистрированных на карточке	----------!×■----------

12.2 Идентификатор блока данных: все "события", зарегистрированные на карточке



12.3 Идентификатор блока данных: все "неисправности", зарегистрированные на карточке



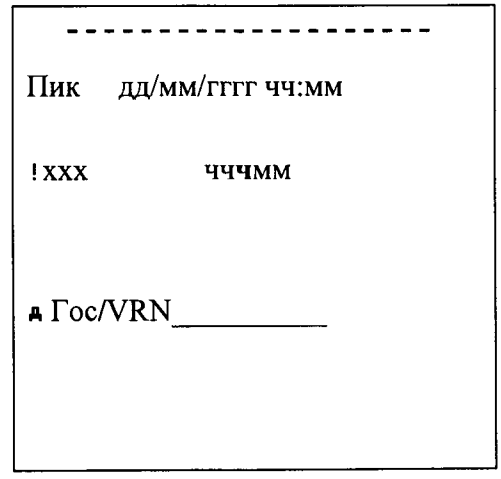
12.4 *Запись о событии и/или неисправности*

Идентификатор записи

Пиктограмма события/неисправности, назначение записи, дата и время начала

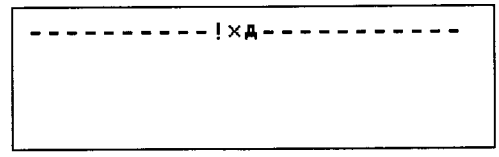
Дополнительный код события/неисправности (если имеется), продолжительность

Договаривающаяся сторона регистрации транспортного средства, в котором имело место событие или неисправность, и VRN этого транспортного средства

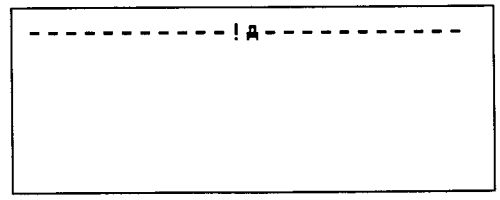


13. ***Прошлые или текущие события и/или неисправности, зарегистрированные или регистрируемые бортовым устройством***

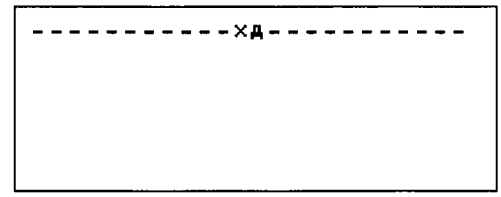
13.1 Идентификатор блока данных: последние 5 "событий и неисправностей" по данным БУ



13.2 Идентификатор блока данных: все прошлые или текущие "события", зарегистрированные или регистрируемые БУ



13.3 Идентификатор блока данных: все прошлые или текущие "неисправности", зарегистрированные или регистрируемые БУ



13.4 *Запись о событии и/или неисправности*

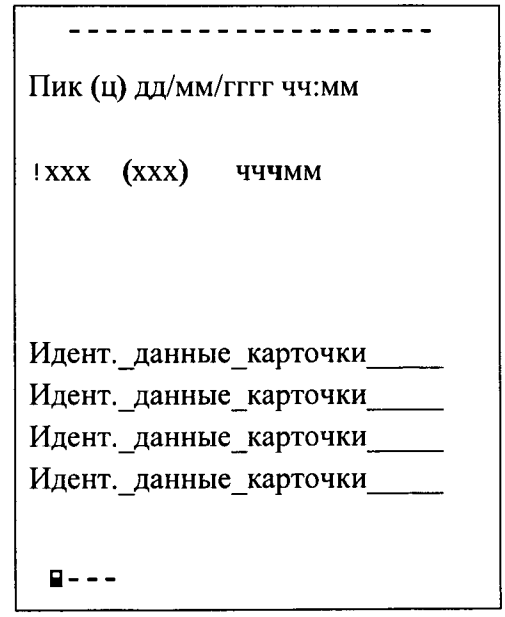
Идентификатор записи

Пиктограмма события/неисправности, цель записи, дата и время начала

Дополнительный код события/неисправности (если имеется), количество аналогичных событий за текущий день, продолжительность

Идентификационные данные карточек, находившихся в устройстве на момент начала или окончания события или неисправности (до 4 строк без повторения одних и тех же номеров карточек)

Отсутствие карточки в устройстве



Цель записи (ц) указывается числовым кодом, обозначающим цель регистрации события или неисправности и определяемым в порядке, предусмотренном для элемента данных EventFaultRecordPurpose.

14. ***Идентификационные данные БУ***

Идентификатор блока данных

Название изготовителя БУ

Адрес изготовителя БУ

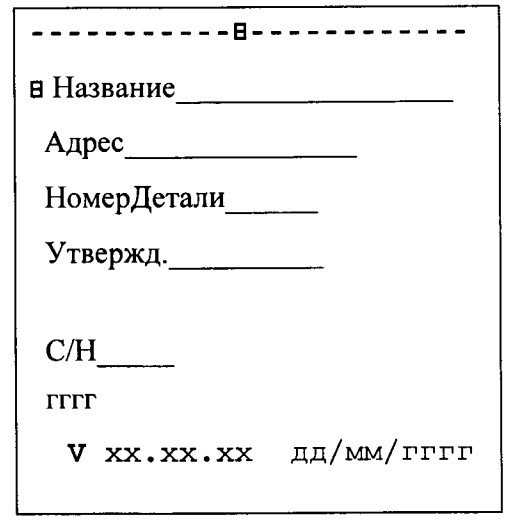
Номер детали БУ

Номер решения об официальном утверждении данного образца БУ

Серийный номер БУ

Год выпуска БУ

Версия и дата установки программного обеспечения БУ



15. ***Идентификационные данные датчика***

Идентификатор блока данных	----------л----------
Серийный номер датчика	л С/Н_____
Номер решения об официальном утверждении данного образца датчика	Утвержд._____
Дата первой установки датчика	дд/мм/гггг

16. ***Данные калибровки***

Идентификатор блока данных	----------т----------

16.1 *Запись о калибровке*

Идентификатор записи	----------
Мастерская, где произведена калибровка	т Название_мастерской _____
Адрес мастерской	Адрес_мастерской _____
Идентификационные данные карточки мастерской	Идент._данные_карточки_____
Срок действия карточки мастерской	дд/мм/гггг
Пустая строка	
Дата калибровки + цель калибровки	т дд/мм/гггг (ц)
VIN	д VIN_____
Договаривающаяся сторона регистрации транспортного средства и его VRN	Гос/VRN_____
Характеристический коэффициент транспортного средства	**w** xx xxx **имп/км**
Постоянная контрольного устройства	**k** xx xxx **имп/км**
Эффективная окружность шин колес	**l** xx xxx **мм**
Размер шин, установленных на транспортном средстве	о РазмерШин_____
Положение устройства ограничения скорости	**>** xxx **км/ч**
Показания счетчика пробега до и после калибровки	x xxx xxx – x xxx xxx **км**

Цель калибровки (p) указывается числовым кодом, обозначающим цель регистрации соответствующих калибровочных параметров и определяемым в порядке, предусмотренном для элемента данных CalibrationPurpose.

17. ***Корректировка времени***

Идентификатор блока данных	----------o----------

17.1 *Запись о корректировке времени*

Идентификатор записи	----------
Дата и время до корректировки	дд/мм/гггг чч:мм
Дата и время после корректировки	дд/мм/гггг чч:мм
Мастерская, где произведена корректировка времени	Название_мастерской____
Адрес мастерской	Адрес_мастерской_____
Идентификационные данные карточки мастерской	Идент._данные_карточки__
Срок действия карточки мастерской	дд/мм/гггг

18. ***Зарегистрированные БУ данные о последних по времени событии и неисправности***

Идентификатор блока данных	----------!×▲----------
Дата и время последнего события	дд/мм/гггг чч:мм
Дата и время последней неисправности	дд/мм/гггг чч:мм

19. ***Информация о контроле за превышениями скорости***

Идентификатор блока данных	----------»»----------
Дата и время последнего контроля за превышениями скорости	»дд/мм/гггг чч:мм
Дата и время первого превышения скорости и количество последующих превышений скорости	»»дд/мм/гггг чч:мм (nnn)

20. ***Запись о превышениях скорости***

20.1	Идентификатор блока данных: первое превышение скорости со времени последней калибровки	--------->>T---------
20.2	Идентификатор блока данных: 5 наиболее серьезных превышений за последние 365 дней	-------->>(365)------
20.3	Идентификатор блока данных: наиболее серьезное превышение за каждые из последних 10 дней, когда превышения имели место	-------->>(10)-------
20.4	Идентификатор записи Дата, время и продолжительность Максимальная и средняя скорость, количество аналогичных событий за данный день Фамилия водителя Имя (имена) водителя Идентификационные данные карточки водителя	---------- >>дд/мм/гггг чч:мм ччмм xxx **км/ч** xxx **км/ч**(xxx) ⊙ Фамилия_____ Имя_____ Идент._данные_карточки_____
20.5	Если в блоке данных записи о превышениях скорости отсутствуют	>>---

21 ***Информация, вписываемая от руки***

	Идентификатор блока данных	----------
21.1	Место контроля	⊡• .....
21.2	Подпись контролера	⊡ .....
21.3	Время: от	⊙+ .....
21.4	Время: до	+⊙ .....
21.5	Подпись водителя	⊙ .....

"Информация, вписываемая от руки": над названием графы, заполняемой от руки, следует оставить достаточное количество пустых строк для вписывания необходимой информации или для собственноручной подписи.

3. Спецификации распечатки данных

В тексте данной главы применяются следующие условные обозначения:

N	Распечатка блока или записи данных под номером N
N	Распечатка блока или записи данных под номером N нужное количество раз
X / Y	Распечатка по мере необходимости блоков или записей данных под номером X и/или Y и ее повторение нужное количество раз

3.1 Распечатка сохраненных на карточке данных о деятельности водителя за сутки

PRT_007 При распечатке сохраненных на карточке данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные)
6	Последняя калибровка данного БУ
7	Предыдущий контроль деятельности проверяемого водителя
8	Ограничитель данных о деятельности водителя
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Деятельность водителя в хронологическом порядке
11	Ограничитель данных суточной сводки

11.4	Въезд в географические пункты в хронологическом порядке
11.5	Суммарные данные о деятельности
12.1	Ограничитель сохраненных на карточке данных о событиях и неисправностях
12.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные на карточке)
13.1	Ограничитель данных БУ о событиях и неисправностях
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.2 Распечатка сохраненных в БУ данных о деятельности водителя за сутки

PRT_008 При распечатке сохраненных в БУ данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные)
6	Последняя калибровка данного БУ
7	Предыдущий контроль с помощью данного контрольного устройства
9	Ограничитель данных о деятельности водителя
10	Ограничитель данных со считывающего устройства для карточки водителя (считывающее устройство 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства для карточки водителя)

10	Ограничитель данных со считывающего устройства для карточки второго водителя (считывающее устройство 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства для карточки второго водителя)
11	Ограничитель данных суточной сводки
11.1	Сводные данные о периодах отсутствия карточки в считывающем устройстве для карточки водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.6	Суммарные данные о деятельности
11.2	Сводные данные о периодах отсутствия карточки в считывающем устройстве для карточки второго водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.7	Суммарные данные о деятельности
11.3	Суммарные данные о деятельности водителя по данным обоих считывающих устройств
11.4	Въезд данного водителя в географические пункты в хронологическом порядке
11.7	Суммарные данные о деятельности данного водителя
13.1	Ограничитель данных о событиях и отказах
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
21.1	Место контроля
21.2	Подпись контролера
21.3	Время: с (место для указания водителем, не имеющим
21.4	Время: до карточки, относящихся к нему периодов времени)
21.5	Подпись водителя

3.3 Распечатка сохраненных на карточке данных о событиях и неисправностях

PRT_009 При распечатке сохраненных на карточке данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
12.2	Ограничитель данных о событиях
12.4	Записи о событиях (все события, зарегистрированные на карточке)
12.3	Ограничитель данных о неисправностях
12.4	Записи о неисправностях (все неисправности, зарегистрированные на карточке)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.4 Распечатка сохраненных в БУ данных о событиях и неисправностях

PRT_010 При распечатке сохраненных в БУ данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
13.2	Ограничитель данных о событиях
13.4	Записи о событиях (все события, зарегистрированные или регистрируемые БУ)

13.3	Ограничитель данных о неисправностях
13.4	Записи о событиях (все неисправности, зарегистрированные или регистрируемые БУ)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.5 Распечатка технических данных

PRT_011 При распечатке технических данных соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
14	Идентификационные данные БУ
15	Идентификационные данные датчика

16	Ограничитель данных калибровки
16.1	Записи о калибровке (все имеющиеся записи в хронологическом порядке)
17	Ограничитель данных о корректировке времени
17.1	Записи о корректировке времени (все имеющиеся записи о корректировке времени, в том числе относящиеся к калибровке)
18	Последние по времени событие и неисправность, зарегистрированные БУ

3.6 Распечатка данных о превышениях скорости

PRT_012 При распечатке данных о превышениях скорости соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
19	Информация о контроле за превышениями скорости
20.1	Идентификатор данных о превышениях скорости
20.4 / 20.5	Первое превышение скорости со времени последней калибровки
20.2	Идентификатор данных о превышениях скорости
20.4 / 20.5	5 наиболее серьезных превышений скорости за последние 365 дней
20.3	Идентификатор данных о превышениях скорости
20.4 / 20.5	Наиболее серьезное превышение скорости за каждые из последних 10 дней, когда превышения имели место
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

ПОДРАЗДЕЛ V

ИНДИКАЦИЯ НА ДИСПЛЕЕ

В тексте настоящего подраздела применяются следующие условные обозначения:

- **жирным шрифтом** обозначена информация, выводимая на дисплей в текстовой форме (на дисплее используется обычный шрифт),
- обычным шрифтом указаны переменные параметры (поля для пиктограмм или виды данных), вместо которых отображаются соответствующие пиктограммы или значения:

- дд мм гггг: день, месяц, год;
- чч: часы;
- мм: минуты;
- B: пиктограмма периода времени;
- CO: комбинация пиктограмм события и неисправности;
- P: пиктограмма режима работы.

DIS_001 При индикации данных контрольного устройства соблюдается следующий формат:

Данные	Формат
Вид дисплея по умолчанию	
Местное время	чч:мм
Режим работы	P
Информация, касающаяся водителя	1Bччмм ▮ччмм
Информация, касающаяся второго водителя	2Bччмм
Начало ситуации "неприменимо"	OUT
Предупреждающие индикаторы	
Превышение времени непрерывного управления	1◉ччмм ▮ччмм
Событие или неисправность	CO
Прочие индикаторы	
Дата в формате UTC Время	**UTC**◉дд/мм/гггг или **UTC**◉дд.мм.гггг чч:мм
Время непрерывного управления и совокупная продолжительность перерывов у водителя	1◉ччмм ▮ччмм

Время непрерывного управления и совокупная продолжительность перерывов у второго водителя	2⊙чччмм ııчччмм
Совокупное время управления за прошлую и текущую неделю у водителя	1⊙‖ ччччмм
Совокупное время управления за прошлую и текущую неделю у второго водителя	2⊙‖ ччччмм

ПОДРАЗДЕЛ VI

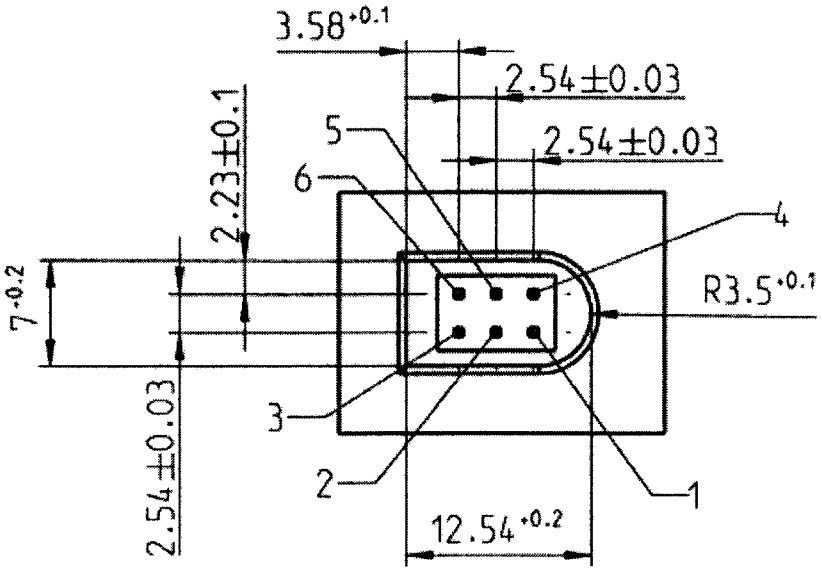
ВНЕШНИЕ ИНТЕРФЕЙСЫ

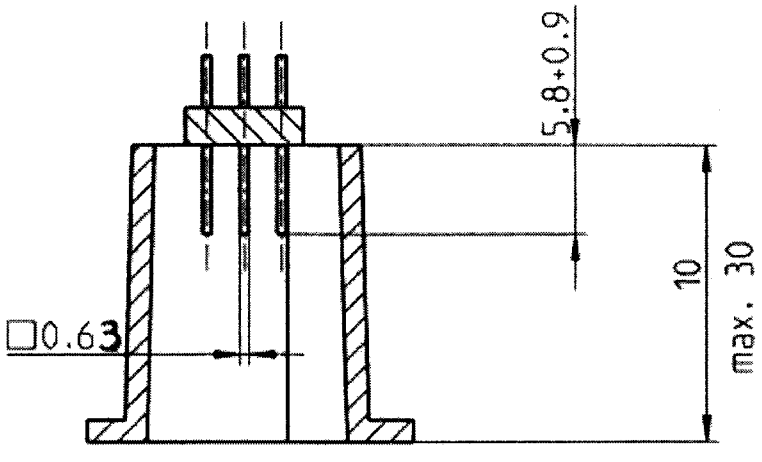
СОДЕРЖАНИЕ

1. Аппаратная часть

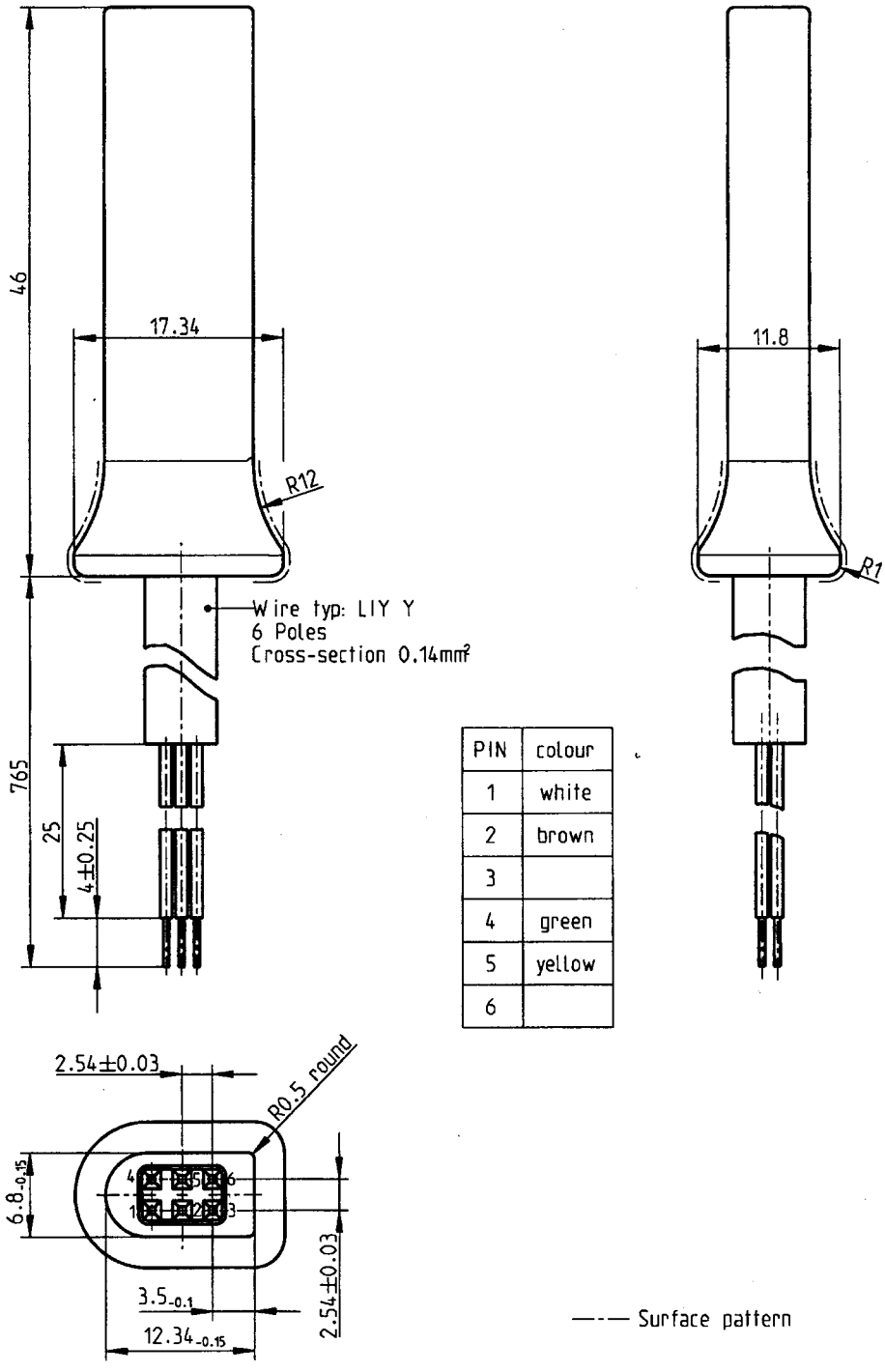
1.1 Разъем

INT_001 Соединительное гнездо для загрузки данных и калибровки должно располагаться на передней панели, быть доступным без снятия каких-либо деталей контрольного устройства и представлять собой 6-контактный разъем, выполненный в соответствии с нижеследующими чертежами (все размеры указаны в миллиметрах):





Типовая схема вилки 6-контактного штепсельного разъема:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

Тип провода: LIY Y	
6 полюсов	
Поперечное сечение 0,14 мм^2	
Контакт	Цвет
1	белый
2	коричневый

3	
4	зеленый
5	желтый
6	
Закругление R0,5	Профиль поверхности

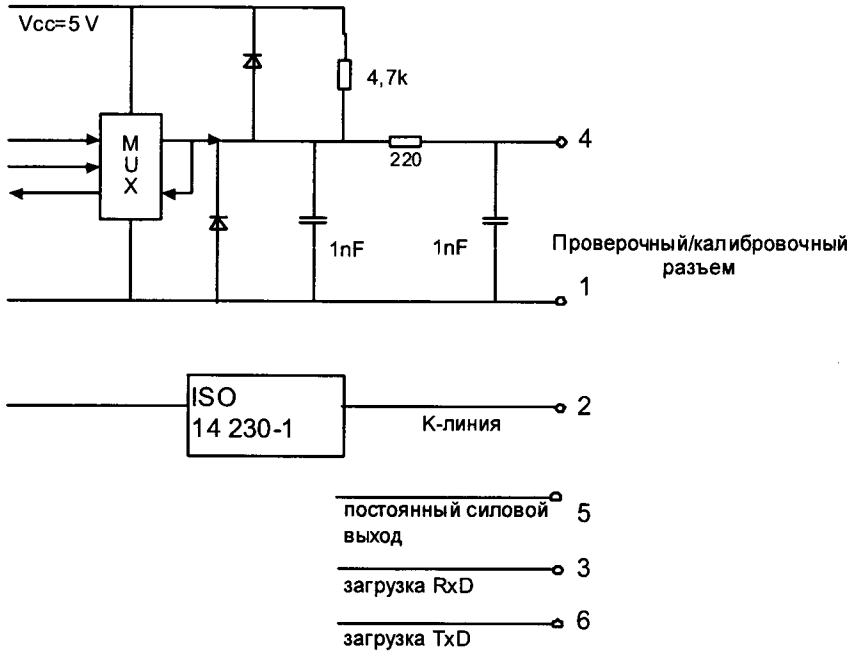
1.2 Разводка контактов

INT_002 Разводка контактов указана в таблице ниже.

Контакт	Назначение	Примечания
1	Отрицательный полюс источника питания	Соединяется с отрицательным полюсом бортовой аккумуляторной батареи
2	Передача данных	K-линия (ISO 14230-1)
3	RxD – Загрузка данных	Ввод данных в контрольное устройство
4	Входной/выходной сигнал	Калибровка
5	Постоянный силовой выход	Номинальный диапазон напряжений равен напряжению бортовой сети питания минус 3 В с учетом падения напряжения на предохранительных цепях Выход 40 мА
6	TxD – Загрузка данных	Вывод данных из контрольного устройства

1.3 Блок-схема

INT_003 Блок-схема должна соответствовать приведенной ниже.



2. Интерфейс загрузки данных

INT_004 Интерфейс загрузки данных должен соответствовать спецификациям RS232.

INT_005 Порядок загрузки данных через интерфейс: один стартовый бит, 8 битов данных начиная с младшего бита, один бит контроля по четности, один стоп-бит.

Структура байта данных

Стартовый бит:	один бит с уровнем логического нуля;
Биты данных:	бит младшего разряда передается первым;
Бит контроля по четности:	положительная четность;
Стоп-бит:	один бит с уровнем логической единицы.

При передаче числовых данных объемом больше одного байта байт старшего разряда передается первым, байт младшего разряда – последним.

INT_006 Скорость передачи данных должна быть регулируемой в диапазоне от 9 600 бит/с до 115 200 бит/с. При инициализации обмена данными задается начальная скорость передачи 9 600 бит/с; затем скорость доводится до максимальной возможной величины.

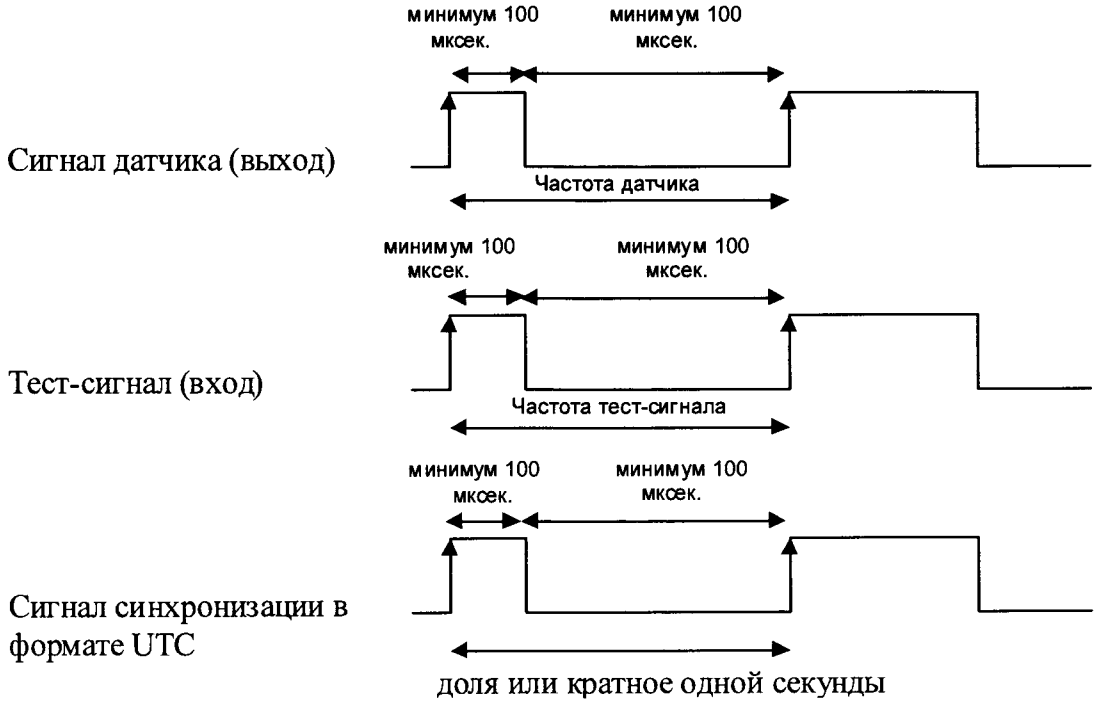
3. Интерфейс калибровки

INT_007 Обмен данных осуществляется в соответствии со стандартом ISO 14230-1 (Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 1. Физический уровень. Издание первое, 1999 год).

INT_008 Электрические характеристики входного/выходного сигнала должны соответствовать указанным ниже.

Параметр	Минимум	Норма	Максимум	Примечание
$U_{ниж}$ (вход)			1,0 В	I = 750 мкА
$U_{верх}$ (вход)	4 В			I = 200 мкА
Частота			4 кГц	
$U_{ниж}$ (выход)			1,0 В	I = 1 мА
$U_{верх}$ (выход)	4 В			I = 1 мА

INT_009 Временные диаграммы входного/выходного сигнала приводятся ниже:



ПОДРАЗДЕЛ VII

ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

1. Введение

В настоящем подразделе изложены процедуры различных вариантов загрузки данных на внешний носитель (ВН), а также протоколы, применение которых необходимо для правильной передачи данных и для обеспечения универсальной совместимости формата, в котором они загружаются, с тем чтобы любой контролер имел возможность ознакомиться с этими данными и перед началом их анализа убедиться в их подлинности и достоверности.

1.1 Сфера применения

На ВН могут загружаться данные:

- из бортового устройства при помощи подключенной к БУ специализированной программируемой аппаратуры (СПА),
- с карточки тахографа при помощи СПА, оснащенной устройством считывания карточек (УСК),
- с карточки тахографа через бортовое устройство путем подключения СПА к БУ.

Для целей контроля подлинности и целостности данных, сохраняемых на ВН, при загрузке они снабжаются подписью в соответствии с указанным в подразделе XI ("Общие механизмы защиты"). В состав загружаемой информации включаются идентификационные данные аппаратного источника (БУ или карточки) и соответствующие ему сертификаты безопасности (Договаривающейся стороны и аппаратуры). Лицо, осуществляющее проверку данных, должно иметь собственный открытый криптографический ключ от надежного европейского поставщика.

DDP_001 Данные, загруженные за один сеанс загрузки, должны сохраняться на ВН в виде одного файла.

1.2 Сокращения и обозначения

В настоящем подразделе используются следующие сокращения:

AID (ИП) Идентификатор приложений
ATR Ответ на сигнал перезагрузки
CS Байт контрольной суммы
DF Каталог

DS_	Диагностический сеанс
EF	Элементарный файл
ESM	(ВН) Внешний носитель
FID	(ID файла) Идентификатор файла
FMT	Байт формата (первый байт в заголовке сообщения)
Hex	Шестнадцатеричное значение
ICC	(МПК) Микропроцессорная карточка
IDE	(СПА) Специализированная программируемая аппаратура: аппаратура, используемая для загрузки данных на ВН (например, персональный компьютер)
IFD	(УСК) Устройство считывания карточек (интерфейс)
KWP	Протокол ключевых слов 2000
LEN	Байт длины (последний байт в заголовке сообщения)
PPS	(ВПП) Выбор параметров протокола
PSO	Выполнение защитной операции
SID	Идентификатор функции
SRC	Байт адреса источника
TGT	Байт адреса приемника
TLV	Метка-длина-значение
TREP	Параметр ответа на запрос передачи
TRTP	Параметр запроса передачи
VU	(БУ) Бортовое устройство

2. Загрузка данных из БУ

2.1 Процедура загрузки

Для загрузки данных из БУ оператору необходимо выполнить следующие действия:

- ввести свою карточку тахографа в считывающее устройство БУ(*);
- подсоединить СПА к выходному разъему БУ;
- установить канал связи между СПА и БУ;
- с помощью СПА выбрать данные для загрузки и передать запрос в БУ;
- завершить сеанс загрузки.

*) Ввод карточки инициирует подтверждение соответствующих прав доступа к функции загрузки и загружаемым данным.

2.2 Протокол загрузки данных

Протокол построен по принципу "ведущий-ведомый", при котором в роли ведущего выступает СПА, а в роли ведомого – БУ.

Структура, типы и поток сообщений в основном соответствуют протоколу ключевых слов KWP 2000 (ISO 14230-2 Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 2. Уровень обмена данными).

Уровень приложений в основном соответствует нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции. Версия 6 от 22 февраля 2001 года).

2.2.1 Структура сообщений

DDP_002 Все сообщения, которыми обмениваются СПА и БУ, форматируются в соответствии с трехкомпонентной структурой:

- заголовок, состоящий из байта формата (FMT), байта адреса приемника (TGT), байта адреса источника (SRC) и в некоторых случаях также байта длины сообщения (LEN);

- поле данных, образуемое байтом идентификатора функции (SID) и переменным числом байтов данных, включая необязательный байт диагностического сеанса (DS_) и необязательный байт параметра передачи (TRTP или TREP);

- контрольная сумма, определяемая байтом контрольной суммы (CS).

Заголовок				Поле данных					Контрольная сумма
FMT	TGT	SRC	LEN	SID	DATA	……	…..	…..	CS
4 байта				до 255 байт					1 байт

Байты TGT и SRC указывают физические адреса получателя и отправителя сообщения. Их значения – F0 Hex для СПА и EE Hex для БУ.

Байт LEN представляет собой длину поля данных в сообщении.

Байт контрольной суммы представляет собой 8-битную сумму по модулю 256 всех байт сообщения, за исключением самой контрольной суммы.

Определения байтов FMT, SID, DS_, TRTP и TREP приводятся далее в настоящем документе.

DDP_003 Если объем передаваемых в сообщении данных превышает длину поля данных, то сообщение фактически высылается в виде нескольких подсообщений. Каждое подсообщение содержит заголовок, одни и те же байты SID и TREP, а также 2-байтовый счетчик подсообщений, указывающий порядковый номер данного подсообщения в общем сообщении. Чтобы обеспечить возможность обнаружения ошибок и отмены передачи, СПА подтверждает получение каждого подсообщения. СПА может принять подсообщение, запросить его повторную передачу, выдать БУ команду начать передачу заново или отменить ее.

DDP_004 Если поле данных последнего подсообщения содержит ровно 255 байт, то к нему должно добавляться заключительное подсообщение с пустым (то есть содержащим только SID, TREP и счетчик подсообщений) полем данных, означающее конец сообщения.

Пример:

Заголовок	SID	TREP	Сообщение	CS
4 байта	Более 255 байт			

Передается как

Заголовок	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байт					
Заголовок	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байт					

...

Заголовок	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	Менее 255 байт					

или как:

Заголовок	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байт					

Заголовок	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байт					

...

Заголовок	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	255 байт					

Заголовок	SID	TREP	xx	yy+1	CS
4 байта	4 байта				

2.2.2 Типы сообщений

Протокол загрузки данных для БУ и СПА предусматривает обязательный обмен сообщениями восьми типов.

Общая характеристика этих сообщений представлена в таблице ниже.

Структура сообщения	До 4 байт Заголовок				До 255 байт Данные			1 байт Контр. сумма
СПА -> <- БУ	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	ДАННЫЕ	CS
Запрос инициализации обмена данными	81	EE	F0		81			E0
Положит. ответ: инициализ. обмена данными	80	F0	EE	03	C1		'EA' '8F'	9B
Запрос инициализ. диагност. сеанса	80	EE	F0	02	10	81		F1
Положит. ответ: инициализ. диагност. сеанса	80	F0	EE	02	50	81		31
Функция регулировки канала обмена данными								
Проверка скорости передачи данных (этап 1)								
9 600 бод	80	EE	F0	04	87		01,01,01	EC
19 200 бод	80	EE	F0	04	87		01,01,02	ED
38 400 бод	80	EE	F0	04	87		01,01,03	EE
57 600 бод	80	EE	F0	04	87		01,01,04	EF
115 200 бод	80	EE	F0	04	87		01,01,05	F0
Положит. ответ: проверка скорости передачи	80	F0	EE	02	C7		01	28
Переходная скорость передачи (этап 2)	80	EE	F0	03	87		02,03	ED
Запрос загрузки	80	EE	F0	0A	35		00,00,00,00 ,00,FF,FF, FF,FF	99
Положит. ответ: запрос загрузки	80	F0	EE	03	75		00,FF	D5
Запрос передачи данных								
Обзор	80	EE	F0	02	36	01		97
Деятельность	80	EE	F0	06	36	02	Дата	CS

События и отказы	80	EE	F0	02	36	03		99
Подробные данные о скоростном режиме	80	EE	F0	02	36	04		9A
Технические данные	80	EE	F0	02	36	05		9B
Загрузка с карточки	80	EE	F0	02	36	06		9C
Положит. ответ: передача данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос завершения передачи	80	EE	F0	01	37			96
Положит. ответ: завершение передачи	80	F0	EE	01	77			D6
Запрос завершения обмена данными	80	EE	F0	01	82			E1
Положит. ответ: завершение обмена данными	80	F0	EE	01	C2			21
Подтверждение приема подсообщения	80	EE	F0	Len	83		Данные	CS
Отрицательные ответы								
Общий отрицательный результат	80	F0	EE	03	7F	Sid Req	10	CS
Функция не поддерживается	80	F0	EE	03	7F	Sid Req	11	CS
Подфункция не поддерживается	80	F0	EE	03	7F	Sid Req	12	CS
Неверная длина сообщения	80	F0	EE	03	7F	Sid Req	13	CS
Недопустимые условия или ошибка очередн.	80	F0	EE	03	7F	Sid Req	22	CS
Нештатный запрос	80	F0	EE	03	7F	Sid Req	31	CS
Отказ в приеме загружаемых данных	80	F0	EE	03	7F	Sid Req	50	CS
Ожидается ответ	80	F0	EE	03	7F	Sid Req	78	CS
Данные отсутствуют	80	F0	EE	03	7F	Sid Req	FA	CS

Примечания:

- Sid Req = Sid соответствующего запроса.
- TREP = TRTP соответствующего запроса.
- Темный фон ячейки в таблице означает отсутствие передачи данных.
- Термин "upload" (загрузка со стороны СПА) используется для целей совместимости с ISO 14229. Он имеет тот же смысл, что и термин "download" (загрузка со стороны БУ).
- 2-байтные счетчики подсообщений, которые могут содержаться в сообщениях, в таблице не показаны.

2.2.2.1 Start Communication Request – Запрос инициализации обмена данными (SID 81)

DDP_005 Данное сообщение высылается СПА для установления канала обмена данными с БУ. Начальная скорость передачи данных во всех случаях составляет 9600 бод (до тех пор, пока она не будет изменена при помощи соответствующих функций управления передачей данных).

2.2.2.2 Positive Response Start Communication – Положительный ответ: инициализация обмена данными (SID C1)

DDP_006 Данное сообщение высылается БУ в качестве положительного ответа на запрос инициализации обмена данными. Оно включает два байта ключей – ‘EA’ и ‘8F’,

указывающие на поддержку данного протокола устройством, и заголовок с информацией о получателе, источнике и длине сообщения.

2.2.2.3 Start Diagnostic Session Request – Запрос инициализации диагностического сеанса (SID 10)

DDP_007 Сообщение с запросом инициализации диагностического сеанса высылается СПА, чтобы начать новый сеанс обмена диагностическими данными с БУ. Подфункция "default session" (сеанс по умолчанию) (81 Hex) указывает на то, что будет начат стандартный диагностический сеанс.

2.2.2.4 Positive Response Start Diagnostic – Положительный ответ: инициализация диагностики (SID 50)

DDP_008 Сообщение с положительным ответом на запрос инициализации диагностики высылает БУ, чтобы подтвердить начало диагностического сеанса.

2.2.2.5 Link Control Service – Функция регулировки канала обмена данными (SID 87)

DDP_052 Функция регулировки канала обмена данными используется СПА для того, чтобы инициировать изменение скорости передачи данных. Это происходит в два этапа. На первом этапе СПА предлагает изменение скорости передачи, указывая новую скорость. По получении от БУ положительного ответа СПА высылает БУ подтверждение изменения скорости (второй этап). Затем СПА переключается на новую скорость передачи данных. Получив подтверждение, БУ также переключается на новую скорость передачи.

2.2.2.6 Link Control Positive Response – Регулировка канала обмена данными: положительный ответ (SID C7)

DDP_053 Это сообщение высылается БУ в качестве положительного ответа на запрос регулировки канала обмена данными (первый этап). Следует обратить внимание на то, что ответ на запрос подтверждения не высылается (второй этап).

2.2.2.7 Request Upload – Запрос загрузки (SID 35)

DDP_009 Сообщение с запросом загрузки высылается СПА с целью указать БУ на необходимость загрузить данные. В соответствии с требованиями ISO 14229 в него должна включаться информация об адресе, объеме и формате запрашиваемых данных. Поскольку до загрузки данных СПА такой информацией не располагает,

адрес ячейки памяти при этом устанавливается на 0, формат указывается как нешифрованный и без сжатия, а объем памяти задается максимальным.

2.2.2.8 Positive Response Request Upload – Положительный ответ на запрос загрузки (SID 75)

DDP_010 Сообщение с положительным ответом на запрос загрузки высылается БУс целью указать СПА на готовность БУ к загрузке данных. В соответствии с требованиями ISO 14229 в это сообщение включаются данные, указывающие СПА о том, что последующие положительные ответы на запросы передачи данных будут содержать максимум 00FF Hex байт.

2.2.2.9 Transfer Data Request – Запрос передачи данных (SID 36)

DDP_011 Запрос передачи данных высылается СПА с целью указать БУ тип данных, которые должны быть загружены. Тип данных указывается однобайтовым параметром запроса передачи (TRTP).

Возможна передача шести типов данных:

- Обзор (TRTP 01),
- Деятельность на указанную дату (TRTP 02),
- События и неисправности (TRTP 03),
- Подробные данные о скоростном режиме (TRTP 04),
- Технические данные (TRTP 05),
- Загрузка с карточки (TRTP 06).

DDP_054 В ходе сеанса загрузки СПА в обязательном порядке запрашивает передачу обзорных данных (TRTP 01), так как только при этом в загружаемом файле регистрируются сертификаты БУ (что создает возможность проверки цифровой подписи).

Во втором случае (TRTP 02) сообщение с запросом передачи данных включает указание календарной даты (в формате реального времени), данные за которую подлежат загрузке.

2.2.2.10 Positive Response Transfer Data – Положительный ответ на запрос передачи данных (SID 76)

DDP_012 Положительный ответ на запрос передачи данных высылается БУ по получении запроса передачи данных. Это сообщение содержит запрошенные данные и параметр ответа на запрос передачи (TREP), который соответствует TRTP запроса.

DDP055 В первом случае (TREP 01) БУ высылает данные, помогающие оператору СПА выбрать информацию, загрузку которой он желает продолжить. Сообщение содержит данные о:

- сертификатах безопасности;
- идентификации транспортного средства;
- текущей дате и времени по хронометражу БУ;
- самой ранней и самой поздней дате, данные за которую могут быть загружены из БУ;
- наличии карточек в считывающих устройствах БУ;
- предыдущей загрузке данных представителем предприятия;
- блокировках, установленных предприятием;
- предыдущих проверках.

2.2.2.11 Request Transfer Exit – Запрос завершения передачи (SID 37)

DDP_013 Сообщение с запросом завершения передачи высылается СПА с целью указать БУ на завершение сеанса загрузки.

2.2.2.12 Positive Response Request Transfer Exit – Положительный ответ на запрос завершения передачи (SID 77)

DDP_014 Сообщение с положительным ответом на запрос завершения передачи высылает БУ с целью подтвердить прием запроса завершения передачи.

2.2.2.13 Stop Communication Request – Запрос завершения обмена данными (SID 82)

DDP_015 Сообщение с запросом завершения обмена данными высылается СПА с целью закрыть канал обмена данными с БУ.

2.2.2.14 Positive Response Stop Communication – Положительный ответ на запрос на завершение обмена данными (SID C2)

DDP_016 Сообщение с положительным ответом на запрос завершения обмена данными высылается БУ с целью подтвердить прием запроса завершения обмена данными.

2.2.2.15 Acknowledge Sub Message – Подтверждение приема подсообщения (SID 83)

DDP_017 Подтверждение приема подсообщения высылается СПА, подтверждая этим получение каждой части сообщения, передаваемого в виде ряда подсообщений. Поле данных содержит SID, полученный от БУ, и двухбайтовый код со следующими возможными значениями:

- MsgC +1 – подтверждение правильного приема подсообщения номер MsgC. Запрос от СПА к БУ на отправку следующего подсообщения;

MsgC – указание на сбой при приеме подсообщения номер MsgC.
Запрос от СПА к БУ на повторную отправку данного подсообщения;

FFFF – запрос прекращения передачи сообщения.
Эта функция может использоваться СПА для прекращения по каким-либо причинам передачи сообщения от БУ.

Прием последнего подсообщения в сообщении (LEN < 255 байт) может подтверждаться любым из вышеуказанных кодов или оставаться без подтверждения.

К ответам БУ, которые состоят из нескольких подсообщений, относятся:
- положительный ответ на запрос передачи данных (SID 76).

2.2.2.16 Отрицательный ответ (SID 7F)

DDP_018 Сообщение с отрицательным ответом на те или иные из перечисленных выше запросов БУ высылает в тех случаях, когда запрос не может быть выполнен. Поле данных сообщения содержит SID ответа (7F), SID запроса и код, указывающий причину отрицательного ответа. Могут использоваться следующие коды:

- 10 Общее отклонение запроса
  Действие не может быть выполнено по причине, не входящей в число нижеперечисленных;

- 11 Функция не поддерживается
  Не опознан SID запроса;

- 12 Подфункция не поддерживается
  Не опознан DS_ или TRTP запроса либо отсутствуют другие подсообщения для передачи;

- 13 Неверная длина сообщения
  Получено сообщение неверной длины;

- 22 Недопустимые условия или ошибка очередности запросов
  Требуемая функция не активирована либо неверная очередность запросов;

- 31 Нештатный запрос
  Значение параметра запроса (поле данных) недействительно;

- 50 Отказ в приеме загружаемых данных
  Невозможно выполнить запрос (несоответствие режима работы БУ или внутренние неполадки в БУ);

- 78 Ожидается ответ
  Запрошенная операция не может быть завершена своевременно; БУ не готов к приему нового запроса;

- FA Данные отсутствуют
  Запрошенный к передаче объект данных отсутствует в БУ (например, не введена карточка, и т.п.).

2.2.3 Поток сообщений

При нормальной загрузке данных поток сообщений, как правило, выглядит следующим образом:

СПА		**БУ**
Запрос инициализации обмена данными	⇨	
	⇦	Положительный ответ
Запрос инициализации диагностического сеанса	⇨	
	⇦	Положительный ответ
Запрос загрузки	⇨	
	⇦	Положительный ответ
Запрос передачи обзорных данных	⇨	
	⇦	Положительный ответ

Запрос передачи данных #2	⇨	
	⇦	Положительный ответ #1
Подтверждение приема подсообщения #1	⇨	
	⇦	Положительный ответ #2
Подтверждение приема подсообщения #2	⇨	
	⇦	Положительный ответ #m
Подтверждение приема подсообщения #m	⇨	
	⇦	Положительный ответ (поле данных <255 байт)
Подтверждение приема подсообщения (не обязательно)	⇨	
…		
Запрос передачи данных #n	⇨	
	⇦	Положительный ответ
Запрос завершения передачи	⇨	
	⇦	Положительный ответ
Запрос завершения обмена данными	⇨	
	⇦	Положительный ответ

2.2.4 Временные параметры

DDP_019 Временные параметры для нормального режима работы указаны в таблице ниже:

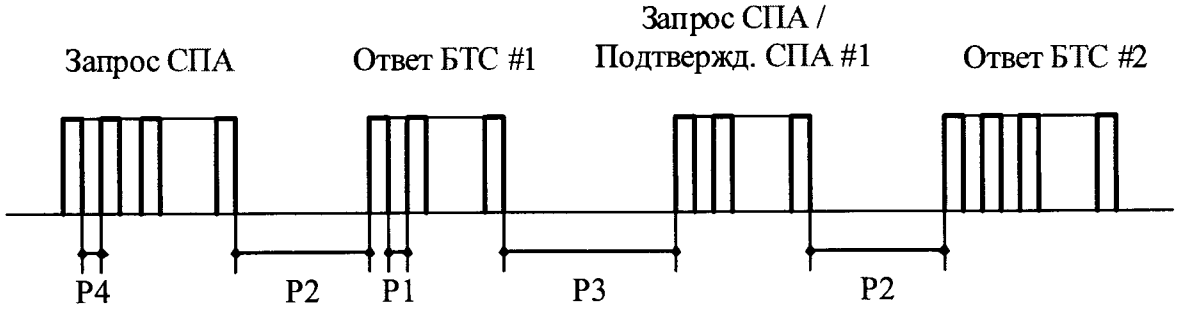


Рис. 1
Поток сообщений и временные параметры

Где:

P1 = Межбайтовый интервал для ответа БУ.

P2 = Время между окончанием запроса СПА и началом ответа БУ или между окончанием подтверждения СПА и началом следующего ответа БУ.

P3 = Время между окончанием ответа БУ и началом нового запроса СПА или между окончанием ответа БУ и началом подтверждения СПА, или между окончанием запроса СПА и началом нового запроса СПА при отсутствии ответа от БУ.

P4 = Межбайтовый интервал для запроса СПА.

P5 = Увеличенное значение P3 для загрузки данных с карточек.

Допустимые значения временных параметров приводятся в нижеследующей таблице (расширенный диапазон временных параметров протокола KWP для использования при физической адресации в целях ускорения передачи данных).

Временной параметр	Нижнее предельное значение (мс)	Верхнее предельное значение (мс)
P1	0	20
P2	20	1000 *)
P3	10	5000
P4	5	20
P5	10	20 минут

*) если БУ выдает отрицательный ответ с кодом, означающим "запрос получен правильно – ожидается ответ", то это значение увеличивается до соответствующего верхнего предельного значения P3.

2.2.5 Обработка ошибок

При возникновении ошибки в процессе обмена сообщениями схема потока сообщений модифицируется в зависимости от того, каким из приборов обнаружена ошибка и каким сообщением она вызвана.

На рис. 2 и рис. 3 показаны процедуры обработки ошибок, соответственно, для БУ и для СПА.

2.2.5.1 Стадия инициализации обмена данными

DDP_020 Если СПА обнаруживает ошибку синхронизации или ошибку в битовом потоке на стадии инициализации обмена данными, то период ожидания СПА перед повторением запроса равняется P3 min.

DDP_021 Если БУ обнаруживает ошибку в очередности сообщений от СПА, то оно не высылает ответа и ожидает нового сообщения с запросом инициализации обмена данными в течение периода, равного P3 max.

2.2.5.2 Стадия обмена данными

На этой стадии можно выделить два типовых случая обработки ошибок:

БУ обнаруживает ошибку в передаче данных от СПА

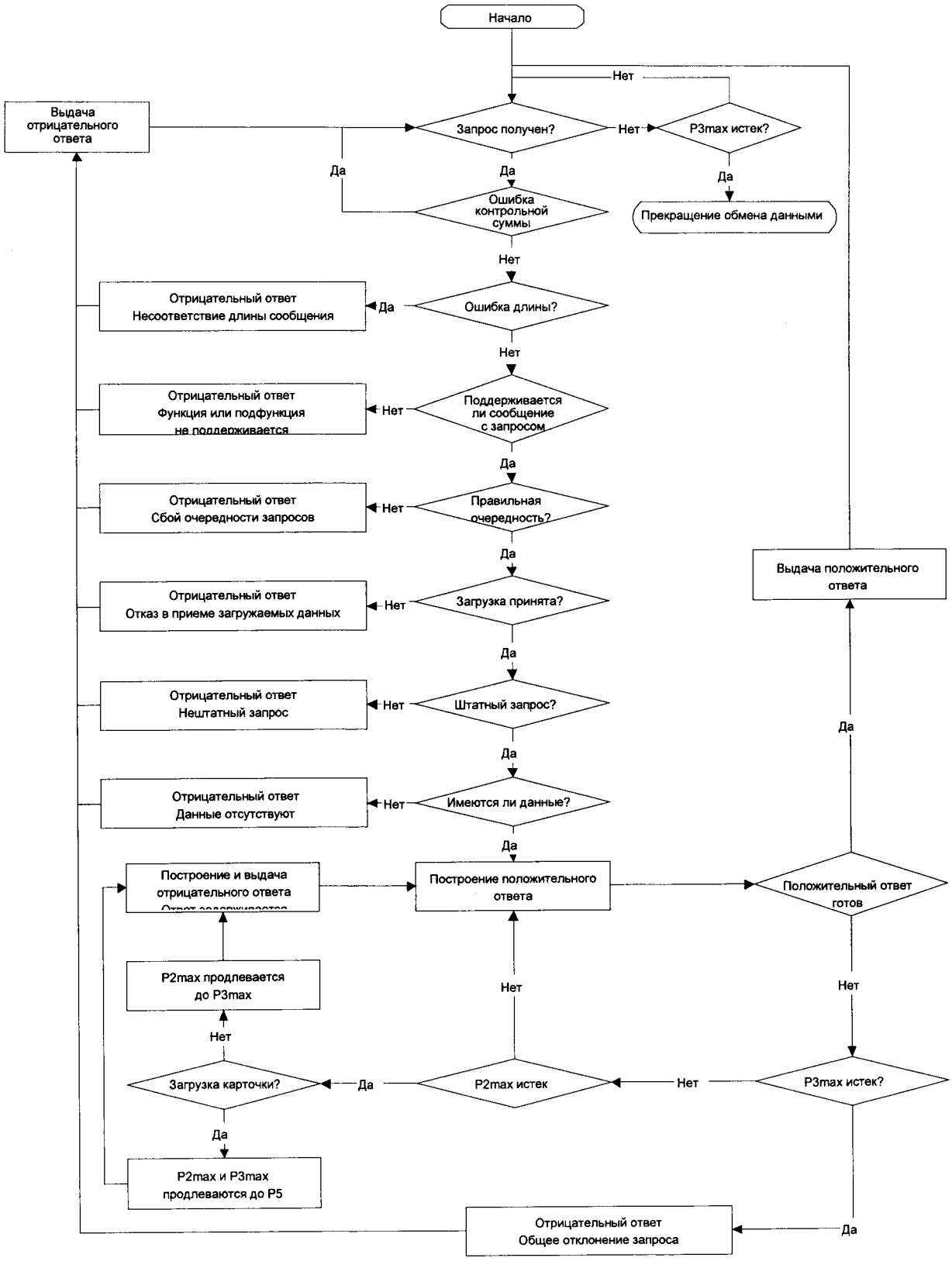
DDP_022 БУ проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки передачи кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).

DDP_023 При обнаружении одной из вышеназванных ошибок БУ не высылает ответа и игнорирует поступившее сообщение.

DDP_024 БУ может обнаружить и другие ошибки в формате или содержании полученного сообщения (например, "сообщение не поддерживается"), даже если оно соответствует требованиям по длине и контрольной сумме; в этом случае БУ высылает СПА отрицательный ответ с указанием характера ошибки.

Рис. 2

Обработка ошибок: БТС



2. СПА обнаруживает ошибку в передаче данных от БУ

DDP_025 СПА проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки в передаче кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).

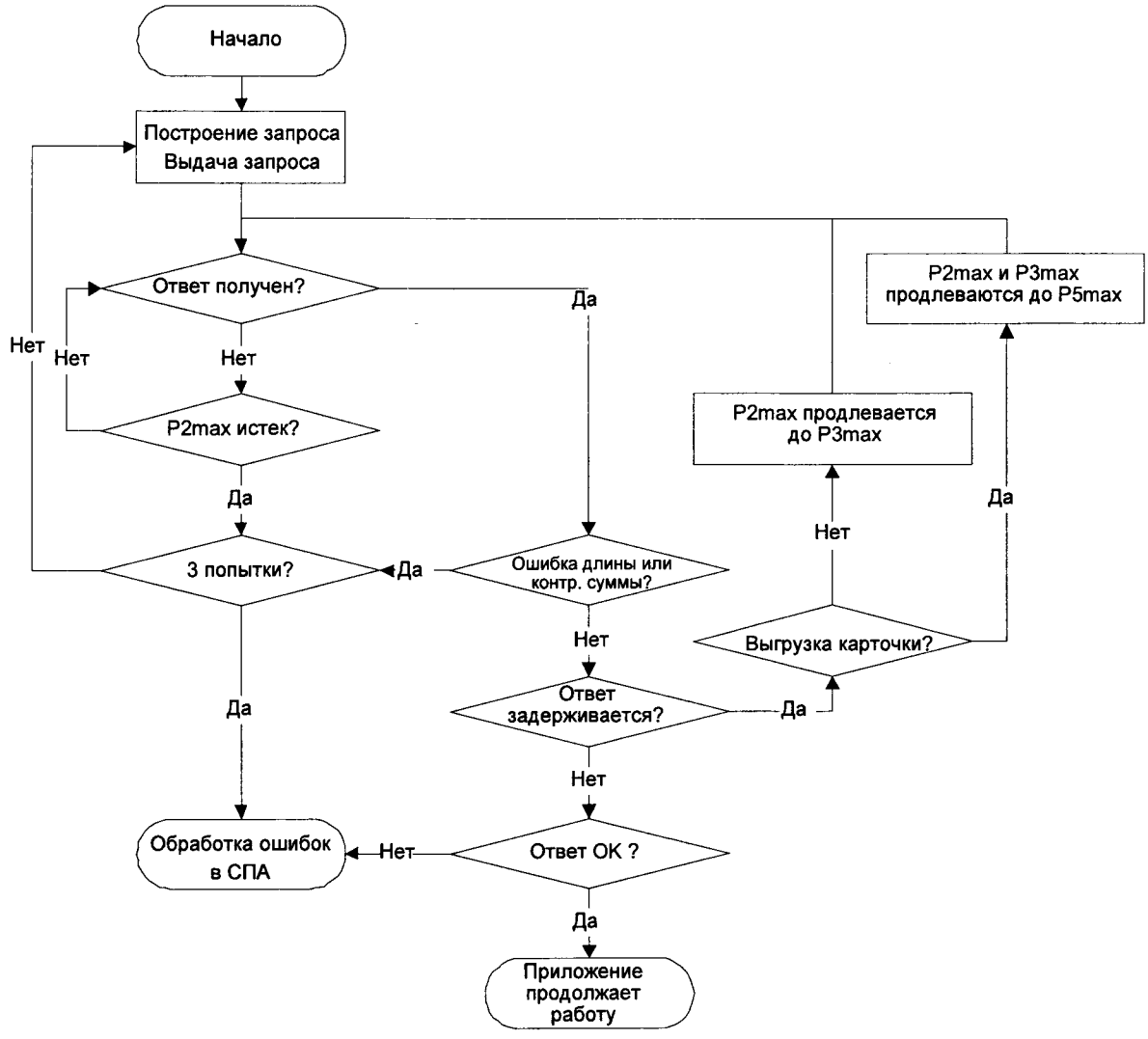
DDP_026 СПА проверяет поступающие сообщения на ошибки очередности, такие как сбои возрастания порядковых номеров подсообщений в последовательно поступающих сообщениях.

DDP_027 Если СПА обнаруживает ошибку или не получает от БУ ответа в течение периода, равного P2max, то запрос высылается повторно, причем общее число передач ограничивается тремя. Для случаев обнаружения ошибок данного вида подтверждение приема подсообщения рассматривается как запрос к БУ.

DDP_028 Период ожидания СПА перед началом каждой передачи равняется или превышает P3min; этот период отсчитывается с расчетного момента приема последнего стопового бита после обнаруженной ошибки.

Рис. 3

Обработка ошибок: СПА



2.2.6 Содержание ответного сообщения

В данном пункте указано содержание полей данных различных сообщений с положительным ответом.

Определения элементов данных приводятся в подразделе I (словарь данных).

2.2.6.1 *Positive Response Transfer Data Overview – Положительный ответ на запрос передачи обзорных данных*

DDP_029 В поле данных сообщения "Положительный ответ на запрос передачи обзорных данных" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 01 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
MemberStateCertificate	194	Сертификаты защиты БУ
VUCertificate	194	
VehicleIdentificationNumber	17	Идентификационные данные транспортного средства
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Текущая дата и время согласно хронометражу БУ
VuDownloadablePeriod		Период, за который могут быть загружены данные
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Типы карточек, введенных в считывающее устройство БУ
VuDownloadActivityData		Предыдущая загрузка данных из БУ
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Все сохраненные блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0.
noOfLocks	1	
...	(98)	
БУ Company Locks Record: lockInTime	4	
БУ Company Locks Record: lockOutTime	4	
БУ Company Locks Record: companyName	36	
БУ Company Locks Record: companyAddress	36	
БУ Company Locks Record: companyCardNumber	18	
...		
VuControlActivityData		Все сохраненные в БУ контрольные записи. Если раздел не заполнен, высылается только noOfControls = 0.
noOfControls	1	
...	(31)	
БУ Control Activity Record: controlType	1	
БУ Control Activity Record: controlTime	4	
БУ Control Activity Record: controlCardNumber	18	
БУ Control Activity Record: downloadPeriodBeginTime	4	
БУ Control Activity Record: downloadPeriodEndTime	4	
...		

Подпись	128	Подпись криптосистемы RSA для всех данных (кроме сертификатов), от VehicleIdentificationNumber до последнего байта последней VuControlActivityRecord.

2.2.6.2 Positive Response Transfer Data Activities – Положительный ответ на запрос передачи данных о деятельности водителей

DDP_030 В поле данных сообщения "Положительный ответ на запрос передачи данных о деятельности водителей" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 02 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
TimeReal	4	Дата загрузки
OdometerValueMidnight	3	Показания счетчика пробега на конец суток, к которым относятся загружаемые данные.
VuCardIWData		Информация о циклах ввода/извлечения карточек. – Если в разделе нет данных, высылается только noOfVuCardIWRecords = 0. – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объеме включается в данные за оба дня.
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord: cardHolderName		
VuCardIWRecord: holderSurname	36	
VuCardIWRecord: holderFirstNames	36	
VuCardIWRecord: fullCardNumber	18	
VuCardIWRecord: cardExpiryDate	4	
VuCardIWRecord: cardInsertionTime	4	
VuCardIWRecord: vehicleOdometerValueAtInsertion	3	
VuCardIWRecord: cardSlotNumber	1	
VuCardIWRecord: cardWithdrawalTime	4	
VuCardIWRecord: vehicleOdometerValueAtWithdrawal	3	
VuCardIWRecord: previousVehicleInfo		
VuCardIWRecord: vehicleRegistrationIdentification		
VuCardIWRecord: vehicleRegistrationNation	1	
VuCardIWRecord: vehicleRegistrationNumber	14	
VuCardIWRecord: cardWithdrawalTime	4	
VuCardIWRecord: manualInputFlag	1	
...		
VuActivityDailyData		Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord: fullCardNumber	18	
VuPlaceDailyWorkPeriodRecord: placeRecord		
VuPlaceDailyWorkPeriodRecord: entryTime	4	
VuPlaceDailyWorkPeriodRecord: entryTypeDailyWorkPeriod	1	
VuPlaceDailyWorkPeriodRecord: dailyWorkPeriodCountry	1	
VuPlaceDailyWorkPeriodRecord: dailyWorkPeriodRegion	1	
VuPlaceDailyWorkPeriodRecord: vehicleOdometerValue	3	
...		

VuSpecificConditionData		Информация об особых ситуациях, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfSpecificConditionRecords=0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
entryTime	4	
specificConditionType	1	
...		
Подпись	128	Подпись криптосистемы RSA для всех данных, от TimeReal до последнего байта последней записи об особых ситуациях.

2.2.6.3 Positive Response Transfer Data Events and Faults – Положительный ответ на запрос передачи данных о событиях и неисправностях

DDP_031 В поле данных сообщения "Положительный ответ на запрос передачи данных о событиях и неисправностях" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 03 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
VuFaultData		Вся сохраненная в БУ и текущая информация о неисправностях. Если раздел не заполнен, высылается только noOfVuFaults = 0.
noOfVuFaults	1	
...	(82)	
VuFaultRecord: faultType	1	
VuFaultRecord: faultRecordPurpose	1	
VuFaultRecord: faultBeginTime	4	
VuFaultRecord: faultEndTime	4	
VuFaultRecord: cardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: cardNumberDriverSlotEnd	18	
VuFaultRecord: cardNumberCodriverSlotEnd	18	
...		
VuEventData		Вся сохраненная в БУ и текущая информация о событиях (кроме превышений скорости). Если раздел не заполнен, высылается только noOfVuEvents = 0.
noOfVuEvents	1	
...	(83)	
ntReco: eventType	1	
ntReco: eventRecordPurpose	1	
ntReco: eventBeginTime	4	

	eventEndTime	4	
	cardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	cardNumberDriverSlotEnd	18	
	cardNumberCodriverSlotEnd	18	
	similarEventsNumber	1	
...			

VuOverSpeedingControlData			Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).
lastOverspeedControlTime		4	
firstOverspeedSince		4	
numberOfOverspeedSince		1	
VuOverSpeedingEventData			Вся сохраненная в БУ и текущая информация о превышениях скорости. Если раздел не заполнен, высылается только noOfVuOverSpeedingEvents = 0.
noOfVuOverSpeedingEvents		1	
...		(31)	
VuOverSpeedingEventRecord	eventType	1	
	eventRecordPurpose	1	
	eventBeginTime	4	
	eventEndTime	4	
	maxSpeedValue	1	
	averageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	similarEventsNumber	1	
...			
VuTimeAdjustmentData			Вся сохраненная в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки). Если раздел не заполнен, высылается только noOfVuTimeAdjRecords = 0.
noOfVuTimeAdjRecords		1	
...		(98)	
VuTimeAdjustmentRecord	oldTimeValue	4	
	newTimeValue	4	
	workshopName	36	
	workshopAddress	36	
	workshopCardNumber	18	
...			
Подпись		128	Подпись криптосистемы RSA для всех данных, от noOfVuFaults до последнего байта последней записи о корректировках времени.

2.2.6.4 Positive Response Transfer Data Detailed Speed – Положительный ответ на запрос передачи подробных данных о скоростном режиме

DDP_032 В поле данных сообщения "Положительный ответ на запрос передачи подробных данных о скоростном режиме" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 04 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
VuDetailedSpeedData		Вся сохраненная в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства); 60 значений скорости в минуту (по одному в секунду).
noOfSpeedBlocks	2	
...		
VuDeatailedSpeedBlock: speedBlockBeginDate	4	
VuDeatailedSpeedBlock: speedsPerSecond	60	
...		
Подпись	128	Подпись криптосистемы RSA для всех данных, от noOfSpeedBlocks до последнего байта последнего блока данных о скорости.

2.2.6.5 Positive Response Transfer Data Technical Data – Положительный ответ на запрос передачи технических данных

DDP_033 В поле данных сообщения "Положительный ответ на запрос передачи технических данных" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 05 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Все сохраненные в БУ калибровочные записи.
noOfVuCalibrationRecords	1	
...	(167)	
VuCalibrationRecord: calibrationPurpose	1	
VuCalibrationRecord: workshopName	36	
VuCalibrationRecord: workshopAddress	36	
VuCalibrationRecord: workshopCardNumber	18	
VuCalibrationRecord: workshopCardExpiryDate	4	
VuCalibrationRecord: vehicleIdentificationNumber	17	
VuCalibrationRecord: vehicleRegistrationIdentification		
VuCalibrationRecord: vehicleRegistrationNation	1	
VuCalibrationRecord: vehicleRegistrationNumber	14	
VuCalibrationRecord: wVehicleCharacteristicConstant	2	
VuCalibrationRecord: kConstantOfRecordingEquipment	2	
VuCalibrationRecord: lTyreCircumference	2	
VuCalibrationRecord: tyreSize	15	
VuCalibrationRecord: authorisedSpeed	1	
VuCalibrationRecord: oldOdometerValue	3	
VuCalibrationRecord: newOdometerValue	3	
VuCalibrationRecord: oldTimeValue	4	
VuCalibrationRecord: newTimeValue	4	
VuCalibrationRecord: nextCalibrationDate	4	
...		
Подпись	128	Подпись криптосистемы RSA для всех данных, от vuManufacturerName до последнего байта последней VuCalibrationRecord.

2.3 Сохранение данных на ВН

DDP_034 В случаях, когда сеанс загрузки данных включает передачу данных с БУ, СПА сохраняет в виде одного физического файла все данные, полученные от БУ в ходе сеанса загрузки в сообщениях типа "Положительный ответ на запрос передачи данных". Сохраняемые данные не включают заголовки сообщений, счетчики подсообщений, пустые подсообщения и контрольные суммы, но включают SID и TREP (при наличии нескольких подсообщений – только для первого подсообщения).

3. Протокол загрузки данных с карточек тахографа

3.1 Сфера применения

В настоящем пункте изложен порядок прямой загрузки данных с карточки тахографа на СПА. СПА не является частью защищенной среды; поэтому процедура аутентификации между карточкой и СПА не предусмотрена.

3.2 Определения

Сеанс загрузки: Каждая загрузка данных с МПК. Сеанс включает всю процедуру, от перезапуска карточки считывающим устройством до дезактивации МПК (т.е. извлечения или новой перезагрузки карточки).

Подписанный файл данных: Файл, полученный с МПК. Файл передается на УСК в текстовой форме. В МПК файл хешируется и подписывается; подпись высылается на УСК.

3.3 Загрузка данных с карточки

DDP_035 Процесс загрузки данных с карточки тахографа состоит из следующих этапов:

- Загрузка общей информации, записанной на карточке в элементарных файлах ICC и IC. Эта информация не является обязательной и не защищена цифровой подписью.
- Загрузка элементарных файлов Card_Certificate и CA_Certificate. Эта информация не защищена цифровой подписью.

Вышеуказанные файлы загружаются в обязательном порядке при каждом сеансе загрузки.

- Загрузка элементарных файлов с другими прикладными данными (входящих в каталог тахографа), кроме файла Card_Download. Эта информация защищена цифровой подписью.
- При каждом сеансе загрузки обязательно загружаются как минимум элементарные файлы Application_Identification и ID.
    - При загрузке данных с карточки водителя в обязательном порядке загружаются также следующие элементарные файлы:
        - Events_Data,
        - Faults_Data,
        - Driver_Activity_Data,
        - Vehicles_Used,
        - Places,
        - Control_Activity_Data,
        - Specific_Conditions.
- При загрузке данных с карточки водителя обновляется дата LastCardDownload в элементарном файле Card_Download.
- При загрузке данных с карточки мастерской обнуляется счетчик калибровок в элементарном файле Card_Download.

3.3.1 Процедура инициализации

DDP_036 СПА запускает процедуру следующим образом:

Карточка	Направл.	СПА / УСК	Пояснение / Примечания
	⇦	Перезапуск аппаратуры	
ATR	⇨		

Возможно использование ВПП для переключения на более высокую скорость передачи данных, если она поддерживается МПК.

3.3.2 Процедура для неподписанных файлов данных

DDP_037 Процедура загрузки элементарных файлов ICC, IC, Card_Certificate и CA_Certificate выглядит следующим образом:

Карточка	Направл.	СПА / УСК	Пояснение / Примечания
	⇦	Выбор файла	Выбор файла по идентификаторам
OK	⇨		
	⇦	Считывание данных	Если объем данных файла превышает емкость буфера считывающего устройства или карточки, команда повторяется до тех пор, пока не будет считан весь файл.
Данные файла OK	⇨	Сохранение данных на ВН	В соответствии с 3.4 (3.4 Формат сохранения данных)

Примечание: перед выбором элементарного файла Card_Certificate необходимо выбрать приложение "Тахограф" (выбор по ИП).

3.3.3 Процедура для подписанных файлов данных

DDP_038 Для каждого из нижеперечисленных файлов, загружаемых вместе с соответствующей подписью, применяется следующая процедура:

Карточка	Напр.	СПА / УСК	Пояснение / Примечания
	⇦	Выбор файла	
OK	⇨		
	⇦	Расчет хеш-функции	Рассчитывает хеш-функцию по данным, содержащимся в выбранном файле, на основе хеш-алгоритма, предписанного в соответствии с подразделом 11. Эта команда не является ISO-командой.
Расчет и временное сохранение хеш-функции файла			
OK	⇨		
	⇦	Считывание данных	Если объем данных файла превышает емкость буфера считывающего устройства или

			карточки, команда повторяется до тех пор, пока не будет считан весь файл.
Данные файла OK	⇨	Сохранение полученных данных на ВН	В соответствии с 3.4 (3.4 Формат сохранения данных)
	⇦	PSO: Расчет цифровой подписи	
На основе временно сохраненной хеш-функции выполняется защитная операция "Генерировать цифровую подпись"			
Подпись OK	⇨	Данные приобщаются к данным, сохраненным на ВН ранее	В соответствии с 3.4 (3.4 Формат сохранения данных)

3.3.4 Процедура обнуления счетчика калибровок

DDP_039 Для обнуления счетчика NoOfCalibrationsSinceDownload в элементарном файле Card_Download, хранящемся на карточке мастерской, применяется следующая процедура:

Карточка	**Напр.**	**СПА / УСК**	**Пояснение / Примечания**
	⇦	Выбор файла Card_Download	Выбор файла по идентификаторам
OK	⇨		
	⇦	Считывание файла NoOfCalibrationsSinceDownload = '00 00'	
Обнуление счетчика сеансов загрузки данных с карточки			
OK	⇨		

3.4 Формат сохранения данных

3.4.1 Введение

DDP_040 Загружаемые данные должны сохраняться с соблюдением следующих требований:

- данные сохраняются транспарентно. Это означает, что последовательность байтов, а также последовательность битов внутри каждого байта переносимых с карточки данных должна при их сохранении оставаться неизменной;

- все файлы, загружаемые с карточки за один сеанс загрузки, сохраняются на ВН в виде одного файла.

3.4.2 Формат файлов

DDP_041 Формат файла представляет собой совокупность нескольких взаимосвязанных TLV-объектов.

DDP_042 Меткой EF является FID с добавлением „00“.

DDP_043 Меткой подписи EF является FID файла с добавлением „01“.

DDP_044 Значение длины состоит из двух байтов. Им определяется число байтов в поле значений. Значение „FF FF“ в поле длины резервируется для последующего использования.

DDP_045 Если файл не загружается, то никакая информация о нем сохранению не подлежит (т.е. не сохраняется ни метка, ни нулевой параметр длины).

DDP_046 В качестве TLV-объекта, следующего непосредственно за TLV-объектом с данными файла, сохраняется подпись.

Определение	Пояснение	Длина
FID (2 байта) || „00“	Метка EF (FID)	3 байта
FID (2 байта) || „01“	Метка подписи EF (FID)	3 байта
Xx xx	Длина поля значений	2 байта

Пример данных в файле, загруженном на ВН:

Метка	Длина	Значение
00 02 00	00 11	Данные EF ICC
C1 00 00	00 C2	Данные EF Card_Certificate
		...
05 05 00	0A 2E	Данные EF Vehicles_Used
05 05 01	00 80	Подпись EF Vehicles_Used

4. Загрузка данных с карточек тахографа через бортовое устройство

DDP_047 БУ должно обеспечивать возможность загрузки данных с введенной в него карточки водителя на подключенную СПА.

DDP_048 Для инициализации данного режима СПА направляет БУ сообщение "Transfer Data Request Card Download" – "Запрос передачи данных, загруженных с карточки" (см. 2.2.2.9).

DDP_049 После этого БУ файл за файлом загружает с карточки все имеющиеся на ней данные в соответствии с протоколом загрузки, который определен в пункте 0, и передает все полученные таким образом данные на СПА в соответствующем TLV-формате (см. 3.4.2), заключенные внутри сообщения "Положительный ответ на запрос передачи данных".

DDP_050 СПА извлекает данные карточки из сообщения "Положительный ответ на запрос передачи данных" (освобождая их от всех заголовков, SIDов, TREPов, счетчиков подсообщений и контрольных сумм) и сохраняет их в одном физическом файле, как указано в пункте 2.3.

DDP_051 Затем БУ при необходимости обновляет содержание файла Control_Activity_Data или файла Card_Download на карточке водителя.

ПОДРАЗДЕЛ VIII

ПРОТОКОЛ КАЛИБРОВКИ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

1. Введение

В настоящем подразделе рассматривается процесс обмена данными между бортовым устройством и тестером по К-линии, предусмотренной в калибровочном интерфейсе, описание которого приводится в подразделе VI. В нем также указан способ управления каналом ввода-вывода на калибровочном разъеме.

Процедура установления связи по К-линии описана в пункте 4 "Функции обмена данными".

Для определения задач управления обменом данными по К-линии при различных условиях в данном подразделе используется понятие "диагностических сеансов". По умолчанию под этим понимается сеанс “StandardDiagnosticSession”, при котором с бортового устройства могут быть считаны все имеющиеся данные, однако сохранение данных на бортовом устройстве невозможно.

Выбор вида диагностического сеанса рассмотрен в пункте 5 ("Административные функции").

CPR_001 Сеанс “ECUProgrammingSession” позволяет вводить данные в бортовое устройство. При этом для ввода калибровочных данных (требования 097 и 098) бортовое устройство должно быть переведено в режим CALIBRATION.

Процесс передачи данных по К-линии описан в пункте 6 ("Функции передачи данных"). Форматы передаваемых данных подробно указаны в пункте 8 ("Форматы записей данных").

CPR_002 Сеанс “ECUAdjustmentSession” позволяет выбирать режим работы канала ввода-вывода калибровочных данных через интерфейс К-линии. Способ управления каналом ввода-вывода калибровочных данных изложен в пункте 7 ("Настройка проверочных импульсов – функциональный блок регулировки входного/выходного сигнала").

CPR_003 Адрес тестера везде в настоящем документе обозначен как 'tt'. Хотя для тестеров могут существовать общепринятые адреса, БУ должно быть способно правильно поддерживать связь с тестером по любому адресу. Физический адрес БУ - 0xEE.

2. Термины, определения и источники

Протоколы, сообщения и коды ошибок в основном соответствуют нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции. Версия 6 от 22 февраля 2001 года).

Для идентификаторов функций, запросов функций и ответов на них, а также для стандартных параметров используются байтовое кодирование и шестнадцатеричные величины.

Под термином "тестер" понимается аппаратура, используемая для ввода программных/калибровочных данных в БУ.

Под терминами "клиент" и "сервер" понимаются, соответственно, тестер и БУ.

Под аббревиатурой "ECU", означающей "электронный контрольный блок", понимается БУ.

Источники:

ISO 14230-2 Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 2. Уровень обмена данными. Первое издание, 1999 год. Транспортные средства. Системы диагностического контроля.

3. Обзор функций

3.1 Перечень имеющихся функций

В таблице ниже представлен обзорный перечень функций, которые должны быть предусмотрены в контрольном устройстве и определения которых приводятся в настоящем документе.

CPR_004 В таблице показаны функции, доступные после начала диагностического сеанса.

- В **1-м столбце** приведен перечень имеющихся функций.
- Во **2-м столбце** перечислены номера пунктов данного подраздела, содержащих развернутые определения соответствующих функций.
- В **3-м столбце** указаны значения идентификаторов соответствующих функций, используемые в запросах.
- В **4-м столбце** указаны функции сеанса **"StandardDiagnosticSession" (SD)**, которые должны быть реализованы в каждом БУ.

В **5-м столбце** указаны функции сеанса **"ECUAdjustmentSession" (ECUAS)**, которые должны быть реализованы для обеспечения возможности управления каналом ввода-вывода калибровочного разъема на передней панели БУ.

- В **6-м столбце** указаны функции сеанса **"ECUProgrammingSession" (ECUPS)**, которые должны быть выполнены для обеспечения возможности программирования параметров работы БУ.

Таблица 1

Сводная таблица идентификаторов функций

			Диагностические сеансы		
Название диагностической функции	**No. пунктов**	**Идент. функции д/запроса**	**SD**	**ECUAS**	**ECUPS**
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Символ, означающий обязательность функции для данного диагностического сеанса.

Отсутствие символа означает, что в процессе данного диагностического сеанса указанная функция невозможна.

3.2 Коды ответов

Для каждой функции предусмотрены определенные коды ответов.

4. Функции обмена данными

Ряд функций необходимы для установления и поддержания канала обмена данными. На уровне приложений они не отображаются. Описание имеющихся функций приведено в таблице ниже.

Таблица 2

Функции обмена данными

Название функции	Описание
StartCommunication	Запрос клиента на инициализацию сеанса обмена данными с сервером(ами).
StopCommunication	Запрос клиента на прекращение текущего сеанса обмена данными.
TesterPresent	Сообщение клиента серверу о продолжении своего присутствия на линии.

CPR_005 Функция StartCommunication используется для инициализации обмена данными. Для выполнения любой функции необходимо начать обмен данными и обеспечить, чтобы его параметры соответствовали нужному режиму.

4.1 Функция StartCommunication

CPR_006 По получении примитива индикации StartCommunication БУ проверяет возможность инициализации запрошенного канала обмена данными при существующих условиях. Описание условий, необходимых для инициализации канала обмена данными, приведено в документе ISO 14230-2.

CPR_007 После этого БУ выполняет все действия, необходимые для инициализации канала обмена данными, и возвращает примитив ответа StartCommunication с выбранными параметрами положительного ответа.

CPR_008 Если на БУ, которое уже инициализовано (и уже находится в процессе того или иного диагностического сеанса), поступает новый запрос StartCommunication (например, при восстановлении работы тестера после сбоя), то этот запрос принимается и производится повторная инициализация БУ.

CPR_009 Если по каким-либо причинам канал обмена данными не может быть инициализован, то БУ продолжает функционировать в том же режиме, в котором оно находилось непосредственно перед попыткой инициализации канала обмена данными.

CPR_010 Сообщение с запросом StartCommunication должно иметь физическую адресацию.

CPR_011 Инициализация БУ для выполнения соответствующих функций производится методом "ускоренной инициализации":

- любой операции предшествует определенный период бездействия шины;
- затем тестер высылает шаблон инициализации;
- ответ БУ содержит всю информацию, необходимую для установления канала обмена данными.

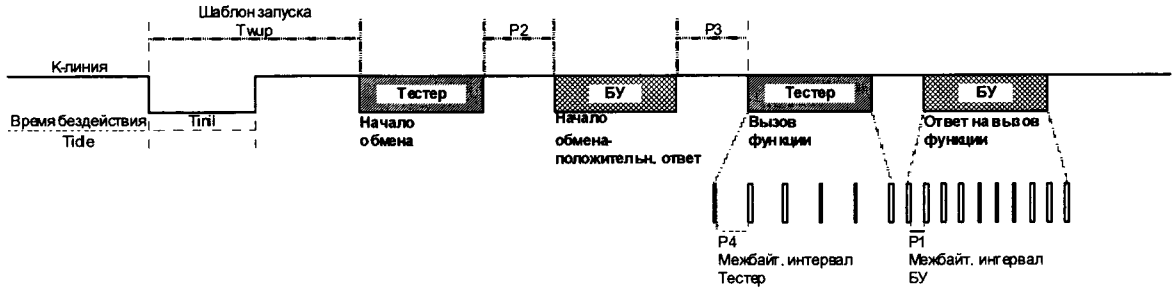
CPR_012 По завершении инициализации

значения всех параметров обмена данными задаются такими, как определено в

- в соответствии с байтами ключей;
- БУ ожидает первого запроса от тестера;
- БУ находится в диагностическом режиме, выбираемом по умолчанию, т.е. в режиме StandardDiagnosticSession;
- канал ввода-вывода калибровочных данных находится в состоянии, выбираемом по умолчанию, т.е. не активирован.

CPR_014 Скорость передачи данных по К-линии составляет 10 400 бод.

CPR_016 Для вызова ускоренной инициализации тестер передает по К-линии шаблон запуска (Wup). Этот шаблон начинает действовать после периода бездействия на К-линии, с периода низкого уровня тактового сигнала, равного Tinil. Тестер высылает первый бит сообщения StartCommunicationService по истечении периода Twup с момента первого спада тактового сигнала.



CPR_017 Значения временных параметров ускоренной инициализации и обмена данными в целом приведены в нижеследующих таблицах. Время бездействия может быть различным:

- от включения питания до первой передачи данных: Tidle = 300 мс;
- после завершения функции StopCommunication: Tidle = P3 мин;
- после прекращения обмена данными из-за превышения времени ожидания P3 max: Tidle = 0.

Таблица 3

Временные параметры ускоренной инициализации

Параметр		мин. значение	макс. значение
Tinil	25 ± 1 мс	24 мс	26 мс
Twup	50 ± 1 мс	49 мс	51 мс

Таблица 4

Временные параметры обмена данными

Временной параметр	Описание параметра	Нижние предельные значения [мс]	Верхние предельные значения [мс]
		мин.	макс.
P1	Межбайтовый интервал для ответа БУ	0	20
P2	Интервал между запросом тестера и ответом БУ или между двумя ответами БУ	25	250
P3	Интервал между окончанием ответов БУ и началом нового запроса тестера	55	5000
P4	Межбайтовый интервал для запроса тестера	5	20

CPR_018 Формат сообщений для ускоренной инициализации подробно указан в нижеследующих таблицах.

Таблица 5

Запрос StartCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	81	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	**Идентификатор функции запроса StartCommunication**	**81**	**SCR**
#5	Контрольная сумма	00-FF	CS

Таблица 6

Положительный ответ на запрос StartCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции положительного ответа на запрос StartCommunication**	**C1**	**SCRPR**
#6	Байт ключа 1	EA	KB1
#7	Байт ключа 2	8F	KB2
#8	Контрольная сумма	00-FF	CS

CPR_019 Отрицательный ответ на запрос StartCommunication невозможен. При отсутствии положительного ответа инициализация БУ не происходит, никакие сообщения не передаются, и устройство продолжает функционировать в обычном режиме.

4.2 Функция StopCommunication

4.2.1 Описание сообщения

Эта функции уровня обмена данными предназначена для прекращения сеанса обмена.

CPR_020 По получении примитива индикации StopCommunication БУ проверяет возможность прекращения текущего обмена данными. Если это возможно, то в этом случае БУ выполняет все действия, необходимые для прекращения сеанса обмена данными.

CPR_021 Если обмен данными может быть прекращен, то перед прекращением обмена данными БУ возвращает примитив ответа StopCommunication с выбранными параметрами положительного ответа.

CPR_022 Если по каким-либо причинам прекращение обмена данными невозможно, то БУ возвращает примитив ответа StopCommunication с выбранными параметрами отрицательного ответа.

CPR_023 Если БУ фиксирует истечение периода ожидания P3max, то обмен данными прекращается без направления какого-либо примитива ответа.

4.2.2 Формат сообщений

CPR_024 Форматы сообщений для примитивов StopCommunication подробно указаны в нижеследующих таблицах.

Таблица 7

Запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	01	LEN
#5	**Идентификатор функции запроса StopCommunication**	**82**	**SPR**
#6	Контрольная сумма	00-FF	CS

Таблица 8

Положительный ответ на запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	**Идентификатор функции положительного ответа на запрос StopCommunication**	**C2**	**SPRPR**
#6	Контрольная сумма	00-FF	CS

Таблица 9

Отрицательный ответ на запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Контрольная сумма	00-FF	CS

Определение параметров

Данная функция не требует определения каких-либо параметров.

4.3 Функция TesterPresent

4.3.1 Описание сообщения

Функция TesterPresent используется тестером для оповещения сервера о продолжении присутствия на линии с целью предотвратить автоматическое возвращение сервера в обычный режим работы и возможный обрыв связи. Периодически высылаемый запрос данной функции позволяет поддерживать непрерывный сеанс диагностики/обмена данными, так как счетчик времени P3 обнуляется при каждом очередном поступлении этого запроса.

4.3.2 Формат сообщений

CPR_079 Форматы сообщений для примитивов TesterPresent подробно указаны в нижеследующих таблицах.

Таблица 10

Запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	**Идентификатор функции запроса TesterPresent**	**3E**	**TP**
#6	Подфункция = responseRequired да (требуется ответ) нет	01 02	RESPREQ_Y RESPREQ_NO
#7	Контрольная сумма	00-FF	CS

CPR_080 Если параметр responseRequired установлен на ответ "да", то сервер возвращает положительный ответ, показанный ниже. Если параметр установлен на ответ "нет", то на данный запрос сервер не отвечает.

Таблица 11

Положительный ответ на запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	**Идентификатор функции положительного ответа на запрос TesterPresent**	**7E**	**TPPR**
#6	Контрольная сумма	00-FF	CS

CPR_081 В данной функции предусмотрены следующие коды возможного отрицательного ответа:

Таблица 12

Отрицательный ответ на запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса TesterPresent	3E	TP
#7	ResponseCode (код ответа) = [SubFunctionNotSupported- InvalidFormat incorrectMessageLength] (подфункция не поддерживается-неправильный формат- неверная длина сообщения)	12 13	RC_SFNS_IF RC_IML
#8	Контрольная сумма	00-FF	CS

5. Административные функции

Описание имеющихся функций приводится в таблице ниже.

Таблица 13

Административные функции

Название функции	Описание
StartDiagnosticSession	Клиент запрашивает инициализацию диагностического сеанса с БУ.
SecurityAccess	Клиент запрашивает доступ к функциям, предназначенным только для санкционированных пользователей.

5.1 Функция StartDiagnosticSession

5.1.1 Описание сообщения

CPR_025 Функция StartDiagnosticSession используется для запуска различных диагностических сеансов на сервере. В ходе диагностического сеанса предоставляется доступ к определенному набору функций, согласно указанному в таблице 17. Некоторые функции, возможные в ходе таких сеансов, специфичны для транспортных средств конкретных изготовителей и в настоящем документе не рассматриваются. Правила технической реализации соответствующих систем должны отвечать следующим требованиям:

- БУ должно постоянно поддерживать только один текущий диагностический сеанс;
- при подаче питания БУ во всех случаях должно начинать стандартный сеанс диагностики (StandardDiagnosticSession). Если после этого не будет начат другой диагностический сеанс, то стандартный сеанс диагностики продолжается до тех пор, пока питание БУ не будет отключено;
- если тестером запрашивается уже запущенный диагностический сеанс, то БУ возвращает положительный ответ;
- если тестером запрашивается новый диагностический сеанс, то БУ сначала высылает положительный ответ на запрос StartDiagnosticSession, а затем запускает новый сеанс. Если БУ не имеет возможности начать новый диагностический сеанс в соответствии с запросом, оно возвращает отрицательный ответ на запрос StartDiagnosticSession, а текущий сеанс продолжается.

CPR_026 Диагностический сеанс может быть начат только при условии, что между клиентом и БУ установлен канал обмена данными.

CPR_027 Временные параметры, определенные в таблице, начинают применяться после успешного выполнения запроса StartDiagnosticSession, в котором параметр diagnosticSession был установлен на “StandardDiagnosticSession” (стандартный сеанс диагностики), если до этого выполнялся другой диагностический сеанс.

5.1.2 Формат сообщений

CPR_028 Формат сообщений для примитивов StartDiagnosticSession подробно указан в нижеследующих таблицах.

Таблица 14
Административные функции

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	**Идентификатор функции запроса StartDiagnosticSession**	10	STDS
#6	DiagnosticSession (диагностический сеанс) = [одно из значений в Таблице 17]	xx	DS_…
#7	Контрольная сумма	00-FF	CS

Таблица 15
Положительный ответ на запрос StartDiagnosticSession

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	**Идентификатор функции положительного ответа на запрос StartDiagnosticSession**	**50**	**STDSPR**
#6	DiagnosticSession (диагностический сеанс) = [то же значение, что и у байта #6 в Таблице 14]	xx	DS_…
#7	Контрольная сумма	00-FF	CS

Таблица 16

Отрицательный ответ на запрос StartDiagnosticSession

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#7	ResponseCode = [subFunctionNotSupported [a] (код ответа) (подфункция не поддерживается) incorrectMessageLength [b] (неверная длина сообщения) conditionsNotCorrect [c] (недопустимые условия)	12 13 22	RC_SFNS RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

[a] – значение, заданное в байте #6 запроса, не поддерживается и поэтому не фигурирует в таблице 17,

[b] – длина сообщения не соответствует ожидаемой,

[c] – не соблюдены критерии выполнения запроса StartDiagnosticSession.

5.1.3 Определение параметров

CPR_029 Параметр ***diagnosticSession (DS_)*** используется функцией StartDiagnosticSession для выбора того или иного режима работы сервера(ов). В настоящем документе указаны его значения для следующих видов диагностических сеансов:

Таблица 17

Определение значений параметра diagnosticSession

Шестн. значение	Описание	Мнемокод
81	StandardDiagnosticSession (стандартный диагностический сеанс). В ходе данного диагностического сеанса могут использоваться все функции, указанные в **столбце 4 ("SD") таблицы 1**. Эти функции позволяют считывать данные, хранящиеся на сервере (БУ). Данный диагностический сеанс запускается после успешного завершения инициализации канала связи между клиентом (тестер) and сервером (БУ). Этот сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.	SD
85	ECUProgrammingSession (сеанс программирования контрольной аппаратуры). В ходе данного диагностического сеанса могут использоваться все функции, указанные в **столбце 6 ("ECUPS") таблицы 1**. Эти функции обеспечивают программирование памяти сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.	ECUPS
87	ECUAdjustmentSession (сеанс настройки контрольной аппаратуры). В ходе данного диагностического сеанса могут использоваться все функции, указанные в **столбце 5 ("ECUAS") таблицы 1**. Эти функции обеспечивают регулировку параметров входного/выходного сигнала сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.	ECUAS

5.2 Функция SecurityAccess (защищенный доступ)

Запись калибровочных данных и доступ к каналу ввода/вывода этих данных возможны лишь при условии, что БУ находится в режиме CALIBRATION (калибровка). Для получения доступа к режиму CALIBRATION необходимо, помимо ввода в БУ действительной карточки мастерской, ввести в бортовое устройство соответствующий PIN-код.

Функция SecurityAccess обеспечивает возможность введения PIN-кода и получения тестером информации о том, находится ли БУ в режиме CALIBRATION.

Допустимы и другие методы введения PIN-кода.

5.2.1 Описание сообщения

Функция SecurityAccess предусматривает направление сообщения SecurityAccess "requestSeed" (запрос стартового значения для генерации ключа), за которым на соответствующем этапе следует сообщение SecurityAccess "sendKey" (передача ключа). Функция SecurityAccess выполняется в обязательном порядке после функции StartDiagnosticSession.

CPR_033 Сообщение SecurityAccess "requestSeed" используется тестером для проверки готовности бортового устройства к приему PIN-кода.

CPR_034 Если бортовое устройство уже находится в режиме CALIBRATION, то в ответ на запрос оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение 0x0000.

CPR_035 Если бортовое устройство готово принять PIN-код для проверки с помощью карточки мастерской, то оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение, превышающее 0x0000.

CPR_036 Если бортовое устройство не готово принять от тестера PIN-код, поскольку карточка мастерской недействительна или не была введена в устройство, либо потому, что бортовое устройство ожидает введения PIN-кода другим способом, то оно возвращает отрицательный ответ с кодом conditionsNotCorrectorRequestSequenceError (недопустимые условия или неверная последовательность запросов).

CPR_037 В таких случаях тестер передает PIN-код на бортовое устройство с помощью сообщения SecurityAccess "sendKey". Для обеспечения достаточного времени, необходимого для завершения процесса аутентификации карточки, БУ использует код отрицательного ответа requestCorrectlyReceived-ResponsePending (запрос получен правильно – ожидается ответ), позволяющий продлить период ожидания ответа. Этот период, однако, не может превышать 5 минут. Как только выполнение запрошенной функции завершается, БУ высылает положительный ответ или отрицательный ответ с кодом, отличным от данного. Код отрицательного ответа requestCorrectlyReceived-ResponsePending может высылаться бортовым устройством

неоднократно, вплоть до завершения запрошенной функции и направления заключительного ответного сообщения.

CPR_038 Бортовое устройство реагирует на данный запрос с помощью функции положительного ответа SecurityAccess лишь тогда, когда оно находится в режиме CALIBRATION.

CPR_039 Ниже перечисляются случаи, когда бортовое устройство возвращает на данный запрос отрицательный ответ, и соответствующие коды ответа.

subFunctionNot supported: неправильный формат параметра подфункции (accessType);

conditionsNotCorrectOrRequestSequenceError: бортовое устройство не готово к введению PIN-кода;

invalidKey: неверный PIN-код; допустимое количество попыток подтверждения PIN-кода не превышено;

exceededNumberOfAttempts: неверный PIN-код; допустимое количество попыток подтверждения PIN-кода превышено;

generalReject: PIN-код верен, но взаимную аутентификацию устройства и карточки мастерской произвести не удалось.

5.2.2 Формат сообщений SecurityAccess –requestSeed

CPR_040 Форматы сообщений для примитивов SecurityAccess "requestSeed" подробно указаны в нижеследующих таблицах.

Таблица 18

Запрос SecurityAccess –requestSeed

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	**Идентификатор функции запроса SecurityAccess**	**27**	**SA**
#6	accessType (тип доступа) – requestSeed	7D	AT_RSD
#7	Контрольная сумма	00-FF	CS

Таблица 19

Положительный ответ на запрос SecurityAccess – requestSeed

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	04	LEN
#5	**Идентификатор функции положительного ответа на запрос SecurityAccess**	**67**	**SAPR**
#6	accessType (тип доступа) – requestSeed	7D	AT_RSD
#7	Стартовое значение - верхний байт	00-FF	SEEDH
#8	Стартовое значение - нижний байт	00-FF	SEEDL
#9	Контрольная сумма	00-FF	CS

Таблица 20

Отрицательный ответ на запрос SecurityAccess

# байта	Параметр	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	responseCode (код ответа) = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	 22 13	 RC_CNC RC_IML
#8	Контрольная сумма	00-FF	CS

5.2.3 Формат сообщений SecurityAccess – sendKey

CPR_041 Форматы сообщений для примитивов SecurityAccess "sendKey" подробно указаны в нижеследующих таблицах.

Таблица 21

Запрос SecurityAccess – sendKey

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+2	LEN
#5	**Идентификатор функции запроса SecurityAccess**	**27**	**SA**
#6	accessType (тип доступа) – sendKey	7E	AT_SK
#7 to #m+6	Ключ #1 (верхний) … Key #m (нижний, m должно составлять не менее 4 и не более 8)	xx … xx	KEY
#m+7	Контрольная сумма	00-FF	CS

Таблица 22

Положительный ответ на запрос SecurityAccess – sendKey

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	**Идентификатор функции положительного ответа на запрос SecurityAcces**	**67**	**SAPR**
#6	accessType (тип доступа) – sendKey	7E	AT_SK
#7	Контрольная сумма	00-FF	CS

Таблица 23

Отрицательный ответ на запрос SecurityAccess

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	ResponseCode (код ответа) = [generalReject subFunctionNotSupported (подфункция не поддерживается) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrectOrRequestSequenceError invalidKey (недопутимые условия – ошибка в запросе – недействительный ключ) exceededNumberOfAttempts (превышение числа попыток) requestCorrectlyReceived-ResponsePending] (запрос получен правильно – ожидается ответ)	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Контрольная сумма	00-FF	CS

6. Функции передачи данных

Описание имеющихся функций приведено в таблице ниже.

Таблица 24

Функции передачи данных

Название функции	Описание
ReadDataByIdentifier	Клиент запрашивает передачу текущего значения записи с доступом по идентификатору recordDataIdentifier.
WriteDataByIdentifier	Клиент запрашивает возможность сохранения записи, доступ к которой был получен по идентификатору recordDataIdentifier.

6.1 Функция ReadDataByIdentifier

6.1.1 Описание сообщения

CPR_050 Функция ReadDataByIdentifier используется клиентом с целью запроса у сервера значения записей данных. Д анные опознаются по идентификатору recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера.

6.1.2 Формат сообщений

CPR_051 Форматы сообщений для примитивов ReadDataByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 25

Запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции запроса ReadDataByIdentifier**	**22**	**RDBI**
#6 to #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_…
#8	Контрольная сумма	00-FF	CS

Таблица 26

Положительный ответ на запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	**Идентификатор функции положительного ответа на запрос ReadDataByIdentifier**	**62**	**RDBIPR**
#6 and #7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в таблице 25]	xxxx	RDI_...
#8 to #m+7	dataRecord[] = [данные#1 : данные#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 27

Отрицательный ответ на запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#7	ResponseCode (код ответа) = [requestOutOfRange (нештатный запрос) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия)]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Определение параметров

CPR_052 Параметр *recordDataIdentifier (RDI_)* в запросе ReadDataByIdentifier служит для идентификации записи данных.

CPR_053 Значения параметра recordDataIdentifier, определенные в настоящем документе, указаны в таблице ниже.

Таблица значений параметра recordDataIdentifier состоит из четырех столбцов и ряда строк.

В 1-м столбце (Шестн. значение) приведено шестнадцатеричное значение, закрепленное за идентификатором recordDataIdentifier, который указан в 3-м столбце.

Во 2-м столбце (Data element) указан элемент данных согласно подразделу I, лежащий в основе параметра recordDataIdentifier (в некоторых случаях требуется перекодирование).

В 3-м столбце (Идентификатор) указано наименование соответствующего идентификатора recordDataIdentifier.

В 4-м столбце (Мнемокод) указан мнемокод данного идентификатора recordDataIdentifier.

Таблица 28

Определение значений параметра recordDataIdentifier

Шестн. значение	**Элемент данных**	**Идентификатор recordDataIdentifier (формат см. в пункте 8.2)**	**Мнемокод**
F90B	CurrentDateTime (текущая дата и время)	TimeDate	RDI_TD
F912	HighResOdometer (показания счетчика пробега с высоким разрешением)	HighResolutionTotalVehicle Distance	RDI_HRTV D
F918	K-ConstantOfRecording Equipment (K- постоянная записывающей аппаратуры)	Kfactor	RDI_KF
F91C	L-TyreCircumference (L- показатель окружности шин)	LfactorTyreCircumference	RDI_LF

Шестн. значение	Элемент данных	Идентификатор recordDataIdentifier (формат см. в пункте 8.2)	Мнемокод
F91D	W-VehicleCharacteristic Constant (W- характеристическая постоянная транспортного средства)	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize (размер шин)	TyreSize	RDI_TS
F922	nextCalibrationDate (дата следующей калибровки)	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised (разрешенная скорость)	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation (страна регистрации транспортного средства)	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber (регистрационный номер транспортного средства)	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber (опознавательный номер транспортного средства)	VIN	RDI_VIN

CPR_054 Параметр ***dataRecord (DREC_)*** используется в положительном ответе на запрос ReadDataByIdentifier для сообщения клиенту (тестеру) значения записи данных, опознаваемой по идентификатору recordDataIdentifier. Форматы данных указаны в пункте 8. Для удобства пользователя могут быть предусмотрены и другие, не определяемые в настоящем документе виды записей данных, включая специфичные для той или иной модели БУ входные, внутренние и выходные данные.

6.2 Функция WriteDataByIdentifier

6.2.1 Описание сообщения

CPR_056 Функция WriteDataByIdentifier используется клиентом в целях сохранения значений записей данных на сервере. Для идентификации данных служит параметр recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера. Для обновления значений параметров, перечисленных в таблице 28, БУ должно быть переведено в режим CALIBRATION.

6.2.2 Формат сообщений

CPR_057 Форматы сообщений для примитивов WriteDataByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 29

Запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	**Идентификатор функции запроса WriteDataByIdentifier**	**2E**	**WDBI**
#6 - #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_…
от #8 до m+7	запись данных[] = [данные#1 : данные#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 30

Положительный ответ на запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции положительного ответа на запрос WriteDataByIdentifier**	**6E**	**WDBIPR**
#6 - #7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в таблице 29]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 31

Отрицательный ответ на запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#7	ResponseCode (код ответа) =[requestOutOfRange (нештатный запрос) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия)]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Определение параметров

Определение параметра recordDataIdentifier (RDI_) приводится в таблице 28.

Параметр dataRecord (DREC_) используется в запросе WriteDataByIdentifier для сообщения серверу (БУ) значений записей данных, опознаваемых по идентификаторам recordDataIdentifier. Форматы данных указаны в пункте 8.

7. Настройка проверочных импульсов – функциональный блок регулировки входного/выходного сигнала

Описание имеющихся функций приведено в таблице ниже.

Таблица 32

Функция InputOutputControlByIdentifier

Название функции	Описание
InputOutputControlByIdentifier	Клиент запрашивает управление параметрами входного/выходного сигнала данного сервера.

7.1 Функция InputOutputControlByIdentifier

Описание сообщения

Подключение соответствующего тестера к разъему на передней панели позволяет производить настройку или мониторинг проверочных импульсов.

CPR_058 Конфигурация калибровочного канала ввода-вывода может быть изменена с помощью команды, передаваемой по K-линии с использованием функции InputOutputControlByIdentifier, позволяющей задавать этому каналу необходимый режим ввода или вывода данных. Предусмотрены следующие режимы:

отключение,

режим speedSignalInput, при котором по каналу ввода-вывода калибровочных данных вводится тест-сигнал скорости, заменяющий собой сигнал скорости от датчика движения,

режим realTimeSpeedSignalOutputSensor, при котором по каналу ввода-вывода калибровочных данных выводится сигнал скорости, поступающий от датчика движения,

режим RTCOutput, при котором по каналу ввода-вывода калибровочных данных выводится сигнал синхронизации в формате UTC.

CPR_059 Для изменения конфигурации канала на бортовом устройстве должен быть инициирован сеанс настройки, а само устройство должно находиться в режиме CALIBRATION. При завершении сеанса настройки или при выходе из режима CALIBRATION бортовое устройство должно обеспечивать возвращение канала ввода-вывода калибровочных данных в "отключенное" состояние (в котором он находится по умолчанию).

CPR_060 В случае поступления импульсов скорости по входному каналу БУ, предназначенному для приема сигнала скорости в реальном времени, когда канал ввода-вывода калибровочных данных переключен на ввод, канал ввода-вывода калибровочных данных переключается на вывод или возвращается в отключенное состояние.

CPR_061 Последовательность операций выглядит следующим образом:

инициализация обмена данными с помощью функции StartCommunication;

запуск сеанса настройки с помощью функции StartDiagnosticSession и переход в режим CALIBRATION (очередность выполнения этих двух операций значения не имеет);

регулировка канала вывода данных с помощью функции InputOutputControlByIdentifier.

7.1.2 Формат сообщений

CPR_062 Форматы сообщений для примитивов InputOutputControlByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 33

Запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	**Идентификатор функции запроса InputOutputControlByIdentifier**	**2F**	**IOCBI**
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 - #9	ControlOptionRecord = [inputOutputControlParameter – одно значение из таблицы 36 controlState – одно значение из таблицы 37 (см. примечание ниже)]	xx xx	COR_... IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Примечание. Параметр controlState (управление конфигурацией) присутствует лишь в некоторых случаях (см. 7.1.3).

Таблица 34

Положительный ответ на запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	**Идентификатор функции положительного ответа на запрос inputOutputControlByIdentifier**	**6F**	**IOCBIPR**
#6 и #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 - #9	controlStatusRecord = [inputOutputControlParameter (то же значение, что и у байта #8 в таблице 33) controlState (то же значение, что и у байта #9 в таблице 33)] (если применимо)	xx xx	CSR_ IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Таблица 35

Отрицательный ответ на запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	**Идентификатор функции отрицательного ответа**	**7F**	**NR**
#6	Идентификатор функции запроса inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode (код ответа) =[incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия) requestOutOfRange (нештатный запрос) deviceControlLimitsExceeded (вне диапазона регулировки устройства)]	 13 22 31 7A	 RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Контрольная сумма	00-FF	CS

Определение параметров

CPR_064 Определение параметра ***inputOutputControlParameter (IOCP_)*** приведено в нижеследующей таблице.

Таблица 36

Определение значений параметра inputOutputControlParameter

Шестн. значение	Описание	Мнемокод
00	**ReturnControlToECU** Это значение оповещает сервер (БУ) о том, что тестер перестал управлять каналом ввода-вывода калибровочных данных.	RCTECU
01	**ResetToDefault** Это значение оповещает сервер (БУ) о том, что ему следует вернуть канал ввода-вывода калибровочных данных в состояние, выбираемое по умолчанию.	RTD
03	**ShortTermAdjustment** Это значение оповещает сервер (БУ) о том, что ему следует настроить канал ввода-вывода калибровочных данных по значению, указанному в параметре controlState.	STA

CPR_065 Параметр ***controlState*** (управление конфигурацией) присутствует лишь в случаях, когда параметр inputOutputControlParameter установлен на ShortTermAdjustment. Определение значений параметра ***controlState*** приводится в таблице ниже.

Таблица 37

Определение значений параметра controlState

Режим	Шестн. значение	Описание
Отключен	00	Канал ввода/вывода отключен (выбирается по умолчанию)
Включен	01	Канал ввода/вывода калибровочных данных функционирует в режиме speedSignalInput (ввод сигнала скорости)
Включен	02	Канал ввода/вывода калибровочных данных функционирует в режиме realTimeSpeedSignalOutputSensor (выход сигнала датчика скорости в реальном времени)
Включен	03	Канал ввода/вывода калибровочных данных функционирует в режиме RTCOutput (выход сигнала синхронизации в формате UTC)

8. Форматы dataRecords (записей данных)

В настоящем разделе изложены:

- общие правила определения диапазона параметров, передаваемых бортовым устройством на тестер;

- форматы данных, передаваемых посредством функций передачи данных, о которых говорится в пункте 6.

CPR_067 Все указанные здесь параметры должны поддерживаться БУ.

CPR_068 Данные, передаваемые БУ на тестер по соответствующему запросу, по своему типу представляют собой результаты замеров (т.е. текущее значение запрошенного параметра, измеренное или зафиксированное бортовым устройством).

8.1 Диапазоны передаваемых параметров

CPR_069 В таблице 38 определены диапазоны, по которым определяется допустимость передаваемых значений параметров.

CPR_070 Используя значения диапазона "указатель ошибки", БУ может незамедлительно сообщать о том, что достоверные параметрические данные на текущий момент отсутствуют из-за той или иной ошибки контрольного устройства.

CPR_071 Значения диапазона "данные отсутствуют" могут использоваться бортовым устройством при передаче сообщений, в которых указаны отсутствующие или не поддерживаемые данным модулем параметры. С помощью значений диапазона "данные не запрашиваются" устройство может при передаче команды указать параметры, ответ по которым от устройства-адресата не требуется.

CPR_072 Если из-за отказа того или иного компонента передача достоверных данных о каком-либо параметре невозможна, то вместо этих данных используется указатель ошибки, приведенный в таблице 38. Если же данные, полученные в результате расчетов или измерений, являются достоверными, но выходят за пределы заданного диапазона значений запрошенного параметра, то указатель ошибки не используется. В этом случае при передаче данных используется соответствующее минимальное или максимальное значение параметра.

Таблица 38

Диапазоны dataRecords

Наименование диапазона	1 байт (Шестн. значение)	2 байта (Шестн. значение)	4 байта (Шестн. значение)	ASCII
Допустимый сигнал	00 - FA	0000 - FAFF	00000000 - FAFFFFFF	1 - 254
Указатель конкретного параметра	FB	FB00 - FBFF	FB000000 - FBFFFFFF	нет
Диапазон зарезервирован под разряды будущих указателей	FC - FD	FC00 - FDFF	FC000000 - FDFFFFFF	нет
Указатель ошибки	FE	FE00 - FEFF	FE000000 - FEFFFFFF	0
Данные отсутствуют или не запрашиваются	FF	FF00 - FFFF	FF000000 - FFFFFFFF	FF

CPR_073 Для параметров, представляемых с помощью кода ASCII, символ ASCII "*" резервируется в качестве ограничителя.

8.2 Форматы dataRecords

В таблицах 39-42 ниже подробно показаны форматы, используемые в связи с функциями ReadDataByIdentifier и WriteDataByIdentifier.

CPR_074 В таблице 39 указываются длина поля данных, разрешение и рабочий диапазон для каждого параметра, определяемого соответствующим идентификатором recordDataIdentifier.

Таблица 39

Формат dataRecords

Наименование параметра	Длина поля данных (байт)	Разрешение	Диапазон
TimeDate (время - дата)	8	*Подробно см. в таблице 40*	
HighResolutionTotalVehicleDistance (общее расстояние пробега)	4	прибавл.: 5 м/бит, обратн. сдвиг: 0 м	от 0 до +21 055 406 км
Kfactor (крэффициент K)	2	прибавл.: 0,001 имп./м/бит, обратн. сдвиг: 0	от 0 до 64,255 имп./м
LfactorTyreCircumference (коэффициент L окружности шины)	2	прибавл.: 0,125 10-3 м /бит, обратн. сдвиг: 0	от 0 до 8,031 м
WvehicleCharacteristicFactor (характеристический коэффициент W)	2	прибавл.: 0,001 имп./м/бит, обратн. сдвиг: 0	от 0 до 64,255 имп./м
TyreSize (размер шин)	15	ASCII	ASCII
NextCalibrationDate (дата следующей калибровки)	3	*Подробно см. в таблице 40*	
SpeedAuthorised (разрешенная скорость)	2	прибавл.: 1/256 км/ч/бит, обратн. сдвиг: 0	0-250,996 км/ч
RegisteringMemberState (государство - член регистрации)	3	ASCII	ASCII
VehicleRegistrationNumber (номер регистрации транспортного средства)	14	*Подробно см. в таблице 40*	
VIN	17	ASCII	ASCII

CPR_075 В таблице 40 подробно указаны форматы различных байтов параметра TimeDate:

Таблица 40

Подробное описание формата TimeDate (значение recordDataIdentifier # F90B)

Байт	Параметр	Разрешение	Диапазон
1	Секунды	прибавл.: 0,25 с/бит, обратн. сдвиг: 0 с	от 0 до 59,75 с
2	Минуты	прибавл.: 1 мин./бит, обратн. сдвиг: 0 мин.	от 0 до 59 мин.
3	Часы	прибавл.: 1 ч/бит, обратн. сдвиг: 0 ч	от 0 до 23 ч
4	Месяц	прибавл.: 1 мес./бит, обратн. сдвиг: 0 мес.	от 1 до 12 месяцев
5	День	прибавл.: 0,25 сут./бит, обратн. сдвиг: 0 сут. (см. ПРИМЕЧАНИЕ к таблице 41)	от 0,25 до 31,75 суток
6	Год	прибавл.: 1 год/бит, обратн. сдвиг: +1985 год (см. ПРИМЕЧАНИЕ к таблице 41)	1985 - 2235 годы
7	Поправка на местное время (мин)	прибавл.: 1 мин./бит обратн. сдвиг: -125 мин.	от -59 до +59 мин.
8	Поправка на местное время (ч)	прибавл.: 1 ч/бит, обратн. сдвиг: -125 ч	от -23 до +23 ч

CPR_076 В таблице 41 подробно указаны форматы различных байтов параметра NextCalibrationDate.

Таблица 41

Подробное описание формата NextCalibrationDate (значение recordDataIdentifier # F922)

Байт	Определение параметра	Разрешение	Диапазон
1	Месяц	прибавл.: 1 мес./бит, обратн. сдвиг: 0 мес.	от 1 до 12 месяцев
2	День	прибавл.: 0,25 сут./бит, обратн. сдвиг: 0 сут. (см. ПРИМЕЧАНИЕ ниже)	от 0,25 до 31,75 суток
3	Год	прибавл.: 1 год/бит, обратн. сдвиг: +1985 год (см. ПРИМЕЧАНИЕ ниже)	1985 - 2235 год

ПРИМЕЧАНИЕ относительно использования параметра "День":
значение даты, равное 0, информации не содержит. Значения 1, 2, 3, и 4 используются для указания первого дня месяца; 5, 6, 7, и 8 – для указания второго дня месяца, и т.д.
Данный параметр никак не влияет на параметр "часы" в таблице выше и не изменяет его.

ПРИМЕЧАНИЕ относительно использования параметра "Год":
значение года, равное 0, соответствует 1985 году; значение, равное 1, –1986 году, и т.д.

CPR_078 В таблице 42 подробно указаны форматы различных байтов параметра VehicleRegistrationNumber.

Таблица 42

Подробное описание формата VehicleRegistrationNumber (значение recordDataIdentifier # F97E)

Байт	Определение параметра	Разрешение	Диапазон
1	Кодовая страница (согласно определению, содержащемуся в подразделе I)	ASCII	от 01 до 0A
2 – 14	Регистрационный номер транспортного средства (согласно определению, содержащемуся в подразделе I)	ASCII	ASCII

ПОДРАЗДЕЛ IX

ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА

ПЕРЕЧЕНЬ МИНИМАЛЬНЫХ ТРЕБУЕМЫХ ИСПЫТАНИЙ

СОДЕРЖАНИЕ

1. Введение

1.1 Официальное утверждение типа

Процедура официального утверждения типа регистрирующей аппаратуры (либо ее компонентов) или карточек тахографа состоит из следующих основных частей:

сертификация защиты, проводимая органом по общей оценке безопасности информационной технологии безопасности в целях подтверждения соответствия тому или иному из контрольных показателей защиты, которые должны полностью отвечать положениям подраздела X настоящего добавления;

- сертификация функциональности, проводимая органом Договаривающейся стороны в целях подтверждения того, что испытываемое изделие соответствует требованиям настоящего добавления по набору выполняемых функций, точности измерений и допустимым условиям эксплуатации;

- сертификация эксплуатационной совместимости, проводимая компетентным органом в целях подтверждения полной эксплуатационной совместимости контрольного устройства (или карточки тахографа) с необходимыми моделями карточек тахографа (или контрольных устройств) (см. главу VIII настоящего добавления).

В данном подразделе содержится перечень минимальных рабочих испытаний, которые должны быть проведены ответственным за это органом Договаривающейся стороны, а также испытаний на совместимость, которые должен провести соответствующий компетентный орган. Процедуры проведения этих испытаний и их виды дополнительно не конкретизируются.

Аспекты, связанные с сертификацией защиты, в настоящем подразделе не рассматриваются. Если какие-либо из испытаний, необходимых для официального утверждения типа, уже были проведены в процессе аттестации и сертификации систем защиты, то повторное их проведение не требуется. В таких случаях можно ограничиться проверкой результатов этих испытаний. Характеристики, которые должны испытываться при сертификации защиты (или которые тесно связаны с проводимыми при этом испытаниями) в справочных целях помечены в настоящем подразделе знаком "*".

Официальное утверждение типа датчика движения и бортового устройства рассматривается в настоящем подразделе отдельно, так как речь идет о разных компонентах контрольного устройства. Эксплуатационная совместимость каждой модели датчика движения с каждой моделью бортового устройства необязательна; поэтому тип датчика движения может быть утвержден только в сочетании с соответствующим типом бортового устройства, и наоборот.

1.2 Источники

При подготовке данного подраздела использовались следующие источники:

IEC 68-2-1 Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание А. Холод. 1990 год + Поправка 2, 1994 год.

IEC 68-2-2 Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание В. Сухое тепло. 1974 + Поправка 2, 1994 год.

IEC 68-2-6 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Fc и руководство. Вибрация (синусоидальная). Издание шестое, 1985 год.

IEC 68-2-14 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание N. Колебания температуры. Изменение 1, 1986 год.

IEC 68-2-27 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Ea и руководство. Ударные воздействия. Издание третье, 1987 год.

IEC 68-2-30 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Db и руководство. Влажное тепло, циклический режим (12 + 12 - часовой цикл). Изменение 1, 1985 год.

IEC 68-2-35 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Fda. Широкополосная случайная вибрация. Высокая воспроизводимость. Изменение 1, 1983 год.

IEC 529 Степени защиты, обеспечиваемой корпусами изделий (код IP). Издание второе, 1989 год.

IEC 61000-4-2 Совместимость электромагнитная (EMC). Методы испытаний и измерений. Испытание на устойчивость к электростатическому разряду. 1995 год/Поправка 1, 1998 год.

ISO 7637-1 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 1. Легковые автомобили и автомобили малой грузоподъемности для коммерческих перевозок с номинальным напряжением электропитания 12 В. Распространение помех, вызываемых переходными процессами, только по линиям, обеспечивающим электропитание. Издание второе, 1990 год.

ISO 7637-2 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 2. Автомобили для коммерческих перевозок с номинальным напряжением электропитания 24 В. Распространение помех, вызываемых переходными процессами, только по линиям, обеспечивающим электропитание. Издание первое, 1990 год.

ISO 7637-3 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 3. Автомобили с номинальным напряжением электропитания 12 В или 24 В. Распространение помех, вызываемых переходными процессами, обусловленными емкостным или индуктивным соединением, по линиям, не обеспечивающим электропитание. Издание первое. 1995 год + Поправка 1, 1995 год.

ISO/IEC 7816-1 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 1. Физические характеристики. Издание первое, 1998 год.

ISO/IEC 7816-2 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 2. Размеры и расположение контактов. Издание первое, 1999 год.

ISO/IEC 7816-3 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 3. Электронные сигналы и протоколы передачи. Издание второе, 1997 год.

ISO/IEC 10373 Карточки идентификационные. Методы испытаний. Издание первое, 1993 год.

2. Рабочие испытания бортового устройства

№	Вид испытания	Описание	Предъявляемые требования
1	**Административная проверка**		
1.1	Документация	Правильность оформления документации	
1.2	Результаты испытаний, проведеннных изготовителем	Результаты испытаний, проводившихся изготовителем при сборке. Проверка технических характеристик по документам.	070, 071, 073
2	**Визуальный осмотр**		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		168, 169
2.3	Материалы		163 - 167
2.4	Пломбировка		251
2.5	Внешние интерфейсы		
3	**Рабочие испытания**		
3.1	Предусмотренные функции		002, 004, 244
3.2	Режимы работы		006*, 007*, 008*, 009*, 106, 107
3.3	Функции и права доступа к данным		010*, 011*, 240, 246, 247
3.4	Контроль за вводом и извлечением карточек		013, 014, 015*, 016*, 106
3.5	Измерение скорости и пробега		017 - 026
3.6	Отсчет времени (испытание проводится при 20°C)		027 - 032
3.7	Контроль за деятельностью водителей		033 - 043, 106
3.8	Контроль за управлением		044, 045, 106
3.9	Ввод данных водителем вручную		046 - 050b
3.10	Установка блокировки предприятием		051 - 055
3.11	Мониторинг контрольных операций		056, 057
3.12	Обнаружение событий и/или неисправностей		059 - 069, 106
3.13	Идентификационные данные аппаратуры		075*, 076*, 079
3.14	Данные о вводе и извлечении карточек водителя		081* - 083*
3.15	Данные о деятельности водителей		084* - 086*
3.16	Данные о географических пунктах		087* - 089*

№	Вид испытания	Описание	Предъявляемые требования
3.17	Показания счетчика пробега		090* - 092*
3.18	Подробные данные о скоростном режиме		093*
3.19	Данные о событиях		094*, 095
3.20	Данные о неисправностях		096*
3.21	Данные калибровки		097*, 098*
3.22	Данные о корректировке времени		100*, 101*
3.23	Данные о контрольных операциях		102*, 103*
3.24	Данные о блокировках, установленных предприятием		104*
3.25	Данные об операциях по загрузке данных		105*
3.26	Данные об особых ситуациях		105a*, 105b*
3.27	Регистрация и сохранение данных на карточках тахографа		108, 109*, 109a*, 110*, 111, 112
3.28	Индикация данных на дисплее		072, 106, 113 - 128, PIC_001, DIS_001
3.29	Распечатка данных		072, 106, 129 - 138, PIC_001, PRT_001 - PRT_012
3.30	Сигналы предупреждения		106, 139 - 148, PIC_001
3.31	Сохранение данных на внешнем носителе		072, 106, 149 - 151
3.32	Вывод данных на дополнительные внешние устройства		152, 153
3.33	Калибровка		154*, 155*, 156*, 245
3.34	Корректировка времени		157*, 158*
3.35	Отсутствие помех при выполнении дополнительных функций		003, 269
4	**Испытания на воздействие внешних факторов**		
4.1	Температура	Проверка работоспособности согласно: - стандарту IEC 68-2-1, испытание Ad: продолжительность испытания - 72 часа при нижней предельной температуре (-20°C); 1 час во включенном состоянии - 1 час в выключенном состоянии; - стандарту IEC 68-2-2, испытание Bd: продолжительность испытания -	

№	Вид испытания	Описание	Предъявляемые требования
		72 часа при верхней предельной температуре (+70°C); 1 час во включенном состоянии - 1 час в выключенном состоянии. Термоциклирование: проверка способности бортового устройства выдерживать резкие перепады окружающей температуры согласно стандарту IEC 68-2-14 (испытание Na): 20 циклов с изменением температуры от нижнего (-20°C) до верхнего (+70°C) предела в каждом цикле, с выдержкой в течение 2 часов соответственно при минимальной и максимальной температуре. Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при минимальной и максимальной предельной температуре, а также на протяжении термоциклов.	
4.2	Испытания во влажной среде	Проверка способности бортового устройства выдерживать циклические колебания температуры во влажной среде согласно стандарту IEC 68-2-30, испытание Db: шесть 24-часовых циклов с изменением температуры от +25°C до + 55°C в каждом цикле и относительной влажностью воздуха, равной 97% при + 25°C и эквивалентной 93% при +55°C.	160
4.3	Вибростойкость	1. Синусоидальные вибрации: Проверка способности бортового устройства выдерживать синусоидальные вибрации со следующими характеристиками: постоянное смещение (пиковая амплитуда 10 мм) в диапазоне 5-11 Гц; постоянное ускорение (5 g) в диапазоне 11–300 Гц. Соответствие данному	163

№	Вид испытания	Описание	Предъявляемые требования
		требованию проверяется согласно стандарту IEC 68–2–6, испытание Fc минимальной продолжительностью 3x12 часов (по 12 часов на каждую ось). 2. Случайные колебания: Проверка способности бортового устройства выдерживать случайные колебания со следующими характеристиками: частота 5–150 Гц, уровень 0,02 g^2/Гц. Соответствие данному требованию проверяется согласно стандарту IEC 68–2–35, испытание Ffda минимальной продолжительностью 3x12 часов (12 часов на каждую ось), 1 час во включенном состоянии – 1 час в выключенном состоянии. Два вышеуказанных испытания проводятся с использованием двух разных экземпляров устройства испытываемого образца.	
4.4	Защита от попадания воды и посторонних предметов	Индекс защищенности согласно IEC 529 для бортового устройства, установленного на транспортном средстве, должен составлять не менее IP 40 в реальных условиях эксплуатации.	164, 165
4.5	Защита от перегрузок по напряжению	Проверка способности бортового устройства выдерживать следующее напряжение в цепи питания: в варианте, рассчитанном на 24 В: 34 В при +40°C в течение 1 часа; в варианте, рассчитанном на 12 В: 17 В при +40°C в течение 1 часа.	161
4.6	Защита от несоблюдения полярности	Проверка способности бортового устройства выдерживать подключение к источнику питания противоположной полярности.	161

№	Вид испытания	Описание	Предъявляемые требования
4.7	Защита от короткого замыкания	Проверка защищенности входного и выходного сигналов от короткого замыкания на источник питания и на массу.	161
5.	**Испытания на электромагнитную совместимость**		
5.1	Излучения и электромагнитная защищенность	Соответствие Правилам ЕЭК ООН N°10	162
5.2	Устойчивость к электростатическому разряду	Соответствие стандарту IEC 61000–4–2, ±2 кВ (уровень 1)	162
5.3	Невосприимчивость к быстрым переходным процессам в цепи питания	В варианте, рассчитанном на 24 В – соответствие стандарту ISO 7637–2: импульс 1a: Vs=–100 В, Ri=10 Ом импульс 2: Vs=+100 В, Ri=10 Ом импульс 3a: Vs=–100 В, Ri=50 Ом импульс 3b: Vs=+100 В, Ri=50 Ом импульс 4: Vs=–16 В Va=–12 В, t6=100 мс импульс 5: Vs=+120 В, Ri=2,2 Ом, в варианте, рассчитанном на 12 В – соответствие стандарту ISO 7637-1: импульс 1: Vs=–100 В, Ri=10 Ом импульс 2: Vs=+100 В, Ri=10 Ом импульс 3a: Vs=–100 В, Ri=50 Ом импульс 3b: Vs=+100 В, Ri=50 Ом импульс 4: Vs=–6 В Va=–5 В, t6=15 мс импульс 5: Vs=+65 В, Ri=3 Ом, Импульс 5 используется только при испытании бортовых устройств для установки на транспортных средствах, не оборудованных единой внешней защитой от сброса нагрузки генератора.	162

3. Рабочие испытания датчика движения

No	Вид испытания	Описание	Предъявляемые требования
1.	**Административная проверка**		
1.1	Документация	Правильность оформления документации	
2.	**Визуальный осмотр**		
2.1	Соответствие документации		
2.2	Идентификация / маркировка		169, 170
2.3	Материалы		163–167
2.4	Наложение пломб		251
3.	**Рабочие испытания**		
3.1	Идентификационные данные датчика		077*
3.2	Подсоединение датчика движения к бортовому устройству		099*, 155
3.3	Регистрация движения Точность измерения параметров движения		022–026
4.	**Испытания на воздействие внешних факторов**		
4.1	Рабочая температура	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) в температурном диапазоне [–40°C; +135°C] согласно: - стандарту IEC 68–2–1, испытание Ad: продолжительность испытания – 96 часов при нижней предельной температуре To_{min}, - стандарту IEC 68–2–2, испытание Bd: продолжительность испытания – 96 часов при верхней предельной температуре $To_{max.}$	159
4.2	Термоциклиро-вание	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68–2–14,	159

No	Вид испытания	Описание	Предъявляемые требования
		испытание Na: 20 циклов с изменением температуры от нижнего (–40°C) до верхнего (+135°C) предела в каждом цикле, с выдержкой в течение 2 часов соответственно при минимальной и максимальной температуре. Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3.3) при минимальной и максимальной температуре, а также на протяжении термоциклов.	
4.3	Циклические испытания во влажной среде	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68–2–30, испытание Db: шесть 24–часовых циклов с изменением температуры от +25°C до +55°C в каждом цикле и относительной влажностью воздуха, равной 97% при +25°C и эквивалентной 93% при +55°C.	160
4.4	Вибростойкость	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68–2–6, испытание Fc, продолжительность испытания не менее 100 частотных циклов: постоянное смещение (амплитуда 1,5 мм) в диапазоне 10–57 Гц; постоянное ускорение (20 g) в диапазоне 57-500 Гц.	163
4.5	Ударопрочность	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68–2–27, испытание Ea: по 3 ударных импульса в каждом из двух направлений по каждой из 3 осей.	163
4.6	Защита от попадания воды и посторонних	Индекс защищенности согласно IEC 529 для датчика движения, установленного на	165

No	Вид испытания	Описание	Предъявляемые требования
	предметов	транспортном средстве, должен составлять не менее IP 64 в реальных условиях эксплуатации.	
4.7	Защита от несоблюдения полярности	Проверка способности датчика движения выдерживать подключение к источнику питания противоположной полярности.	161
4.8	Защита от короткого замыкания	Проверка защищенности входного и выходного сигналов от короткого замыкания на источник питания и на массу.	161
5.	**Испытания на электромагнитную совместимость**		
5.1	Излучения и электромагнит-ная защищенность	Проверка соответствия Правилам ЕЭК ООН N°10	162
5.2	Устойчивость к электростати-ческому разряду	Соответствие стандарту IEC 61000–4–2, ±2 кВ (уровень 1)	162
5.3	Невосприимчи-вость к быстрым переходным процессам на линиях передачи данных	Соответствие стандарту ISO7637–3 (уровень III)	162

4. Рабочие испытания карточек тахографа

№	Вид испытания	Описание	Предъявляемые требования
1.	**Административная проверка**		
1.1	Документация	Проверка правильности оформления документации	
2.	**Визуальный осмотр**		
2.1		Проверка правильности нанесения на карточку всех элементов защиты и визуальной информации и их соответствия установленным требованиям	171 - 181
3.	**Физический контроль**		

№	Вид испытания	Описание	Предъявляемые требования
3.1		Проверка размеров карточки и расположения контактов	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Тестирование протоколов**		
4.1	ATR	Проверка совместимости ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Проверка совместимости протокола T=0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS	Проверка совместимости команды PTS путем задания протокола T=1 при исходном T=0	ISO/IEC 7816-3 TCS 309 - 311
4.4	T=1	Проверка совместимости протокола T=1	ISO/IEC 7816-3 TCS 303, / 306
5.	**Структура данных на карточке**		
5.1		Подтверждение соответствия файловой структуры на карточке путем проверки наличия обязательных файлов и тестирования условий доступа к ним	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Рабочие испытания**		
6.1	Обработка данных в обычном режиме	Как минимум однократное тестирование каждого допустимого использования каждой команды (например, проверка исполнения команды UPDATE BINARY при CLA = "00", CLA = "0C" и при разных значениях параметров P1, P2 и Lc). Подтверждение фактического выполнения карточкой соответствующих операций (например, путем считки файла после исполнения команды на его обработку)	TCS 313 - TCS 379
6.2	Сообщения об ошибках	Как минимум однократное тестирование каждого сообщения об ошибке (из числа указанных в подразделе 2) при исполнении каждой команды. Как минимум однократное тестирование на общую ошибку каждого вида (кроме ошибок серии **'6400'** (искажение данных), которые тестируются при сертификации систем защиты)	

№	Вид испытания	Описание	Предъявляемые требования
7.	**Испытания на воздействие внешних факторов**		
7.1		Подтверждение способности карточек к функционированию в предельных режимах, определенных согласно стандарту ISO/IEC 10373	185 - 188 ISO/IEC 7816-1

5. Испытания на эксплуатационную совместимость

№	Вид испытания	Описание
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации бортового устройства и карточки тахографа
2	Проверка записи/считки данных	Отработка типового сценария функционирования бортового устройства. Сценарий должен быть выбран с учетом типа тестируемой карточки и включать операции по записи данных в максимально возможном числе элементарных файлов на карточке. Загрузка данных с карточки для проверки наличия и правильности всех соответствующих записей данных. Распечатка данных с карточки за соответствующие сутки для проверки возможности правильной считки всех соответствующих записей

ПОДРАЗДЕЛ X

ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

СОДЕРЖАНИЕ (продолжение)

О содержании настоящего подраздела

В настоящем подразделе содержится минимальный перечень обязательных контрольных показателей защиты датчиков движения, бортовых устройств и карточек тахографа.

В целях выработки контрольных показателей защиты соответствующих изделий, на основании которых им могут присваиваться сертификаты защиты, изготовители этих изделий должны по мере необходимости уточнять и дополнять соответствующую документацию, не изменяя и не удаляя при этом существующих определений опасностей, а также целей, процедурных средств и защитных функций.

Общие контрольные показатели ЗАЩИТЫ датчика движения

1. Введение

В настоящем документе приводится описание датчика движения с перечислением опасностей, которым он должен противостоять, и целей, на которые должна быть направлена его защита. В нем указаны необходимые для этого защитные функции, минимальный уровень заданной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1B. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1B. При отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1B следует руководствоваться основным текстом добавления 1B.

Требования основного текста добавления 1B, для которых не определены контрольные показатели, защитными функциями не охватываются.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ Аттестуемое изделие
БУ Бортовое устройство
ЗФ Защитная функция
ROM Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Устройство	Устройство, подключенное к датчику движения.
Данные о движении	Данные, которыми датчик обменивается с БУ, позволяющие определять скорость и пробег транспортного средства.
Физически разделенные	Физические детали датчика движения, установленные на транспортном средстве в разных местах, в отличие от компоненты физических деталей, сгруппированных внутри корпуса датчика.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Человек, пользующийся датчиком движения (за исключением случая "пользователь данных").
Пользовательские данные	Любые данные помимо данных о движении и данных защиты, регистрируемые и сохраняемые датчиком движения.

2.3 Источники

ITSEC	ИТСЕК Критерии оценки безопасности информационной технологии, 1991 год.

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации датчика движения

Датчик движения предназначен для установки на автотранспортных средствах. Он служит для получения и передачи на БУ криптозащищенных данных о движении, позволяющих определять скорость и пробег транспортного средства.

Датчик движения механически сопряжен с движущейся деталью транспортного средства, по движению которой может измеряться скорость транспортного средства или пройденное им расстояние. Он может располагаться в коробке передач или в любом другом месте на транспортном средстве.

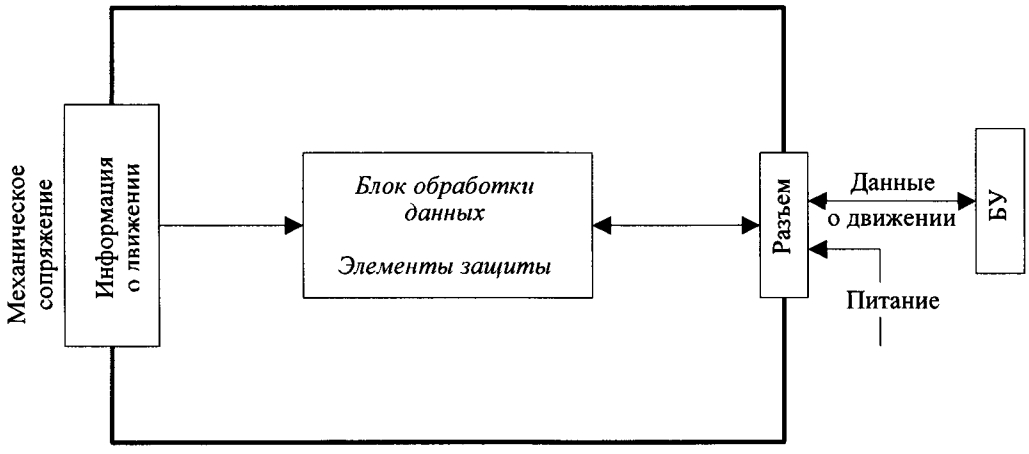
В рабочем режиме датчик движения должен быть подключен к БУ.

В административных целях он также может подключаться к другому оборудованию (*по усмотрению изготовителя*).

Типичная схема датчика движения представлена ниже.

Рис. 1

Обобщенная схема датчика движения

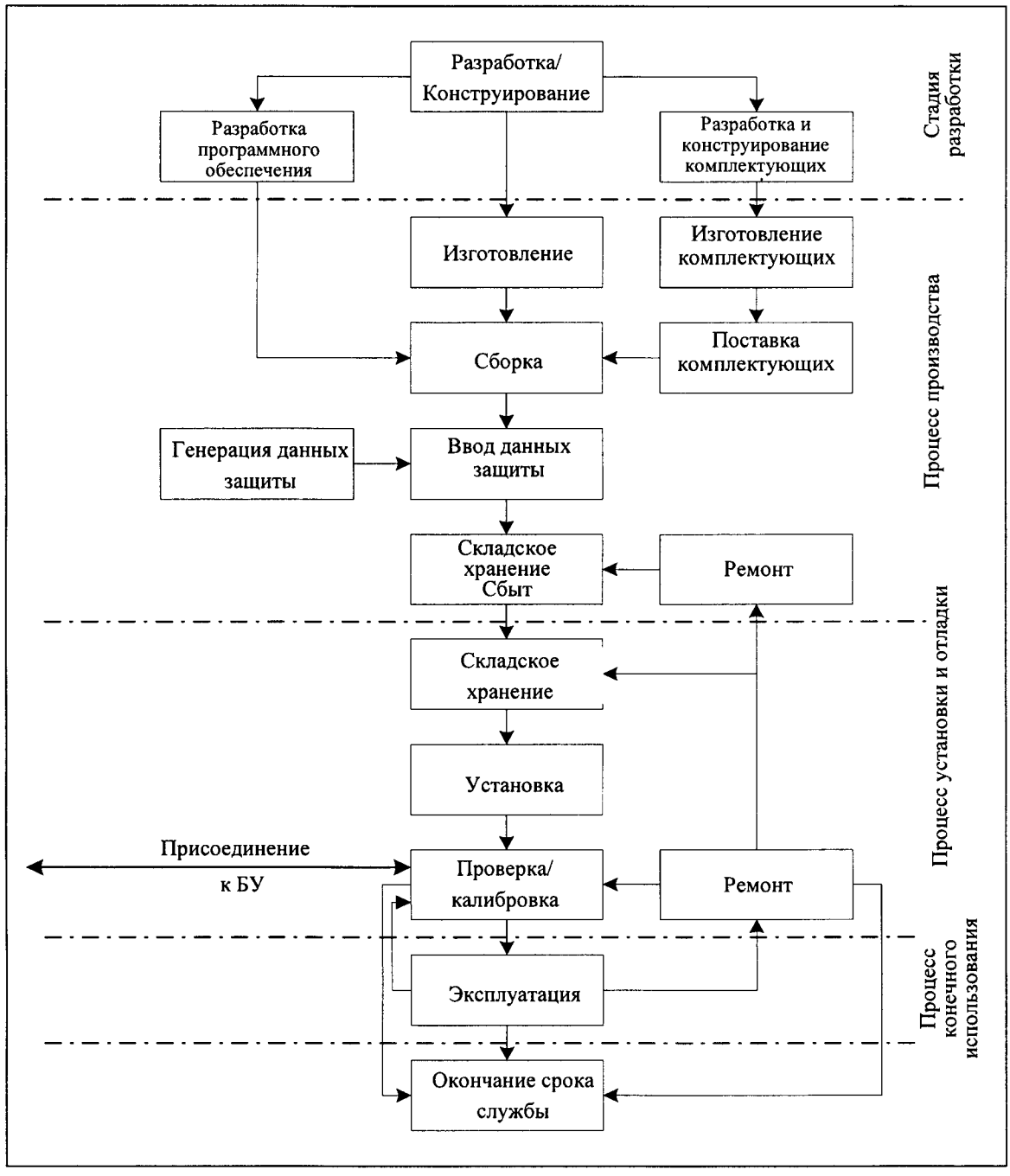


3.2 Жизненный цикл датчика движения

Схема жизненного цикла датчика движения представлена ниже.

Рис. 2

Обобщенная схема жизненного цикла датчика движения



3.3 Опасности

Настоящий пункт содержит описание опасностей, которым может подвергаться датчик движения.

3.3.1 Опасности, связанные с нарушением режима контроля за доступом

O: Доступ	Пользователи могут пытаться получить доступ к не предназначенным для них функциям.

3.3.2 Опасности, связанные с конструкцией датчика

O: Сбои в работе	Отказы аппаратуры, сбои в функционировании программного обеспечения или процедурах обмена данными могут привести к непредвиденным ситуациям и ослабить защиту датчика движения.
O: Испытания	Защита датчика движения может быть нарушена в результате использования неотключенных тест-режимов или имеющихся "обходных путей" доступа.
O: Конструкция	Пользователи могут пытаться незаконным путем добыть сведения о конструкции датчика – будь то у изготовителя (хищение, подкуп и т.п.) или путем инженерного анализа.

3.3.3 Опасности в процессе эксплуатации

O: Внешние_факторы	Для преодоления защиты датчика движения пользователи могут пытаться использовать воздействие внешних факторов (термических, электромагнитных, оптических, химических, механических и т.д.).
O: Аппаратура	Пользователи могут пытаться внести физические изменения в конструкцию датчика движения.

О: Механический_источник_данных	Пользователи могут пытаться нарушить механическое сопряжение датчика с ходовой частью (например, соединение с коробкой передач).
О: Данные_о_движении	Пользователи могут пытаться исказить данные о движении транспортного средства (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).
О: Источник_питания	Пользователи могут пытаться нейтрализовать защиту датчика движения путем изменения параметров тока в цепи питания (отключение, ослабление, усиление).
О: Данные_защиты	Пользователи могут пытаться получить несанкционированный доступ к данным защиты датчика в процессе генерации этих данных, их передачи или хранения аппаратурой.
О: Программное_обеспечение	Пользователи могут пытаться внести изменения в программное обеспечение датчика движения.
О: Сохраненные_данные	Пользователи могут пытаться изменить сохраненные данные (данные защиты или пользовательские данные).

3.4 Цели защиты

Основная цель защиты системы цифрового тахографа заключается в следующем:

Ц: Основная	Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Соответственно цель защиты датчика движения, способствующая достижению вышеупомянутой основной цели, заключается в следующем:

Ц: Основная_(датчик)	Данные, передаваемые датчиком движения, должны поступать на БУ, позволяя ему полностью и точно регистрировать скорость движения и пробег транспортного средства.

3.5 Цели защиты в области информационных технологий

Конкретные цели защиты датчика движения в области ИТ, способствующие достижению главной цели защиты датчика, заключаются в следующем:

Ц: Доступ	Датчик движения должен контролировать доступ подключенных к нему устройств к функциям и данным.
Ц: Контроль	Датчик движения должен обеспечивать контроль за попытками нарушения его защиты и отслеживать их связь с соответствующими устройствами.
Ц: Аутентификация	Датчик движения должен производить аутентификацию подключенных к нему устройств.
Ц: Обработка	Датчик движения должен обеспечивать точность обработки поступающей информации, на основании которой рассчитываются данные о движении.
Ц: Надежность	Датчик движения должен функционировать надежно.
Ц: Защищенный_обмен_данными	Датчик движения должен обеспечивать защиту данных, которыми он обменивается с БУ.

3.6 Технические, организационные и процедурные средства

В данном пункте излагаются технические, организационные и процедурные требования, связанные с защитой датчика движения.

3.6.1 Конструкция аппаратуры

С: Разработка	Разработчики датчиков движения должны заботиться об обеспечении информационной безопасности при распределении функций на стадии конструирования.
С: Изготовление	Изготовители датчиков движения должны заботиться об обеспечении информационной безопасности при распределении функций на стадии производства, а в процессе непосредственного изготовления датчиков предохранять их от технического вмешательства, способного нарушить информационную защиту.

3.6.2 Поставка аппаратуры

С: Поставка	Изготовители датчиков движения, изготовители транспортных средств, сервисные центры и мастерские должны заботиться об обеспечении информационной безопасности на всех этапах работы с датчиком движения

3.6.3 Генерация, передача и ввод данных защиты

С-З: Генерация_данных	Доступ к алгоритмам генерации данных защиты должны иметь только уполномоченные и пользующиеся доверием лица.
С-З: Перенос_данных_защиты	Генерация и передача данных защиты, а также их ввод в датчик движения должны производиться с обеспечением должной конфиденциальности и целостности этих данных.

3.6.4 Установка, калибровка и проверка контрольного устройства

С: Утвержденные_мастерские	Установка, калибровка и ремонт контрольных устройств должны производиться только в

	сервисных центрах или мастерских, пользующихся доверием и допущенных к таким работам.
C: Механическое_сопряжение	Должны быть предусмотрены средства выявления попыток физического нарушения механического сопряжения датчика с ходовой частью (например, пломбы).
C: Регулярные_проверки	Контрольное устройство должно регулярно проходить проверку и калибровку.

3.6.5 Правоприменительный контроль

C: Контроль	Правоохранительный контроль должен осуществляться как на регулярной, так и на выборочной основе и включать контрольную проверку систем защиты.

3.6.6 Новые версии программного обеспечения

C: Новое_п/о	Перед установкой на датчик движения новые версии программного обеспечения должны получить сертификат безопасности.

4. Защитные функции

4.1 Идентификация и аутентификация

UIA_101 При каждом взаимодействии с другими устройствами датчик движения должен иметь возможность идентифицировать подключенное устройство.

UIA_102 Идентификационные данные подключенного устройства состоят из:

- указания категории, к которой относится данное устройство, а именно:
  - БУ;
  - административные устройства;
  - прочие устройства;
- собственного идентификатора устройства (только для БУ).

UIA_103 Идентификатор подключенного БУ состоит из номера официального утверждения данного образца БУ и серийного номера БУ.

UIA_104 Датчик движения должен иметь возможность аутентифицировать любое подключенное к нему БУ или административное устройство:

- при подключении устройства;
- при восстановлении подачи питания.

UIA_105 Датчик движения должен иметь возможность периодически производить повторную аутентификацию БУ, к которому он подключен.

UIA_106 Датчик движения должен выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_107 После регистрации (*количество определяется изготовителем, но не должно превышать 20*) неудачных попыток аутентификации подряд защитные функции должны обеспечивать:

- генерацию контрольной записи о событии;
- выдачу предупреждения на подключенное устройство;
- продолжение экспорта данных о движении в незащищенном режиме.

4.2 Контроль за доступом

Средства контроля за доступом обеспечивают возможность считывания, ввода или изменения информации в АИ только для уполномоченных на то лиц.

4.2.1 Режим контроля за доступом

ACC_101 Датчик движения должен обеспечивать контроль прав доступа к функциям и данным.

4.2.2 Права доступа к данным

ACC_102 Должна быть предусмотрена лишь однократная возможность сохранения идентификационных данных датчика движения (требование 078).

ACC_103 Датчик движения должен принимать и/или сохранять пользовательские данные только при их поступлении от аутентифицированных устройств.

ACC_104 Датчик движения должен обеспечивать соответствующий режим доступа к функциям считывания и сохранения данных защиты.

4.2.3 Структура файлов и условия доступа к ним

ACC_105 Структура файлов приложений и файлов данных и условия доступа к ним определяются в процессе изготовления и защищаются от любого последующего изменения или удаления.

4.3 Учет

ACT_101 В памяти датчика движения должны храниться идентификационные данные этого датчика (требование 077).

ACT_102 В памяти датчика движения должны храниться данные об установке (требование 099).

ACT_103 Должна быть предусмотрена возможность передачи учетных данных с датчика движения на аутентифицированные устройства по их запросу.

4.4 Контроль

AUD_101 Датчик движения должен генерировать контрольные записи о событиях, способных нарушить его защиту.

AUD_102 К событиям, затрагивающим защиту датчика движения, относятся:

- попытки преодоления защиты:
  - отрицательный результат аутентификации;
  - ошибка при проверке целостности сохраненных данных;
  - ошибка при внутренней передаче данных;
  - несанкционированное вскрытие корпуса;
  - умышленная порча оборудования;
- отказ датчика.

AUD_103 Надзорные записи должны включать следующие данные:

- дата и время события;
- тип события;
- идентификационные данные подключенного устройства.

Если необходимые данные отсутствуют, должно использоваться соответствующее обозначение по умолчанию (*определяется изготовителем*).

AUD_104 Генерируемые датчиком движения контрольные записи передаются на БУ в момент их генерации и могут также сохраняться в памяти датчика.

AUD_105 Если контрольные записи сохраняются в памяти датчика движения, то должно быть обеспечено хранение 20 таких записей даже после того, как емкость выделенной для них памяти будет исчерпана, с возможностью выдачи сохраненных записей на аутентифицированные устройства по их запросу.

4.5 Достоверность

4.5.1 Правила контроля за поступлением информации

ACR_101 Датчик движения должен воспринимать и обрабатывать данные о движении, поступающие только через устройства его механического сопряжения с ходовой частью.

4.5.2 Внутренняя передача данных

Требования настоящего пункта применяются лишь к датчикам движения, в которых используются физически разделенные компоненты.

ACR_102 Если между физически разделенными компонентами датчика движения передаются данные, то эти данные должны быть защищены от изменения.

ACR_103 При обнаружении ошибки передачи данных в процессе их внутренней передачи передача осуществляется повторно, а защитная функция (ЗФ) генерирует контрольную запись об этом событии.

4.5.3 Целостность сохраненных данных

ACR_104 Датчик движения должен проверять целостность хранящихся в его памяти пользовательских данных.

ACR_105 В случае ошибки при проверке неискаженности сохраненных пользовательских данных защитная функция генерирует надзорную запись.

4.6 Надежность функционирования

4.6.1 Испытания

RLB_101 Все команды, функции и контакты, предназначенные исключительно для тестирования датчика на стадии производства, перед выпуском готового изделия блокируются или удаляются. Возможность их восстановления для последующего использования должна быть исключена.

RLB_102 При включении, а также в процессе работы в обычном режиме датчик движения должен производить самопроверку для подтверждения того, что он функционирует нормально. При самопроверке датчика движения проверяются целостность данных защиты и хранящихся в памяти исполнимых команд (если они не сохранены в ROM).

RLB_103 В случае обнаружения внутренних неполадок в процессе самопроверки система защиты генерирует отчетную запись (сбой в работе датчика).

4.6.2 Программное обеспечение

RLB_104 Возможность анализа или отладки программного обеспечения датчика движения в полевых условиях должна быть исключена.

RLB_105 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.6.3 Физическая защита

RLB_106 Если конструкция датчика движения допускает вскрытие его корпуса, то датчик должен быть способен регистрировать любое такое вскрытие и сохранять эту способность даже при отключении от внешнего источника питания в течение как минимум шести месяцев. При этом ЗФ генерирует отчетную запись о данном событии (допускается возможность генерации и сохранения такой записи после возобновления питания).

Если конструкция датчика движения не предусматривает вскрытия корпуса, то она должна обеспечивать легкое обнаружение следов физического воздействия (например, при внешнем осмотре).

RLB_107 Датчик движения должен быть способен регистрировать конкретные (*определяемые заводом-изготовителем*) виды умышленной порчи оборудования.

RLB_108 В вышеупомянутых случаях ЗФ должна генерировать контрольную запись, а датчик движения должен: (*определяется заводом-изготовителем*).

4.6.4 Прекращение электропитания

RLB_109 Защита датчика движения не должна нарушаться при отключении от источника питания или при изменениях параметров тока в цепи питания.

4.6.5 Перезапуск

RLB_110 В случае прекращения питания, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, датчик движения полностью перезапускается.

4.6.6 Доступность данных

RLB_111 Датчик движения должен предоставлять доступ к имеющимся ресурсам данных по мере необходимости, обеспечивать отсутствие неоправданных обращений к ресурсам и удалять ненужные данные.

4.6.7 Многоцелевое использование

RLB_112 Если датчик движения используется для других целей, помимо обеспечения работы тахографа, то все соответствующие приложения должны быть физически и/или логически отделены друг от друга. Данные защиты не должны быть общими для этих приложений. Одновременное выполнение более чем одной функции не допускается.

4.7 Обмен данными

DEX_101 Датчик движения выдает данные о движении транспортного средства на БУ с соответствующими атрибутами защиты, позволяющими БУ проверять их целостность и подлинность.

4.8 Криптографическая защита

Требования данного пункта применяются лишь в необходимых случаях в зависимости от используемых механизмов защиты и примененных заводом-изготовителем технических решений.

CSP_101 Любые криптографические операции, выполняемые датчиком движения, должны соответствовать заданному алгоритму при заданном размере ключа.

CSP_102 Если датчик движения генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей.

CSP_103 Если датчик движения рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки криптографических ключей.

CSP_104 Если датчик движения получает доступ к криптографическим ключам, то это должно соответствовать установленному порядку доступа к криптографическим ключам.

CSP_105 Если датчик движения уничтожает криптографические ключи, то это должно делаться в соответствии с установленными методами уничтожения криптографических ключей.

5. Определение механизмов защиты

Механизмы защиты, обеспечивающие выполнение защитных функций датчика движения, определяются заводами-изготовителями датчиков движения.

6. Минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты датчика движения должна соответствовать **Высокому** уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты датчика движения по системе ITSEC должна соответствовать уровню **E3** (согласно определению, содержащемуся в [ITSEC]).

8. Обоснование

В нижеследующей таблице приводится обоснование ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

	Опасности												**ИТ-цели**					
	Доступ	**Сбои в работе**	**Испытания**	**Конструкция**	**Внешние_факторы**	**Аппаратная часть**	**Механическая_часть**	**Данные_о_движении**	**Питание**	**Данные_защиты**	**Программное_обеспечение**	**Сохраненные_данные**	**Доступ**	**Контроль**	**Аутентификация**	**Обработка**	**Надежность**	**Криптообмен_данными**
Технические, организационные и процедурные средства																		
Разработка		x	x	x														
Изготовление			x	x														
Поставка						x					x	x						
Генерация данных защиты										x								
Передача данных защиты										x								
Утвержденные мастерские							x											
Механическое сопряжение							x											
Регулярная инспекция						x	x		x		x							
Правоприменительный контроль					x	x	x		x	x	x							
Новые версии п/о											x							
Защитные функции																		
Идентификация и аутентификация																		
UIA_101 Идентификация устройств	x							x					x		x			x

	Опасности												ИТ-цели					
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
UIA_102 Идентификационные данные устройств	x												x		x			
UIA_103 Идент. данные БУ														x				
UIA_104 Аутентификация устройств	x							x					x		x			x
UIA_105 Повторная аутентификация	x							x					x		x			x
UIA_106 Нефальсифициру-емая аутентификация	x							x					x		x			
UIA_107 Отрицательная аутентификация								x						x			x	
Контроль доступа																		
ACC_101 Режим контроля за доступом	x									x		x	x					
ACC_102 ID датчика движения												x	x					
ACC_103 Пользовательские данные												x	x					
ACC_104 Данные защиты										x		x	x					
ACC_105 Структура файлов и условия доступа	x									x		x	x					
Отчетность																		
ACT_101 Идент. данные датчика движения														x				
ACT_102 Данные о подсоединении														x				
ACT_103 Учетные данные														x				

	Опасности												ИТ-цели					
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
Надзор																		
AUD_101 Контрольные записи														x				
AUD_102 Список зафиксированных подконтрольных событий	x				x	x						x		x				
AUD_103 Данные контроля														x				
AUD_104 Средства контроля														x				
AUD_105 Хранение контрольных записей														x				
Достоверность																		
ACR_101 Правила контроля за поступлением информации								x								x	x	
ACR_102 Внутр. передача																x	x	
ACR_103 Внутр. передача														x				
ACR_104 Целостность сохраненных данных												x					x	
ACR_105 Целостность сохраненных данных												x		x				
Надежность																		
RLB_101 Заводские испытания			x	x													x	
RLB_102 Самопроверка		x				x			x		x						x	
RLB_103 Самопроверка						x			x		x			x				
RLB_104 Анализ п/о				x							x						x	
RLB_105 Установка п/о											x					x	x	
RLB_106 Вскрытие корпуса				x	x	x				x	x	x					x	
RLB_107 Умышленная порча						x											x	
RLB_108 Умышленная порча						x								x				
RLB_109 Прекращение электропитания									x								x	

	Опасности												ИТ-цели					
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
RLB_110 Перезагрузка		x															x	
RLB_111 Доступность данных																x	x	
RLB_112 Многоцелевое использование																	x	
Обмен данными																		
DEX_101 Экспорт защищенных данных о движении								x										x
Криптозащита																		
CSP_101 Алгоритмы																	x	x
CSP_102 Генерация ключей																	x	x
CSP_103 Рассылка ключей																	x	x
CSP_104 Доступ к ключам																	x	x
CSP_105 Уничтожение ключей																	x	x

ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ БОРТОВОГО УСТРОЙСТВА

1. Введение

В настоящем документе приводится описание бортового устройства с перечислением опасностей, которым оно должно противостоять, и целей, на которые должна быть направлена его защита. В нем указаны необходимые в этой связи защитные функции, минимальный уровень заявленной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1В. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1В. При

отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1B следует руководствоваться основным текстом добавления 1B.

Требования основного текста добавления 1B, для которых не определены контрольные показатели, защитными функциями не охватываются.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ Аттестуемое изделие
БУ Бортовое устройство
ЗФ Защитная функция
PIN Персональный идентификационный номер
ROM Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Данные о движении	Данные, которыми БУ обменивается с датчиком движения, позволяющие определять скорость и пробег транспортного средства.
Физически разделенные компоненты	Физические детали бортового устройства, установленные на транспортном средстве в разных местах, в отличие от физических деталей, сгруппированных внутри корпуса БУ.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Под пользователями понимаются люди, использующие то или иное оборудование. В круг пользователей БУ обычно входят водители, контролеры, мастерские и предприятия.
Пользовательские данные	Любые данные помимо данных о движении и данных защиты, регистрируемые и сохраняемые БУ в соответствии с требованиями главы III.12.

2.3 Источники

ITSEC Критерии оценки безопасности информационной технологии ITSEC, 1991 год.

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации бортового устройства

БУ предназначено для установки на автотранспортных средствах. Оно служит для регистрации, хранения, отображения, распечатки и выдачи на внешние устройства данных о деятельности водителей.

БУ соединено с датчиком движения, с которым оно обменивается данными о движении транспортного средства.

При взаимодействии с БУ пользователи идентифицируют себя с помощью карточек тахографа.

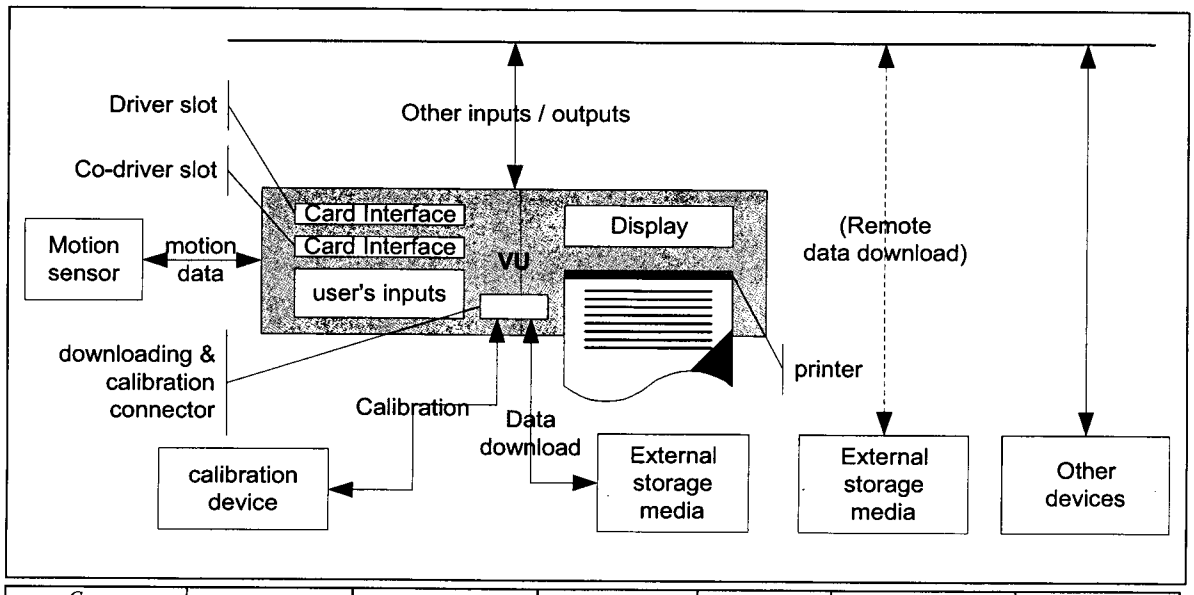
БУ регистрирует и сохраняет в своей памяти данные о деятельности пользователей; кроме того, данные о деятельности пользователей сохраняются им на карточках тахографа.

БУ способно отображать данные на дисплее, распечатывать их и передавать их на внешние устройства.

Операционная среда, в которой функционирует бортовое устройство, установленное на транспортном средстве, схематически показана на рисунке ниже.

Рис. 1

Операционная среда БУ



Счит. устройство карточки водителя			*Другие входы/выходы*			
Счит. устройство карточки 2-го водителя		*Интерфейс карточки* *Интерфейс карточки*	*БУ*	*Дисплей*	*(Дистанционная загрузка данных)*	
Датчик движения	*Данные о движении*	*Ввод данных пользователем*				
Загрузочный/ калибровочный разъем		*Калибровка*	*Загрузка данных*		*Печатающее устройство*	
	Калибровочное устройство			*Внешний носитель*	*Внешний носитель*	*Прочие устройства*

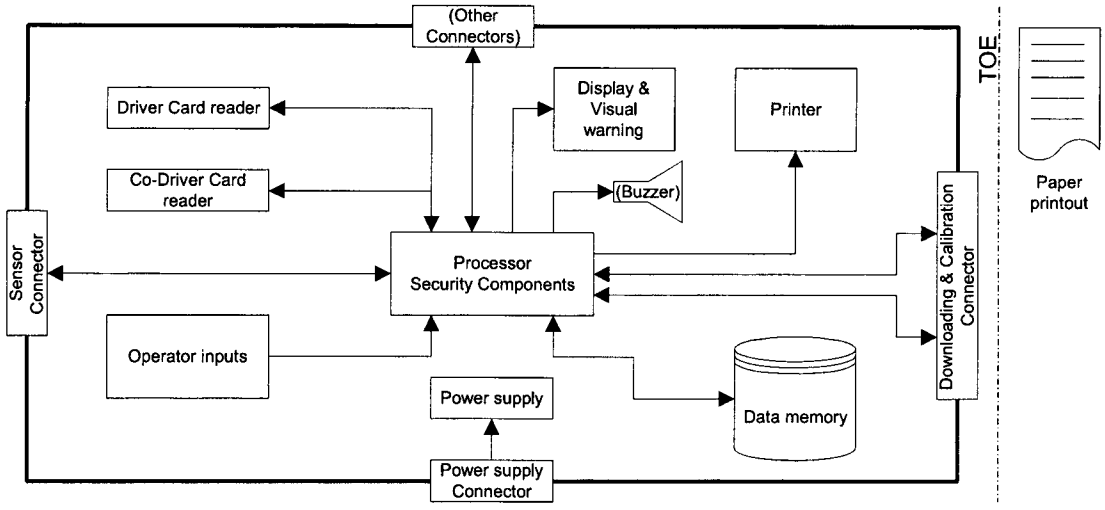
Общие характеристики БУ, описание его функций и режимов работы приводятся в главе II добавления 1B.

Конкретные требования к конструкции БУ изложены в главе III добавления 1B.

Типовая схема БУ представлена ниже.

Рис. 2

Типовая схема БУ (...) (не является обязательной)



	(Прочие разъемы)					*Аттестуемое изделие*	
	Счит. устройство карточки водителя			*Дисплей и визуальные сигналы предупреждения*	*Печатающее устройство*		
	Счит. устройство карточки 2-го водителя			*(Звуковой сигнал)*			*Распе-чатка*
	Элементы защиты процессора						
	Ввод данных оператором		*Питание*		*Запоминающее устройство для данных*	*Загрузочный/ калибровочный разъем*	
Разъем датчика							
	Разъем цепи питания						

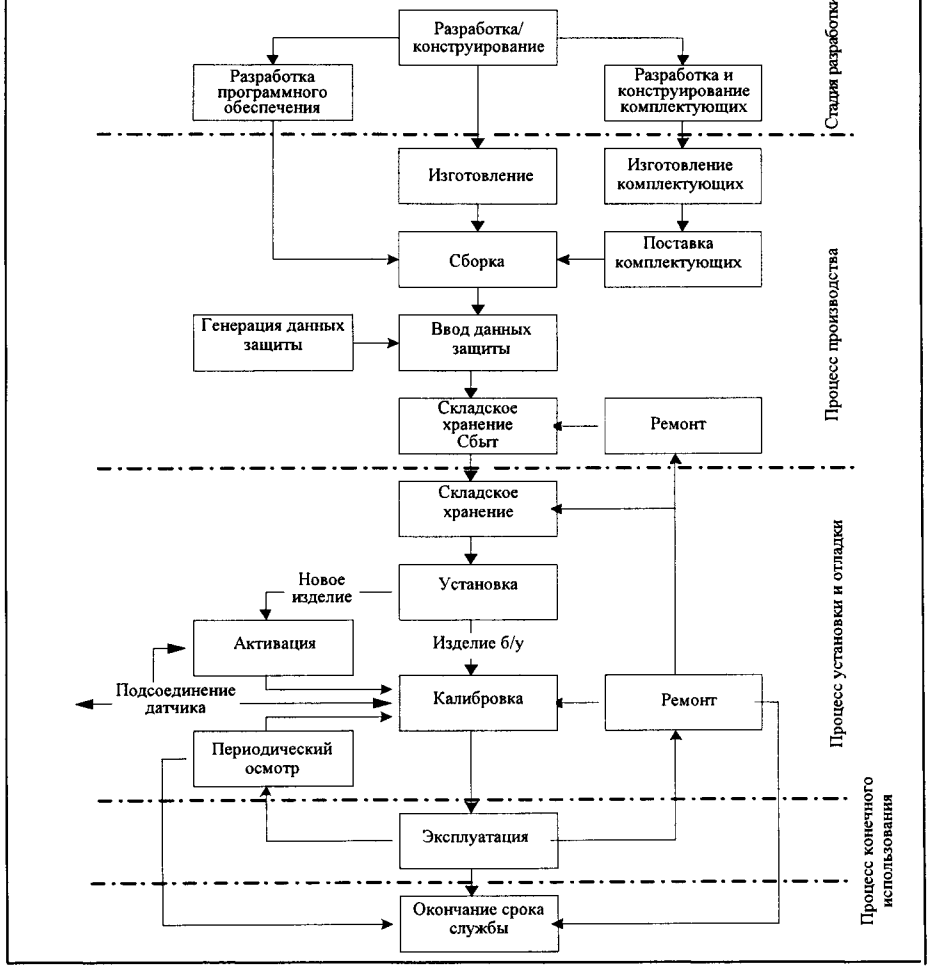
Следует иметь в виду, что хотя печатающее устройство является частью АИ, распечатанные им документы в состав АИ не входят.

3.2 Жизненный цикл бортового устройства

Типовая схема жизненного цикла БУ представлена ниже.

Рис. 3

Обобщенная схема жизненного цикла бортового устройства



3.3 Опасности

Настоящий пункт содержит описание угроз, которым может подвергаться БУ.

3.3.1 Опасности, связанные с идентификационными данными и режимом контроля за доступом

О: Доступ	Пользователи могут пытаться получить доступ к не предназначенным для них функциям (например, водители - к функции калибровки).

O: Идентификационные_данные	Пользователи могут пытаться воспользоваться другими идентификационными данными или вообще не использовать идентификационных данных.

3.3.2 Опасности, связанные с конструкцией устройства

O: Сбои в работе	Отказы аппаратуры, сбои в функционировании программного обеспечения или процедурах обмена данными могут привести к непредвиденным ситуациям и ослабить защиту БУ.
O: Испытания	Защита БУ может быть нарушена в результате использования неотключенных тест-режимов или имеющихся "обходных путей" доступа.
O: Конструкция	Пользователи могут пытаться незаконным путем добыть сведения о конструкции устройства – будь то у изготовителя (хищение, подкуп и т.п.) или путем инженерного анализа.

3.3.3 Опасности в процессе эксплуатации

O: Параметры_калибровки	Пользователи могут пытаться применять неверно откалиброванную аппаратуру (изменяя калибровочные данные или пользуясь организационными недосмотрами).
O: Обмен_данными_с_карточкой	Пользователи могут пытаться внести изменения в данные в процессе их передачи между БУ и карточкой тахографа (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).
O: Часы	Пользователи могут пытаться изменить показания встроенных часов.
O: Внешние_факторы	Для преодоления защиты БУ пользователи могут пытаться использовать воздействие внешних

	факторов (термических, электромагнитных, оптических, химических, механических и т.д.).
О: Фальсификация_устройств	Пользователи могут пытаться подключить к БУ фальсифицированные устройства (датчик движения, микропроцессорные карточки).
О: Аппаратура	Пользователи могут пытаться внести изменения в аппаратную часть БУ.
О: Данные_о_движении	Пользователи могут пытаться исказить данные о движении транспортного средства (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).
О: Неактивированная_аппаратура	Пользователи могут использовать неактивированную аппаратуру.
О: Выходные_данные	Пользователи могут пытаться внести изменения в выходные данные (при их распечатке, выводе на дисплей или загрузке на внешние устройства).
О: Источник_питания	Пользователи могут пытаться нейтрализовать защиту БУ путем изменения параметров тока в цепи питания (отключение, ослабление, усиление).
О: Данные_защиты	Пользователи могут пытаться получить несанкционированный доступ к данным защиты в процессе генерации этих данных, их передачи или хранения аппаратурой.
О: Программное_обеспечение	Пользователи могут пытаться внести изменения в программное обеспечение БУ.
О: Сохраненные_данные	Пользователи могут пытаться изменить сохраненные данные (данные защиты или пользовательские данные).

3.4 Цели защиты

Основная цель защиты системы цифрового тахографа заключается в следующем:

Ц: Основная	Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Соответственно, цели защиты БУ, способствующие достижению вышеупомянутой основной цели, заключаются в следующем:

Ц: Основная (БУ)	Данные, подлежащие измерению, регистрации и последующей проверке контрольными органами, должны иметься в наличии и обеспечивать точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.
Ц: Экспорт_данных (БУ)	БУ должно быть способно экспортировать данные на внешний носитель, обеспечивая при этом возможность проверки их целостности и подлинности.

3.5 Цели защиты в области информационных технологий

Конкретные цели защиты БУ в области ИТ, способствующие достижению главной цели защиты БУ, заключаются в следующем:

Ц: Доступ	БУ должно контролировать доступ пользователей к функциям и данным.

Ц: Отчетность	БУ должно обеспечивать сбор точных отчетных данных.
Ц: Надзор	БУ должно обеспечивать надзор за попытками преодоления защиты системы и отслеживать их связь с соответствующими пользователями.
Ц: Аутентификация	БУ должно производить аутентификацию пользователей и подключенных устройств (в случаях, когда необходим защищенный канал связи между устройствами).
Ц: Целостность	БУ должно защищать сохраненные данные от искажений.
Ц: Выходные_данные	БУ должно обеспечивать точное соответствие выходных данных тем данным, которые получены в результате измерений или хранятся в его памяти.
Ц: Обработка	БУ должно обеспечивать точность переработки вводимой информации в пользовательские данные.
Ц: Надежность	БУ должно функционировать надежно.
Ц: Защищенный_обмен_данными	БУ должно обеспечивать защиту данных, которыми оно обменивается с датчиком движения и карточками тахографа.

3.6 Технические, организационные и процедурные средства

В данном пункте излагаются технические, организационные и процедурные требования, связанные с защитой БУ.

3.6.1 Конструкция аппаратуры

С: Разработка	Разработчики БУ должны заботиться об обеспечении информационной безопасности при распределении функций на стадии конструирования.

С: Изготовление	Изготовители БУ должны заботиться об обеспечении информационной безопасности при распределении функций на стадии производства, а в процессе непосредственного изготовления БУ предохранять их от технического вмешательства, способного нарушить информационную защиту.

3.6.2 Поставка и активация аппаратуры

С: Поставка	Изготовители БУ, изготовители транспортных средств, сервисные центры и мастерские должны заботиться об обеспечении информационной безопасности на всех этапах работы с неактивированными БУ.
С: Активация	Изготовители транспортных средств, сервисные центры и мастерские должны, после установки БУ на транспортных средствах, активировать их до выхода транспортного средства из цеха, где произведена установка.

3.6.3 Генерация, передача и ввод данных защиты

С-З: Генерация_данных	Доступ к алгоритмам генерации данных защиты должны иметь только уполномоченные и пользующиеся доверием лица.
С-З: Перенос_данных_защиты	При генерации и передаче данных защиты, а также при их вводе в датчик движения должны соответствующим образом обеспечиваться конфиденциальность и целостность этих данных.

3.6.4 Выдача карточек

С: Доступ_к_карточкам	Карточки тахографа должны выдаваться только лицам, прошедшим соответствующий отбор.

C: Единственность_карточки_водителя	Водитель не может одновременно иметь более одной действительной карточки водителя.
C: Учет_карточек	Выдача карточек подлежит учету ("белые" и "черные" списки); "черные списки" должны использоваться при ревизионных проверках систем защиты.

3.6.5 Установка, калибровка и проверка контрольного устройства

C: Утвержденные_мастерские	Монтаж, калибровка и ремонт контрольных устройств должны производиться только в сервисных центрах или мастерских, пользующихся доверием и допущенных к таким работам.
C: Регулярные_проверки	Контрольное устройство должно регулярно проходить проверку и калибровку.
C: Добросовестность_калибровки	При калибровке контрольных устройств в утвержденных сервисных центрах или мастерских в эти устройства должны вводиться действительные параметры соответствующих транспортных средств.

3.6.6 Эксплуатация аппаратуры

C: Добросовестность_водителей	Водители должны соблюдать установленные правила и вести себя ответственно (пользоваться карточками водителя, правильно вводить данные о своей деятельности, когда эти данные вводятся вручную, и т.д.).

3.6.7 Правоприменительный контроль

C: Контроль	Правоприменительный контроль должен осуществляться как на регулярной, так и на

выборочной основе и включать ревизионную проверку систем защиты.

3.6.8 Новые версии программного обеспечения

C: Новое_п/о	Перед установкой на БУ новые версии программного обеспечения должны получить сертификат защиты.

4. Защитные функции

4.1 Идентификация и аутентификация

4.1.1 Идентификация и аутентификация датчика движения

UIA_201 При каждом взаимодействии с датчиком движения БУ должно иметь возможность идентифицировать датчик, к которому оно подключено.

UIA_202 Идентификационные данные датчика движения состоят из номера официального утверждения прототипа датчика и серийного номера датчика.

UIA_203 БУ должно производить аутентификацию подключенного к нему датчика движения:

- при подключении датчика движения;
- при каждой калибровке контрольного устройства;
- при восстановлении подачи питания после перерыва.

Процесс аутентификации является двусторонним и инициируется бортовым устройством.

UIA_204 БУ должно периодически (*периодичность определяется изготовителем, но должна составлять более одного раза в час*) производить повторную идентификацию и повторную аутентификацию подключенного к нему датчика движения и подтверждать, что датчик движения, идентифицированный при последней калибровке контрольного устройства, не был заменен другим.

UIA_205 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_206 После регистрации (*количество определяется изготовителем, но не должно превышать 20*) неудачных попыток аутентификации подряд и/или после обнаружения несанкционированной (т.е. произведенной не в процессе калибровки контрольного устройства) замены датчика движения защитная функция должны обеспечивать:

- генерацию контрольный записи о событии;
- выдачу предупреждения пользователю;
- дальнейший прием и использование данных о движении, передаваемых датчиком движения, в незащищенном режиме.

4.1.2 Идентификация и аутентификация пользователей

UIA_207 БУ на постоянной основе избирательно отслеживает идентификационные данные двух пользователей по информации, считываемой с карточек тахографа, которые вводятся в считывающие устройства для карточек водителя и второго водителя.

UIA_208 Идентификационные данные пользователя состоят из:

- указания категории пользователя:
- ВОДИТЕЛЬ (карточка водителя),
- КОНТРОЛЕР (карточка контролера),
- МАСТЕРСКАЯ (карточка мастерской),
- ПРЕДПРИЯТИЕ (карточка предприятия),
- НЕТ ДАННЫХ (карточка не введена),
- идентификатора пользователя, который включает:
- код выдавшей карточку Договаривающейся стороны и номер карточки;
- параметр UNKNOWN, если НЕТ ДАННЫХ о том, к какой категории принадлежит пользователь.

Пользователи, идентификатор которых содержит параметр UNKNOWN, могут быть опознаваемыми непосредственно или по косвенным признакам.

UIA_209 БУ должно аутентифицировать пользователей при вводе карточек.

UIA_210 БУ должно производить повторную аутентификацию пользователей:

- при возобновлении подачи питания;
- на периодической основе или после конкретных событий (*периодичность определяется изготовителем, но должна составлять более одного раза в сутки*).

UIA_211 Аутентификация производится путем подтверждения того, что введенная в устройство карточка является действительной карточкой тахографа и содержит данные защиты, которые могли быть получены только из системы. Процесс аутентификации является двусторонним и инициируется бортовым устройством.

UIA_212 В дополнение к вышеизложенному обязательным требованием является положительная аутентификация мастерских с помощью PIN-кода. PIN-код должен состоять не менее чем из 4 знаков.
Примечание. Если PIN-код передается на БУ с внешней аппаратуры, расположенной вблизи от БУ, то меры по защите конфиденциальности PIN-кода при передаче не требуются.

UIA_213 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_214 После регистрации 5 неудачных попыток аутентификации подряд защитная функция должна обеспечивать:

- генерацию контрольной записи о событии;
- выдачу предупреждения пользователю;
- отнесение пользователя к категории НЕТ ДАННЫХ и признание карточки недействительной (определение "z" и требование 007).

4.1.3 Идентификация и аутентификация предприятия при дистанционном подключении

Возможность дистанционного подключения предприятия не обязательна. Поэтому настоящий пункт применяется лишь в тех случаях, когда эта функция реализована.

UIA_215 При каждом взаимодействии с дистанционно подключенным предприятием БУ должно иметь возможность идентифицировать это предприятие.

UIA_216 Идентификационные данные предприятия, использующего дистанционное подключение, состоят из кода Договаривающейся стороны, которая выдала карточку предприятия, и номера карточки предприятия.

UIA_217 Экспорту каких-либо данных БУ в адрес дистанционно подключенного предприятия должна предшествовать положительная аутентификация этого предприятия бортовым устройством.

UIA_218 Аутентификация производится путем подтверждения того, что у предприятия имеется действительная карточка предприятия, содержащая данные защиты, которые могли быть получены только из системы.

UIA_219 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_220 После регистрации 5 неудачных попыток аутентификации подряд БУ должно обеспечивать:

- выдачу предупреждения дистанционно подключенному предприятию.

4.1.4 Идентификация и аутентификация административных устройств

Изготовителями БУ могут быть предусмотрены специальные устройства для выполнения дополнительных административных функций, связанных с БУ (таких, как установка обновлений программного обеспечения, перезагрузка данных защиты и т.п.). Настоящий пункт применяется лишь при наличии подобных устройств.

UIA_221 При каждом взаимодействии с административным устройством БУ должно иметь возможность идентифицировать это устройство.

UIA_222 Любому дальнейшему взаимодействию должна предшествовать успешная аутентификация административного устройства бортовым устройством.

UIA_223 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

4.2 Контроль за доступом

Средства контроля за доступом обеспечивают, чтобы возможность считывать, вводить или изменять информацию в АИ имели только санкционированные лица.

Следует иметь в виду, что хотя регистрируемые БУ пользовательские данные могут рассматриваться как чувствительные с точки зрения защиты личных данных или коммерческой тайны, конфиденциального характера они не носят. Поэтому

функциональное требование, касающееся прав доступа к считке этих данных (требование 011), не обеспечивается соответствующей защитной функцией.

4.2.1 Режим контроля за доступом

ACC_201 БУ должно обеспечивать учет и контроль прав доступа к функциям и данным.

4.2.2 Права доступа к функциям

ACC_202 БУ обеспечивает соблюдение правил выбора режима работы устройства (требования 006 - 009).

ACC_203 В рамках соответствующих режимов работы БУ обеспечивает соблюдение правил контроля за доступом к функциям (требование 010).

4.2.3 Права доступа к данным

ACC_204 БУ обеспечивает соблюдение правил доступа к функции сохранения идентификационных данных БУ (требование 076).

ACC_205 БУ обеспечивает соблюдение правил доступа к функции сохранения идентификационных данных подсоединенного к нему датчика движения (требования 079 и 155).

ACC_206 После активации БУ бортовое устройство обеспечивает, чтобы калибровочные данные могли вводиться в БУ и сохраняться в его памяти только тогда, когда устройство находится в режиме калибровки (требования 154 и 156).

ACC_207 После активации БУ бортовое устройство обеспечивает соблюдение правил доступа к функции сохранения и удаления калибровочных данных (требование 097).

ACC_208 После активации БУ бортовое устройство обеспечивает, чтобы данные корректировки времени могли вводиться в БУ и сохраняться в его памяти только тогда, когда устройство находится в режиме калибровки (данное требование не распространяется на незначительные корректировки времени, допустимые согласно требованиям 157 и 158).

ACC_209 После активации БУ бортовое устройство обеспечивает соблюдение правил доступа к функции сохранения и удаления данных корректировки времени (требование 100).

ACC_210 БУ должно обеспечивать соответствующий режим доступа к функциям считывания и сохранения данных защиты (требование 080).

4.2.4 Структура файлов и условия доступа к ним

ACC_211 Структура файлов приложений и файлов данных и условия доступа к ним определяются в процессе изготовления и защищаются от любого последующего изменения или удаления.

4.3 Отчетность

ACT_201 БУ должно обеспечивать отчетность водителей о своей деятельности (требования 081, 084, 087, 105a, 105b, 109 и 109a).

ACT_202 В БУ должны храниться неизменяемые идентификационные данные (требование 075).

ACT_203 БУ должно обеспечивать отчетность мастерских о своей деятельности (требования 098, 101 и 109).

ACT_204 БУ должно обеспечивать отчетность контролеров о своей деятельности (требования 102, 103 и 109).

ACT_205 БУ должно регистрировать данные счетчика пробега (требование 090) и подробные данные о скоростном режиме (требование 093).

ACT_206 БУ должно обеспечивать, чтобы пользовательские данные, имеющие отношение к требованиям 081 - 093 и 102 - 105b включительно, не изменялись после их сохранения, за исключением случаев, когда они становятся наиболее старыми из хранящихся в памяти данных и подлежат замене новыми данными.

ACT_207 БУ должно обеспечивать, чтобы данные, уже сохраненные на карточке тахографа, не изменялись бортовым устройством (требования 109 и 109a), за исключением случаев замены наиболее старых данных новыми данными (требование 110) и случая, о котором говорится в примечании к пункту 2.1 подраздела I.

4.4 Контроль

Контрольные функции необходимы только в связи с событиями, которые могут указывать на попытки вмешательства в работу устройства или нарушения его защиты. При обычном осуществлении пользовательских прав, даже имеющих отношение к защите, эти функции не требуются.

AUD_201 События, затрагивающие защиту БУ, регистрируются БУ вместе с соответствующими данными (требования 094, 096 и 109).

AUD_202 К событиям, затрагивающим защиту БУ, относятся:

- попытки нарушения защиты:
  - отрицательный результат аутентификации датчика движения;
  - отрицательный результат аутентификации карточки тахографа;
  - несанкционированная замена датчика движения;
  - ошибка при проверке целостности данных, введенных с карточки;
  - ошибка при проверке целостности сохраненных пользовательских данных;
  - ошибка внутренней передачи данных;
  - несанкционированное вскрытие корпуса;
  - умышленная порча оборудования;
- ошибка в данных о движении;
- перерыв в подаче питания;
- внутренние неполадки в БУ.

AUD_203 В БУ обеспечивается соответствующий режим хранения контрольных записей (требования 094 и 096).

AUD_204 Контрольные записи, генерированные датчиком движения, сохраняются в памяти БУ.

AUD_205 Должна быть предусмотрена возможность вывода контрольных записей на дисплей, их распечатки и загрузки на внешние устройства.

4.5 Повторное использование объектов

REU_201 БУ обеспечивает возможность повторного использования временно сохраненных объектов без недопустимой дополнительной передачи информации.

4.6 Достоверность

4.6.1 Правила контроля за поступлением информации

ACR_201 БУ должно обеспечивать, чтобы пользовательские данные, имеющие отношение к требованиям 081, 084, 087, 090, 093, 102, 104, 105, 105a и 109, принимались к обработке лишь при условии их поступления из следующих источников:

- данные о движении транспортного средства;
- часы реального времени, встроенные в БУ;
- параметры калибровки контрольного устройства;
- карточки тахографа;
- ввод данных пользователем.

ACR_201a БУ должно обеспечивать возможность ввода пользовательских данных, имеющих отношение к требованию 109a, только за период с момента последнего извлечения карточки до ввода карточки, находящейся в устройстве на данный момент (требование 050a).

4.6.2 Внутренняя передача данных

Требования настоящего пункта применяются лишь к тем БУ, в которых используются физически разделенные компоненты.

ACR_202 Если между физически разделенными компонентами БУ передаются данные, то эти данные должны быть защищены от изменения.

ACR_203 При обнаружении ошибки передачи данных в процессе их внутренней передачи передача осуществляется повторно, а ЗФ генерирует контрольную запись об этом событии.

4.6.3 Целостность сохраненных данных

ACR_204 БУ должно проверять целостность хранящихся в его памяти пользовательских данных.

ACR_205 В случае ошибки при проверке целостности сохраненных пользовательских данных ЗФ генерирует контрольную запись.

4.7 Надежность функционирования

4.7.1 Испытания

RLB_201 Все команды, функции и контакты, предназначенные исключительно для тестирования БУ на стадии производства, перед активацией БУ блокируются или удаляются. Возможность их восстановления для последующего использования должна быть исключена.

RLB_202 При включении, а также в процессе работы в обычном режиме БУ должно производить самопроверку для подтверждения того, что оно функционирует нормально. При самопроверке БУ проверяется целостность данных защиты и хранящихся в памяти исполнимых команд (если они не сохранены в ROM).

RLB_203 В случае обнаружения внутренних неполадок в процессе самопроверки ЗФ обеспечивает:

- генерацию отчетной записи (если устройство не находится в режиме калибровки) (внутренние неполадки в БУ);
- целостность сохраненных данных.

4.7.2 Программное обеспечение

RBL_204 Возможность анализа или отладки программного обеспечения активированного БУ в полевых условиях должна быть исключена.

RLB_205 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.7.3 Физическая защита

RLB_206 Если конструкция БУ допускает вскрытие его корпуса, то БУ, когда оно не находится в режиме калибровки, должно регистрировать любое такое вскрытие и сохранять эту способность даже при отключении от внешнего источника питания в течение как минимум шести месяцев. При этом ЗФ генерирует отчетную запись (допускается возможность генерации и сохранения такой записи после возобновления питания).

Если конструкция БУ не предусматривает вскрытия корпуса, то она должна обеспечивать легкое обнаружение следов физического воздействия (например, при внешнем осмотре).

RLB_207 После активации БУ должно производить тестирование с целью выявления конкретных видов умышленной порчи оборудования (определяются изготовителем).

RLB_208 В случае обнаружения такой порчи оборудования ЗФ генерируют надзорную запись, а БУ (определяется изготовителем).

4.7.4 Прекращение электропитания

RLB_209 БУ должно регистрировать отклонения от номинальных параметров тока в цепи питания, в том числе отключения от источника питания.

RLB_210 В вышеупомянутых случаях ЗФ обеспечивает:

- генерацию надзорной записи (если устройство не находится в режиме калибровки);
- сохранение защищенности БУ;
- сохранение функций защиты не отключенных компонентов и процессов;
- целостность сохраненных данных.

4.7.5 Перезапуск

RLB_211 При перерыве в подаче питания, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, БУ полностью перезапускается.

4.7.6 Доступность данных

RLB_212 БУ должно предоставлять доступ к имеющимся ресурсам данных по мере необходимости, обеспечивать отсутствие неоправданных обращений к ресурсам и предусматривать стирание ненужных данных.

RLB_213 БУ должно обеспечивать невозможность извлечения карточек до сохранения на них соответствующих данных (требования 015 и 016).

RLB_214 В указанном выше случае ЗФ генерирует контрольную запись о данном событии.

4.7.7 Многоцелевое использование

RLB_215 Если БУ используется для других целей, помимо функции тахографа, то все соответствующие приложения должны быть физически и/или логически отделены друг от друга. Данные защиты не должны быть общими для этих приложений. Одновременное выполнение более чем одной функции не допускается.

4.8 Обмен данными

В настоящем пункте рассматривается обмен данными между БУ и подключенными к нему устройствами.

4.8.1 Обмен данными с датчиком движения

DEX_201 БУ должно проверять целостность и подлинность данных о движении, импортируемых с датчика движения.

DEX_202 В случае обнаружения ошибки при проверке целостности или подлинности данных о движении ЗФ обеспечивает:

- генерацию контрольной записи;
- дальнейшее использование импортируемых данных.

4.8.2 Обмен данными с карточками тахографа

DEX_203 БУ должно проверять целостность и подлинность данных, импортируемых с карточек тахографа.

DEX_204 В случае обнаружения ошибки при проверке целостности или подлинности данных, поступающих с карточки, БУ:

- генерирует контрольную запись;
- не использует поступившие данные.

DEX_205 БУ экспортирует данные на микропроцессорные карточки тахографа с соответствующими атрибутами защиты, позволяющими карточке проверять их целостность и подлинность.

4.8.3 Обмен данными с внешним носителем (функция загрузки данных)

DEX_206 БУ генерирует информацию, подтверждающую происхождение данных, загружаемых на внешний носитель.

DEX_207 БУ обеспечивает возможность проверки получателем информации, подтверждающей происхождение загруженных данных.

DEX_208 БУ загружает данные на внешний носитель с соответствующими атрибутами защиты, позволяющими проверять целостность и подлинность загруженных данных.

4.9 Криптографическая защита

Требования данного пункта применяются лишь в необходимых случаях, в зависимости от используемых механизмов защиты и примененных изготовителем технических решений.

CSP_201 Любые криптографические операции, выполняемые БУ, должны соответствовать заданному алгоритму при заданном размере ключа.

CSP_202 Если БУ генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей.

CSP_203 Если БУ рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки ключей.

CSP_204 Если БУ получает доступ к криптографическим ключам, то это должно соответствовать установленному порядку доступа к криптографическим ключам.

CSP_205 Если БУ уничтожает криптографические ключи, то это должно делаться в соответствии с установленными методами уничтожения криптографических ключей.

5. Определение механизмов защиты

Обязательные механизмы защиты указаны в подразделе XI.

Все остальные механизмы защиты определяются изготовителями по их усмотрению.

6. Минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты бортового устройства должна соответствовать "высокому" уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты бортового устройства по системе ITSEC должна соответствовать уровню E3 (согласно определению, содержащемуся в [ITSEC]).

8. Обоснование

В нижеследующей таблице приводится обоснование ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

	Опасности																		ИТ-цели								
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
Технические, организационные и процедурные средства																											
Разработка			x	x	x																						
Изготовление				x	x																						
Поставка													x														
Активация	x												x														
Генерация данных защиты																	x										
Перенос данных защиты																	x										
Наличие карточки		x																									
Единственность карточки водителя		x																									
История карточки		x																									
Утвержденные мастерские						x		x																			
Регулярная инспекция Калибровка						x		x			x				x			x									
Добросовестные мастерские						x		x																			
Добросовестные водители		x																									
Правоприменительный контроль		x				x		x	x		x		x		x		x	x									
Новые версии п/о																		x									
Защитные функции																											
Идентификация и аутентификация																											
UIA_201 Идентификация датчика										x		x											x				x
UIA_202 Идент. данные датчика										x		x											x				
UIA_203 Аутентификация датчика										x		x											x				x

		Опасности																			ИТ-цели								
		Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
UIA_204	Повторная идентификация и аутентификация датчика										x		x											x					x
UIA_205	Нефальсифицируемая аутентификация										x		x											x					
UIA_206	Отрицательная аутентификация										x		x										x					x	
UIA_207	Идентификация пользователей	x	x								x										x			x					x
UIA_208	Идент. данные пользователей	x	x								x										x			x					
UIA_209	Аутентификация пользователей	x	x								x										x			x					x
UIA_210	Повторная аутентификация пользователей	x	x								x										x			x					x
UIA_211	Средства аутентификации	x	x								x										x			x					
UIA_212	Проверка PIN	x	x				x		x												x			x					
UIA_213	Нефальсифицируемая аутентификация	x	x								x										x			x					
UIA_214	Отрицательная аутентификация	x	x								x												x						
UIA_215	Идентификация удаленного пользов.	x	x																		x			x					x
UIA_216	Идент. данные удаленного пользов.	x	x																		x			x					
UIA_217	Аутентификация удаленного пользов.	x	x																		x			x					x

	Опасности																			ИТ-цели								
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
UIA_218 Средства аутентификации	x	x																		x			x					
UIA_219 Нефальсифицируемая аутентификация	x	x																		x			x					
UIA_220 Отрицательная аутентификация	x	x																										
UIA_221 Идентификация admin. устройств	x	x																		x			x					
UIA_222 Аутентификация admin. устройств	x	x																		x			x					
UIA_223 Нефальсифицируемая аутентификация	x	x																		x			x					
Контроль за доступом																												
ACC_201 Режим контроля за доступом	x					x		x									x		x	x								
ACC_202 Права доступа к функциям	x					x		x												x								
ACC_203 Права доступа к функциям	x					x		x												x								
ACC_204 ID БУ																			x	x								
ACC_205 ID подключенного датчика									x										x	x								
ACC_206 Данные калибровки	x					x													x	x								
ACC_207 Данные калибровки						x													x	x								
ACC_208 Данные корректировки времени								x											x	x								

	Опасности																		ИТ-цели								
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
ACC_209 Данные корректировки времени								x											x	x								
ACC_210 Данные защиты																	x		x	x								
ACC_211 Структура файлов и условия доступа	x					x											x		x	x								
Отчетность																												
ACT_201 Отчетность водителей																					x							
ACT_202 Идент. данные БУ																					x	x						
ACT_203 Отчетность мастерских																					x							
ACT_204 Отчетность контролеров																					x							
ACT_205 Отчетность о движении т/с																					x							
ACT_206 Изменение отчетных данных																			x					x			x	
ACT_207 Изменение отчетных данных																			x					x			x	

		Опасности																			ИТ-цели								
		Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
Контроль																													
AUD_201	Контрольные записи																						x						
AUD_202	Список зафиксированных подконтрольных событий	x						x				x	x		x	x				x			x						
AUD_203	Правила хранения контрольных записей																						x						
AUD_204	Контрольные записи датчика																						x						
AUD_205	Средства контроля																						x						
Повторное использование																													
REU_201	Повторное использование																	x									x	x	
Достоверность																													
ACR_201	Правила контроля за поступлением информации							x			x		x														x	x	
ACR_202	Внутр. передача													x												x	x	x	
ACR_203	Внутр. передача													x									x						
ACR_204	Неискаженность сохран. данных																			x					x			x	
ACR_205	Неискаженность сохран. данных																			x			x						

	Опасности																			ИТ-цели								
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
Надежность																												
RLB_201 Заводские испытания				x	x																					x	
RLB_202 Самотест.			x								x				x			x									x	
RLB_203 Самотест.											x				x			x				x						
RLB_204 Анализ п/о					x													x									x	
RLB_205 Установка п/о																		x						x	x	x	
RLB_206 Вскрытие корпуса					x				x		x			x			x	x	x					x			x	
RLB_207 Умышленная порча											x																x	
RLB_208 Умышленная порча											x											x						
RLB_209 Перерывы в подаче питания															x												x	
RLB_210 Перерывы в подаче питания															x							x						
RLB_211 Перезагрузка			x																								x	
RLB_212 Доступность данных																										x	x	
RLB_213 Возврат карточки																											x	
RLB_214 Ошибка при завершении сеанса работы с карточкой																						x						
RLB_215 Многоцелевое использование																											x	
Обмен данными																												
DEX_201 Защищенный импорт данных о движ.												x																x
DEX_202 Защищенный импорт данных о движ.												x										x						

	Опасности																			ИТ-цели								
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
DEX_203 Защищенный импорт данных с карт.							x																					x
DEX_204 Защищенный импорт данных с карт.							x															x						
DEX_205 Защищенный экспорт данных на карт.							x																					x
DEX_206 Доказательство происхождения														x											x			
DEX_207 Доказательство происхождения														x											x			
DEX_208 Защищенный экспорт данных на ВН														x											x			
Криптозащита																												
CSP_201 Алгоритмы																											x	x
CSP_202 Генерация ключей																											x	x
CSP_203 Рассылка ключей																											x	x
CSP_204 Доступ к ключам																											x	x
CSP_205 Уничтожение ключей																											x	x

ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ КАРТОЧКИ ТАХОГРАФА

1. Введение

В настоящем документе приводится описание карточки тахографа с перечислением опасностей, которым она должна противостоять, и целей, на которые должна быть направлена ее защита. В нем указаны необходимые для этого защитные функции, минимальный уровень заданной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1В. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1В. При отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1В следует руководствоваться основным текстом добавления 1В.

Требования основного текста добавления 1В, для которых не определены контрольные показатели, защитными функциями не охватываются.

Карточка тахографа представляет собой стандартную карточку со встроенной микросхемой, в которую введена специализированная прикладная программа тахографа, отвечающую современным требованиям в отношении функциональных возможностей и защиты микропроцессорных карточек. Соответственно, изложенные здесь контрольные показатели защиты касаются только дополнительных потребностей в защите, непосредственно связанных с функциями тахографа.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ Аттестуемое изделие
БУ Бортовое устройство
ЗФАИ Защитная функция АИ

МП Микропроцессор
(электронная схема, предназначенная для обработки и/или хранения данных),
ОС Операционная система
PIN Персональный идентификационный номер
РЗФ Режим защитных функций
ROM Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Чувствительные данные	Данные, хранящиеся на карточке тахографа и нуждающиеся в защите от искажений, несанкционированных изменений и нарушений конфиденциальности (в части, касающейся данных защиты). К чувствительным данным относятся данные защиты и пользовательские данные.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Любой субъект (человек или внешнее электронное устройство) вне АИ, вступающий во взаимодействие с АИ.
Пользовательские данные	Чувствительные данные помимо данных защиты, хранящиеся на карточке тахографа. К пользовательским данным относятся идентификационные данные и данные о деятельности.
Идентификационные данные	Идентификационные данные включают идентификационные данные карточки и идентификационные данные держателя карточки.
Идентификационные данные карточки	Пользовательские данные, имеющие отношение к идентификации карточки, как это определено требованиями 190, 191, 192, 194, 215, 231 и 235.

Идентификационные данные держателя карточки	Пользовательские данные, имеющие отношение к идентификации держателя карточки, как это определено требованиями 195, 196, 216, 232 и 236.
Данные о деятельности	Данные о деятельности включают данные о деятельности держателя карточки, данные о событиях и неисправностях и данные о контрольных мероприятиях.
Данные о деятельности держателя карточки	Пользовательские данные, имеющие отношение к деятельности держателя карточки, как это определено требованиями 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 и 237.
Данные о событиях и отказах	Пользовательские данные, имеющие отношение к событиям или неисправностям, как это определено требованиями 204, 205, 207, 208 и 223.
Данные о контрольных мероприятиях	Пользовательские данные, имеющие отношение к правоприменительному контролю, как это определено требованиями 210 и 225.

2.3 Источники

ITSEC Критерии оценки безопасности информационной технологии ITSEC, 1991 год.

IC PP Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.

ES PP Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации карточки тахографа

Карточка тахографа представляет собой карточку со встроенной микросхемой, соответствующую описанию, которое приводится в источниках [IC PP] и [ES PP], и несущую в себе прикладную программу для использования этой карточки совместно с контрольным устройством.

Основными функциями карточки тахографа являются:

- хранение идентификационных данных карточки и ее держателя. Эти данные используются бортовым устройством для идентификации держателя карточки, предоставления полагающегося ему доступа к функциям и данным и обеспечения отчетности держателя карточки о своих действиях;

- хранения данных о деятельности держателя карточки, данных о событиях и неисправностях и данных о контрольных мероприятиях, имеющих отношение к держателя карточки.

Таким образом, карточка тахографа предназначена для взаимодействия с бортовым устройством через его интерфейс для считки карточек. Она также может использоваться посредством любого считывающего устройства карт (например, подключенного к персональному компьютеру), через который можно получить полный доступ к любым пользовательским данным для их чтения.

На стадии конечного использования карточки тахографа (7-й этап "жизненного цикла", описание которого содержится в [ES PP]), бортовые устройства могут осуществлять только запись на нее пользовательских данных.

Требования к функциональным возможностям карточки тахографа изложены в основном тексте добавления 1B и в подразделе II.

3.2 Жизненный цикл карточек тахографа

Жизненный цикл карточек тахографа соответствует жизненному циклу карточек со встроенной микросхемой, описание которого приводится в [ES PP].

3.3 Опасности

Помимо перечисленных в [ES PP] и [IC PP] общих опасностей, актуальных для всех карточек со встроенной микросхемой, карточки тахографа могут подвергаться следующим опасностям:

3.3.1 Конечные цели нарушителей защиты

Конечной целью попыток преодоления защиты является изменение хранящихся в АИ пользовательских данных.

O: Идент._данные Успешное изменение хранящихся в АИ идентификационных данных (таких, как тип карточки, срок ее действия или идентификационные данные держателя) создает возможность мошенничества при использовании АИ и ставит под серьезную угрозу достижение общих целей защиты системы.

O: Данные_о_деят. Успешное изменение хранящихся в АИ данных о деятельности подрывает защиту АИ.

O: Обмен_данными Успешное изменение (добавление, изъятие, искажение) данных о деятельности при их импорте или экспорте подрывает защиту АИ.

3.3.2 Пути преодоления защиты

Для преодоления защиты АИ могут использоваться следующие методы:

- несанкционированное получение сведений об устройстве аппаратной части и программного обеспечения АИ, и в первую очередь о его защитных функциях или данных защиты. Такие сведения могут быть получены в результате незаконного завладения материалами разработчика или изготовителя (путем хищения, подкупа и т.д.) или в результате непосредственного изучения АИ (физическое исследование, дедуктивный анализ и т.д.);

- использование слабых мест конструкции или технического исполнения АИ (инженерных просчетов, ошибок программного обеспечения, сбоев при передаче данных, отклонений в работе АИ, спровоцированных экстремальным воздействием внешних факторов, недостатков защитных функций – таких, как процедуры аутентификации, контроль за доступом к данным, криптографическая защита и т.д.).

- воздействие на АИ или его защитные функции с помощью физических, электрических или логических средств по отдельности или в сочетании друг с другом.

3.4 Цели защиты

Основная цель защиты всей системы цифрового тахографа заключается в следующем:

Ц: Основная	Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Соответственно, основные цели защиты АИ, способствующие достижению вышеупомянутой основной цели, заключаются в следующем:

Ц: Идент._данные_карточки	АИ должно сохранять в неприкосновенности идентификационные данные карточки и идентификационные данные держателя карточки, введенные в память в процессе его персонализации.
Ц: Сохр._карточкой_данных_о_деят.	АИ должно сохранять в неприкосновенности пользовательские данные, введенные в память карточки бортовым устройством.

3.5 Цели защиты в области информационных технологий

Помимо перечисленных в [ES PP] и [IC PP] целей защиты, являющихся общими для всех карточек со встроенной микросхемой, реализации основных целей защиты АИ на стадии его конечного использования способствует достижение следующих специфических целей, связанных с информационными технологиями:

Ц: Доступ_к_данным	АИ должно предоставлять доступ к функции сохранения пользовательских данных только аутентифицированным бортовым устройствам.
Ц: Криптозащита_сообщений	АИ должно поддерживать протоколы и процедуры криптозащищенного обмена данными между карточкой и устройством считывания карточек, когда это необходимо для выполнения соответствующих функций.

3.6 Технические, организационные и процедурные средства

Технические, организационные и процедурные требования, направленные на защиту АИ, перечислены в [ES PP] и [IC PP] (разделы о целях защиты, связанных с операционной средой).

4. Защитные функции

В данном пункте конкретизируются некоторые из допустимых операций, такие как постановка функциональных задач или выбор [ES PP], и излагаются дополнительные функциональные требования к ЗФ.

4.1 Соответствие профилям защиты

CPP_301 АИ должно соответствовать [IC PP].

CPP_302 АИ должно соответствовать [ES PP], с учетом дальнейших уточнений.

4.2 Идентификация и аутентификация пользователей

Карточка должна идентифицировать устройство, в которое она введена, и распознавать, является ли это устройство аутентифицированным бортовым устройством. Допускается экспорт любых пользовательских данных с карточки на любое считывающее устройство; исключение составляют карточки контролера и карточки предприятия, идентификационные данные держателей которых могут экспортироваться только на аутентифицированные бортовые устройства (соответственно, появление имени контролера на дисплее или в распечатке служит доказательством того, что бортовое устройство не фальсифицировано).

4.2.1 Идентификация пользователей

Функциональная задача (FIA_UID.1.1) *Перечень действий со стороны ЗФАИ*: не требуются.

Функциональная задача (FIA_ATD.1.1) *Перечень атрибутов защиты*:

- **КАТЕГОРИЯ_ПОЛЬЗОВАТЕЛЕЙ**: БОРТОВОЕ_УСТРОЙСТВО,
  НЕ_БОРТОВОЕ_УСТРОЙСТВО,

- **ID_ПОЛЬЗОВАТЕЛЯ:** Регистрационный номер транспортного средства (VRN) и код Договаривающейся стороны, где оно зарегистрировано (ID_ПОЛЬЗОВАТЕЛЯ известен только в случае, если КАТЕГОРИЯ ПОЛЬЗОВАТЕЛЕЙ = БОРТОВОЕ_УСТРОЙСТВО).

4.2.2 Аутентификация пользователей

Функциональная задача (FIA_UAU.1.1) *Перечень действий со стороны ЗФАИ*:

- карточка водителя и карточка мастерской: экспорт пользовательских данных с атрибутами защиты (функция загрузки данных с карточки);

- карточка контролера: экспорт пользовательских данных без атрибутов защиты помимо идентификационных данных держателя карточки.

UIA_301 Аутентификация бортового устройства осуществляется путем подтверждения наличия в нем данных защиты, которые могут быть получены только из системы.

Выбор (FIA_UAU.3.1 и FIA_UAU.3.2): блокировать.

Функциональная задача (FIA_UAU.4.1) *Заданный(е) механизм(ы) аутентификации:* любой механизм аутентификации.

UIA_302 Для карточки мастерской предусмотрен дополнительный механизм аутентификации, заключающийся в проверке PIN-кода (этот механизм предназначается для подтверждения бортовым устройством данных о личности держателя карточки, а не для защиты содержания карточки мастерской).

4.2.3 Отрицательный результат аутентификации

Ниже представлены функциональные задачи, определяющие реакцию карточки в каждом конкретном случае, когда аутентификация пользователя дает отрицательный результат.

Функциональная задача (FIA_AFL.1.1) *Номер*: 1, *перечень событий в процессе аутентификации*: аутентификация устройства считывания карточек.

Функциональная задача (FIA_AFL.1.2) *Перечень действий*:

- выдача предупреждения на подключенное устройство;
- занесение пользователя в категорию НЕ_БОРТОВОЕ_УСТРОЙСТВО.

Ниже представлены также функциональные задачи, определяющие реакцию карточки в случае, когда аутентификация посредством дополнительного механизма согласно UIA_302 дает отрицательный результат.

Функциональная задача (FIA_AFL.1.1) *Номер*: 5, *перечень событий в процессе аутентификации*: проверка PIN (карточка мастерской).

Функциональная задача (FIA_AFL.1.2) *Перечень действий*:

- выдача предупреждения на подключенное устройство;
- блокировка процедуры проверки PIN-кода таким образом, чтобы любой введенный после этого PIN-код отклонялся;
- возможность информирования последующих пользователей о причинах блокировки.

4.3 Контроль за доступом

4.3.1 Режим контроля за доступом

На стадии конечного использования карточки тахографа для нее предусмотрен единственный защитный режим контроля за доступом (SFP), обозначаемый как AC_SFP.

Функциональная задача (FDP_ACC.2.1) *Контроль за доступом SFP*: AC_SFP.

4.3.2 Функции контроля за доступом

Функциональная задача (FDP_ACF.1.1) *Контроль за доступом SFP*: AC_SFP.

Функциональная задача (FDP_ACF.1.1) *Заданная группа атрибутов защиты*: КАТЕГОРИЯ_ПОЛЬЗОВАТЕЛЕЙ.

Функциональная задача (FDP_ACF.1.2) *Правила, регулирующие доступ контролируемых субъектов к контролируемым объектам посредством контролируемых операций с контролируемыми объектами:*

- ОБЩЕЕ_ЧТЕНИЕ: Пользовательские данные могут считываться с АИ любым устройством; исключение составляют идентификационные данные держателя карточки, считывать которые с карточки контролера или карточки предприятия может только БОРТОВОЕ_УСТРОЙСТВО.

- СОХР._ИДЕНТ._ДАННЫХ: Идентификационные данные могут быть сохранены только один раз, причем до завершения 6-й стадии жизненного цикла карточки. Возможность сохранения или изменения идентификационных данных кем-либо из пользователей на стадии конечного использования карточки исключается.

СОХР._ДАННЫХ_О_ДЕЯТЕЛЬН.: Сохранять на АИ данные о деятельности может только БОРТОВОЕ_УСТРОЙСТВО.

ОБНОВЛЕНИЕ_ПО: Обновление программного обеспечения АИ пользователями не допускается.

СТРУКТУРА_ФАЙЛОВ: Структура файлов и условия доступа к ним определяются до завершения 6-й стадии жизненного цикла АИ и защищаются от любого последующего изменения или удаления кем-либо из пользователей.

4.4 Отчетность

АСТ_301 АИ должно содержать неизменяемые идентификационные данные.

АСТ_302 Должны быть указаны время и дата персонализации АИ. Возможность изменения этих данных должна быть исключена.

4.5 Контроль

АИ должно отслеживать события, свидетельствующие о потенциальном нарушении его защиты.

Функциональная задача (FAU_SAA.1.2) *Подмножество типовых событий, регистрируемых в надзорных целях:*

- отрицательный результат аутентификации держателя карточки (5 неправильных вводов PIN-кода подряд);
- ошибка самопроверки;
- ошибка при проверке целостности сохраненных данных;
- ошибка при проверке целостности вводимых данных о деятельности.

4.6 Достоверность

4.6.1 Целостность сохраненных данных

Функциональная задача (FDP_SDI.2.2) *Необходимые действия*: выдача предупреждения на подключенное устройство,

4.6.2 Аутентификация основных данных

Функциональная задача (FDP_DAU.1.1) *Перечень объектов или типов информации*: данные о деятельности.

Функциональная задача (FDP_DAU.1.2) *Перечень субъектов*: любые.

4.7 Надежность функционирования

4.7.1 Испытания

Выбор (FPT_TST.1.1): при включении, периодически в обычном режиме работы.

Примечание. "При включении" означает до исполнения команды (но не обязательно в ходе процедуры ответа на сигнал перезапуска).

RLB_301 Процедура самопроверки АИ включает проверку целостности любого программного обеспечения кроме хранящегося в ROM.

RLB_302 При обнаружении ошибки во время самопроверки ЗФАИ выдает предупреждение на подключенное устройство.

RLB_303 По окончании тестирования ОС все команды и функции, специально предназначенные для тестирования, блокируются или удаляются. Возможность снятия блокировки и повторного использования этих функций должна быть исключена. Команды, рассчитанные на использование в пределах какой-либо одной стадии жизненного цикла, должны быть полностью недоступными на других стадиях.

4.7.2 Программное обеспечение

RLB_304 Возможность анализа, отладки или изменения программного обеспечения АИ в полевых условиях должна быть исключена.

RLB_305 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.7.3 Питание

RLB_306 Защита АИ не должна нарушаться при отключении от источника питания или при изменениях параметров тока в цепи питания.

4.7.4 Перезапуск

RLB_307 При отключении питания (или при изменениях параметров тока в цепи питания) АИ, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, АИ полностью перезапускается.

4.8 Обмен данными

4.8.1 Обмен данными с бортовым устройством

DEX_301 АИ проверяет целостность и подлинность данных, импортируемых с бортового устройства.

DEX_302 В случае ошибки при проверке целостности импортируемых данных АИ:

- выдает предупреждение устройству, с которого поступают данные;
- не использует импортируемые данные.

DEX_303 АИ экспортирует пользовательские данные на бортовое устройство с соответствующими атрибутами защиты, позволяющими бортовому устройству проверять целостность и подлинность полученных данных.

4.8.2 Экспорт данных на устройства, не являющиеся бортовыми устройствами (функция загрузки)

DEX_304 АИ должно быть способно генерировать информацию, подтверждающую происхождение данных, загружаемых на внешний носитель.

DEX_305 АИ должно быть способно обеспечивать возможность проверки получателем информации, подтверждающей происхождение загруженных данных.

DEX_306 АИ должно быть способно загружать данные на внешний носитель с соответствующими атрибутами защиты, позволяющими проверять целостность загруженных данных.

4.9 Криптографическая защита

CSP_301 Если ЗФАИ генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей. Генерируемые криптографические сеансовые ключи должны быть пригодными для использования ограниченное количество раз *(количество определяется изготовителем, но не должно превышать 240)*.

CSP_302 Если ЗФАИ рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки криптографических ключей.

5. Определение механизмов защиты

Обязательные механизмы защиты указаны в подразделе XI.

Все остальные механизмы защиты определяются изготовителем АИ по собственному усмотрению.

6. Заявленная минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты карточки тахографа должна соответствовать **"Высокому"** уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты карточки тахографа по системе ITSEC должна соответствовать уровню **E3** согласно определению, содержащемуся в [ITSEC].

8. Обоснование

В ниеследующей таблице приводится обоснование дополнительных ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

		Опасности											ИТ-цели								
		У:CLON*	У:DIS_ES2	У:T_ES	У:T_CMD	У:MOD_SOFT*	У:MOD_LOAD	У:MOD_EXE	У:MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Доступ_к_данным	Криптообмен_данными
UIA_301	Средства аутентификации																			x	
UIA_302	Проверка PIN																			x	
ACT_301	Идент. данные																				
ACT_302	Данные персонализации																				
RLB_301	Целостность ПО												x		x						
RLB_302	Самотестирование												x		x						
RLB_303	Заводские испытания					x	x						x		x						
RLB_304	Анализ ПО					x		x	x				x		x						
RLB_305	Установка ПО					x	x		x				x		x						
RLB_306	Питание									x	x		x		x						
RLB_307	Перезагрузка												x		x						
DEX_301	Криптозащищенный импорт данных											x									x
DEX_302	Криптозащищенный импорт данных											x									x
DEX_303	Криптозащищенный экспорт данных на БУ											x									x
DEX_304	Доказательство происхождения											x									x
DEX_305	Доказательство происхождения											x									x
DEX_306	Криптозащищенный экспорт данных на ВН											x									x
CSP_301	Генерация ключей												x								x
CSP_302	Рассылка ключей												x								x

ПОДРАЗДЕЛ XI

ОБЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ

СОДЕРЖАНИЕ

1. Общие положения

Настоящий подраздел содержит конкретные указания относительно механизмов защиты, обеспечивающих:

- взаимную аутентификацию БУ и карточек тахографа, включая согласование сеансовых ключей;
- конфиденциальность, целостность и аутентификацию данных, передаваемых между БУ и карточками тахографа;
- целостность и аутентификацию данных, загружаемых с БУ и сохраняемых на внешнем носителе;
- целостность и аутентификацию данных, загружаемых с карточек тахографа и сохраняемых на внешнем носителе.

1.1 Источники

При подготовке настоящего подраздела использовались следующие источники:

SHA-1 National Institute of Standards and Technology (NIST). *FIPS Publication 180-1 : Secure Hash Standard.* April 1995.

PKCS1 RSA Laboratories. PKCS # 1 : *RSA Encryption Standard.* Version 2.0. October 1998.

TDES National Institute of Standards and Technology (NIST). *FIPS Publication 46-3 : Data Encryption Standard.* Draft 1999.

TDES-OP ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.

ISO/IEC 7816-4 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 4. Межотраслевые команды обмена данными. Издание первое, 1995 год + Поправка 1, 1997 год.

ISO/IEC 7816-6 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 6. Элементы межотраслевых данных для обмена информацией. Издание первое, 1996 год + Поправка 1, 1998 год.

ISO/IEC 7816-8 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 8. Межотраслевые команды обеспечения защиты. Издание первое, 1999 год.

ISO/IEC 9796-2 Информационные технологии. Методы защиты. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы с использованием хеш-функции. Издание первое, 1997 год.

ISO/IEC 9798-3 Информационные технологии. Методы защиты. Механизмы аутентификации объектов. Часть 3. Аутентификация объектов посредством алгоритма шифрования с открытым ключом. Издание второе, 1998 год.

ISO 16844-3 Транспорт дорожный. Тахографические системы. Часть 3. Интерфейс датчика движения.

1.2 Условные обозначения и сокращенные термины

В настоящем подразделе используются следующие условные обозначения и сокращенные термины:

(K_a, K_b, K_c)	набор ключей, используемый в рамках алгоритма тройного шифрования данных;
CA	(СО) сертификационный орган;
CAR	указатель сертификационного органа;
CC	(ККС) криптографическая контрольная сумма;
CG	криптограмма;
CH	заголовок команды;
CHA	полномочия держателя сертификата;
CHR	указатель держателя сертификата;
D()	расшифровка с помощью DES;
DE	элемент данных;
DO	(ОД) объект данных;
d	закрытый ключ в криптосистеме RSA, закрытая экспонента;
e	открытый ключ в криптосистеме RSA, открытая экспонента;
E()	шифрование с помощью DES;
EQT	аппаратура;
Hash()	значение хеш-функции, результат хеширования;
Hash	хеш-функция;
KID	идентификатор ключа;
Km	ключ TDES: ключ верхнего уровня, определение которого содержится в ISO 16844-3;
Km_{VU}	ключ TDES, вводимый в бортовые устройства;
Km_{WC}	ключ TDES, вводимый в карточки мастерских;
m	репрезентативный параметр сообщения, целое число от 0 до n-1;

n	ключ криптосистемы RSA, модуль;
PB	заполняющие байты;
PI	байт индикации заполнения (используется в криптограммах для обеспечения конфиденциальности объектов данных);
PV	простое значение;
s	репрезентативный параметр подписи, целое число от 0 до *n*-1;
SSC	(СИС) счетчик исходящих сообщений;
SM	(КЗОС) криптозащищенный обмен сообщениями;
TCBC	режим сцепления криптоблоков при тройном шифровании данных;
TDEA	алгоритм тройного шифрования данных;
TLV	"метка-длина-значение";
VU	(БУ) бортовое устройство;
X.C	сертификат, выданный сертификационным органом пользователю X;
X.CA	сертификационный орган пользователя X;
X.CA.PK $_{o}$ X.C	операция по расшифровке сертификата с целью извлечения открытого ключа. Используется двухкомпонентный оператор, левым компонентом которого является открытый ключ сертификационного органа, а правым компонентом - выданный этим сертификационный органом сертификат. Результатом операции является открытый ключ пользователя X, сертификат которого использовался в качестве правого компонента;
X.PK	открытый ключ пользователя X в криптосистеме RSA;
X.PK[I]	шифрование информации I по системе RSA с использованием открытого ключа пользователя X;
X.SK	закрытый ключ пользователя X в криптосистеме RSA;
X.SK[I]	шифрование информации I по системе RSA с использованием закрытого ключа пользователя X;
‘xx’	шестнадцатеричное значение;
||	оператор конкатенации.

2. Криптографические системы и алгоритмы

2.1 Криптографические системы

CSM_001 В бортовых устройствах и карточках тахографа применяется классический вариант криптосистемы RSA с открытым ключом для решения следующих задач защиты:

- взаимная аутентификация бортовых устройств и карточек;

- передача между бортовыми устройствами и карточками тахографа сеансовых ключей тройного шифрования по системе DES;
- цифровая подпись данных, загружаемых с бортовых устройств или карточек тахографа и сохраняемых на внешних носителях.

CSM_002 В бортовых устройствах и карточках тахографа используется симметричная криптосистема DES с тройным шифрованием информации для ее защиты от искажений при пользовательских операциях обмена данными между бортовыми устройствами и карточками тахографа и для обеспечения в необходимых случаях конфиденциальности данных, передаваемых между бортовым устройством и карточкой тахографа.

2.2 Криптографические алгоритмы

2.2.1 Алгоритм RSA

CSM_003 Алгоритм RSA полностью выражается следующими соотношениями:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Более всестороннее описание функции RSA можно найти в источниках [PKCS1]. При вычислениях по методу RSA в качестве открытой экспоненты, e, выбирается целое число в пределах от 3 до n-1, удовлетворяющее
условию gcd(e, lcm(p-1, q-1)) =1.

2.2.2 Хеш-алгоритм

CSM_004 В схемах цифровой подписи используется хеш-алгоритм SHA-1, описание которого приведено в источниках [SHA-1].

2.2.3 Алгоритм шифрования данных

CSM_005 Алгоритмы на базе DES применяются в режиме сцепления криптоблоков.

3. Ключи и сертификаты

3.1 Генерация и рассылка ключей

3.1.1 Генерация и рассылка ключей RSA

CSM_006 Ключи RSA генерируются на трех функциональных уровнях, которые образуют следующую иерархию:

- европейский уровень,
- уровень Договаривающихся сторон,
- аппаратный уровень.

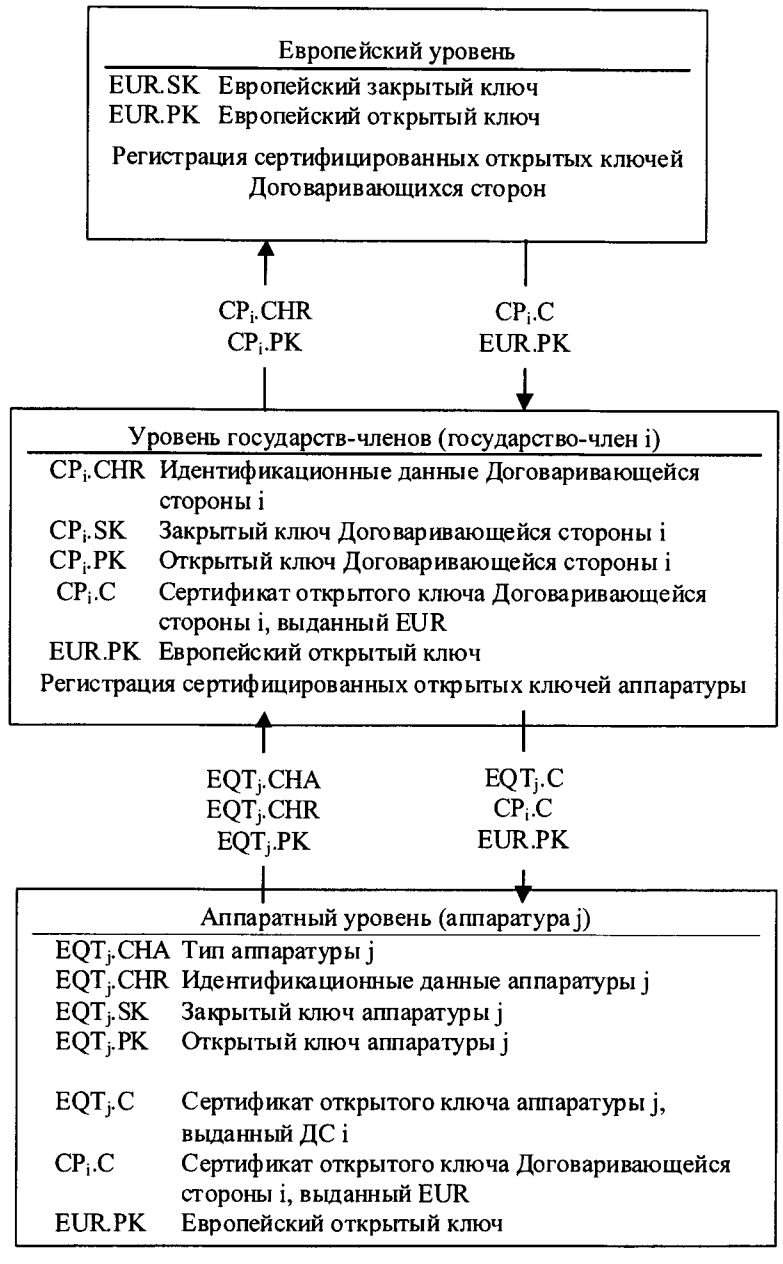
CSM_007 На европейском уровне генерируется единая пара общеевропейских ключей (EUR.SK и EUR.PK). Закрытый европейский ключ служит для сертификации открытых ключей Договаривающихся сторон. Все сертифицируемые ключи подлежат регистрации. Эти функции выполняет пользующийся международным признанием европейский сертификационный орган.

CSM_008 На уровне Договаривающихся сторон генерируется по паре ключей (CP.SK и CP.PK) для каждой Договаривающейся стороны. Открытые ключи Договаривающихся сторон сертифицируются европейским сертификационным органом. Закрытый ключ Договаривающейся стороны используется для сертификации открытых ключей, вводимых в соответствующие аппаратные средства (бортовые устройства и карточки тахографа). Все сертифицируемые открытые ключи подлежат регистрации с указанием аппаратуры, для которой они предназначены. Эти функции выполняет сертификационный орган Договаривающейся стороны. Договаривающаяся сторона может регулярно изменять свою пару ключей.

CSM_009 На аппаратном уровне генерируется единая пара ключей (EQT.SK и EQT.PK), вводимых в каждое устройство. Открытый ключ аппаратного уровня сертифицируется сертификационным органом Договаривающейся стороны. Эти функции могут выполняться изготовителями аппаратуры, предприятиями, персонализирующими аппаратуру, или соответствующими органами Договаривающихся сторон. Данная пара ключей служит для аутентификации, создания цифровых подписей и шифрования данных.

CSM_010 При генерации, транспортировке (если она необходима) и хранении закрытых ключей должен соблюдаться режим конфиденциальности.

Поток данных в ходе этого процесса схематически представлен на рисунке ниже.



3.1.2 Испытательные ключи RSA

CSM_011 В целях испытания аппаратуры (включая испытания на эксплуатационную совместимость) европейский сертификационный орган генерирует отдельную пару общеевропейских испытательных ключей и не менее двух пар испытательных ключей для Договаривающихся сторон, открытые ключи которых сертифицируются закрытым испытательным ключом общеевропейского уровня. При испытаниях, проводимых с целью официального утверждения типовых образцов, в испытываемую аппаратуру изготовителями вводятся испытательные ключи, сертифицированные одним из вышеупомянутых испытательных ключей Договаривающихся сторон.

3.1.3 Ключи датчиков движения

При генерации, транспортировке (если она необходима) и хранении трех ключей TDES, о которых говорится ниже, должен соблюдаться надлежащий режим конфиденциальности.

В целях обеспечения совместимости с контрольными устройствами, соответствующими стандарту ISO 16844, европейский сертификационный орган и сертификационные органы Договаривающихся сторон предпринимают нижеследующие дополнительные меры.

CSM_036 Европейский сертификационный орган генерирует Km_{VU} и Km_{WC} – два независимых уникальных ключа для тройного шифрования по системе DES – после чего вычисляет Km по формуле:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

По запросам сертификационных органов Договаривающихся сторон европейский сертификационный орган высылает им эти ключи с соблюдением надлежащих процедур защиты.

CSM_037 Сертификационные органы Договаривающихся сторон:

- используют ключ Km для шифрования показаний датчиков движения в соответствии с указаниями изготовителей этих датчиков (определение данных, подлежащих шифрованию ключом Km, дается в стандарте ISO 16844-3);
- с соблюдением надлежащих процедур защиты высылают KmVU заводам-изготовителям бортовых устройств для ввода в эти устройства;

- обеспечивают ввод KmWC во все карточки мастерских (запись SensorInstallationSecData в элементарном файле Sensor_Installation_Data) при персонализации карточек.

3.1.4 Генерация и рассылка сеансовых ключей T-DES

CSM_012 Бортовые устройства и карточки тахографа в рамках процесса взаимной аутентификации генерируют необходимые данные и обмениваются ими в целях составления единого сеансового ключа для тройного шифрования по системе DES. Для сохранения конфиденциальности этого обмена данными используется криптографическая защита RSA.

CSM_013 Составленный ключ используется при всех последующих операциях криптозащищенного обмена сообщениями. Он перестает действовать по окончании текущего сеанса (извлечение или перезагрузка карточки) и/или после 240-го использования (однократное использование ключа = передача на карточку одного криптозащищенного сообщения-команды и получение соответствующего ответа).

3.2 Ключи

CSM_014 Ключи RSA (независимо от уровня) имеют следующую длину: модуль n - 1024 бита, открытая экспонента e - до 64 бит, закрытая экспонента d - 1024 бита.

CSM_015 Ключи DES для тройного шифрования имеют вид (K_a, K_b, K_a), где K_a и K_b - независимые ключи длиной 64 бита. Биты контроля по четности не задаются.

3.3 Сертификаты

CSM_016 Сертификаты открытых ключей RSA должны быть "не содержащими самоописания" сертификатами с возможностью "проверки по карточке" (см. ISO/IEC 7816-8).

3.3.1 Содержание сертификатов

CSM_017 Сертификаты открытых ключей RSA составляются из следующих данных в следующем порядке:

Данные	Формат	Байты	Пояснение
CPI	ЦЕЛОЕ ЧИСЛО	1	Идентификатор профиля сертификата (в данной версии – "01")
CAR	ОКТЕТНАЯ СТРОКА	8	Указатель сертификационного органа
CHA	ОКТЕТНАЯ СТРОКА	7	Полномочия владельца сертификата
EOV	TimeReal	4	Дата истечения срока действия сертификата. Может не указываться; в этом случае поле заполняется байтами "FF".
CHR	ОКТЕТНАЯ СТРОКА	8	Указатель держателя сертификата
n	ОКТЕТНАЯ СТРОКА	128	Открытый ключ (модуль)
e	ОКТЕТНАЯ СТРОКА В	8	Открытый ключ (открытая экспонента)
		164	

Примечания:

1. "Идентификатор профиля сертификата" (CPI) определяет конкретную структуру сертификата, используемого в целях аутентификации. Он может применяться аппаратурой в качестве внутреннего идентификатора для вызова соответствующего списка заголовков, заключающего в себе описание конкатенации (последовательности) элементов данных, из которых состоит сертификат.

   Такой список заголовков, отражающий содержание сертификата, выглядит следующим образом:

‘4D’	‘16’	‘5F 29’	‘01 ’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	’81 80’	‘82’	‘08’
Расширенная метка списка заголовков	Длина списка заголовков	Метка CPI	Длина CPI	Метка CAR	Длина CAR	Метка CHA	Длина CHA	Метка EOV	Длина EOV	Метка CHR	Длина CHR	Метка открытого ключа (генерируется)	Длина последующих объектов данных	Метка модуля	Длина модуля	Метка открытой экспоненты	Длина открытой экспоненты

2. "Указатель сертификационного органа" (CAR) служит для обозначения сертификационного органа, выдавшего сертификат; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа сертификационного органа для указания на принадлежащий данному органу открытый ключ (информацию о соответствующих кодах см. ниже, в пункте, посвященном идентификаторам ключей).

3. "Полномочия держателя сертификата" (CHA) – указание на объем прав, предоставляемых сертификатом. Оно включает идентификатор приложения тахографа и тип аппаратуры, для которой предназначен сертификат (соответствует элементу данных EquipmentType; для Договаривающейся стороны используется значение "00").

4. "Указатель держателя сертификата" (CHR) предназначен для однозначной идентификации держателя данного сертификата; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа субъекта для указания на принадлежащий держателю сертификата открытый ключ.

5. Идентификаторы ключей позволяют однозначно идентифицировать держателя сертификата или сертификационный орган. Они кодируются следующим образом:

5.1 Аппаратура (БУ или карточка):

Данные	Серийный номер аппаратуры	Дата	Тип	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг BCD-код	Определяется изготовителем	Код изготовителя

Когда речь идет о бортовом устройстве, его изготовитель, запрашивая сертификаты, не обязательно должен знать идентификационные данные аппаратуры, в которую будут вводиться соответствующие ключи.

Если эти идентификационные данные изготовителю известны, то он направляет их вместе с открытым ключом на сертификацию в сертификационный орган своей Договаривающейся стороны. Выданный в результате сертификат будет содержать идентификационные данные аппаратуры, и изготовителю необходимо будет принять меры к тому, чтобы ключи и сертификат вводились именно в ту аппаратуру, для которой они предназначены. Идентификатор ключа при этом имеет вид, показанный выше.

Если идентификационные данные аппаратуры изготовителю не известны, то он должен снабдить каждую заявку на сертификат индивидуальным обозначением и сообщить это обозначение вместе с открытым ключом сертификационному органу своей Договаривающейся стороны на предмет сертификации. В выданном сертификате будет указано индивидуальное обозначение заявки. После ввода ключа в аппаратуру изготовитель должен информировать сертификационный орган своей Договаривающейся стороны о закреплении этого ключа за соответствующей аппаратурой (т.е. сообщить индивидуальное обозначение заявки на сертификат и идентификационные данные аппаратуры). При этом идентификатор ключа выглядит следующим образом:

Данные	Серийный номер заявки на выдачу сертификата	Дата	Тип	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг BCD-код	'FF'	Код изготовителя

5.2 Сертификационный орган:

Данные	Идентификационные данные органа	Серийный номер ключа	Дополнительная информация	Идентификатор
Длина	4 байта	1 байт	2 байта	1 байт
Значение	1-байтовый числовой код страны 3-байтовый буквенно-числовой код страны	Целое число	Дополнительный код (определяется серт. органом). Если не указан – "FF FF"	"01"

Серийный номер ключа позволяет отличать друг от друга различные ключи Договаривающейся стороны в случае смены ею своего ключа.

6. Сторона, проверяющая сертификат, должна по косвенным признакам распознавать сертифицируемый открытый ключ как ключ криптосистемы RSA, предназначенный для аутентификации, проверки цифровых подписей и шифрования конфиденциальной информации (сам сертификат не содержит прямо указывающих на это идентификаторов объектов).

3.3.2 Выдаваемые сертификаты

CSM_018 Выдаваемый сертификат представляет собой цифровую подпись с возможностью частичного восстановления содержания сертификата, соответствующую стандарту ISO/IEC 9796-2 (за исключением приложения A.4) и сопровождаемую "указателем сертификационного органа".

$$X.C = X.CA.SK[\text{‘6A’} \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, \text{‘BC’}] \,||\, C_n \,||\, X.CAR$$

При содержании сертификата

$= Cc =$	C_r	$\|\|$	C_n
	106 байт		58 байт

Примечания:

1. Длина данного сертификата составляет 194 байта.
2. К подписи также приобщается скрытый ею CAR, что позволяет использовать для проверки сертификата открытый ключ соответствующего сертификационного органа.
3. Сторона, проверяющая сертификат, должна по косвенным признакам определить алгоритм, использованный сертификационным органом для подписания сертификата.

4. Данному сертификату соответствует следующий список заголовков:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Метка сертификата CV (генерируется)	Длина последующих объектов данных	Метка подписи	Длина подписи	Метка остатка	Длина остатка	Метка CAR	Длина CAR

3.3.3 Проверка и расшифровка сертификатов

Процесс проверки и расшифровки сертификатов заключается в проверке подписи согласно стандарту ISO/IEC 9796-2, извлечении содержания сертификата, получении из него соответствующего открытого ключа (X.PK = X.CA.PK $_o$ X.C) и подтверждении действительности сертификата.

CSM_019 Этот процесс состоит из следующих этапов:

Проверка подписи и извлечение содержания:

- из X.C извлекаются Sign, C_n' и CAR':

X.C =	Sign	||	C_n'	||	CAR'
	128 байт		58 байт		8 байт

- из указателя CAR' выбирается открытый ключ соответствующего сертификационного органа (если он не выбран до этого иным способом);
- с помощью открытого ключа сертификационного органа расшифровывается содержание Sign : Sr'= X.CA.PK [Sign];
- проверяется Sr' (начальными символами должны быть "6A", конечными – "BC");
- вычисляются C_r' и H' по формуле:

Sr' =	'6A' ||	C_r'	||	H'	||	'BC'
		106 байт		20 байт		

- извлекается содержание сертификата C' = C_r' || C_n';
- проверяется *Hash*(C') = H'.

Положительный результат проверки указывает на подлинность сертификата, содержание которого соответствует C'.

Подтверждение действительности:

- если применимо, проверяется дата истечения срока действия сертификата, извлекаемая из C'.

Извлечение из C' и сохранение открытого ключа, идентификатора ключа, полномочий держателя сертификата и даты истечения срока его действия:

- X.PK = $n \| e$
- X.KID = CHR
- X.CHA = CHA
- X.EOV = EOV

4. Механизм взаимной аутентификации

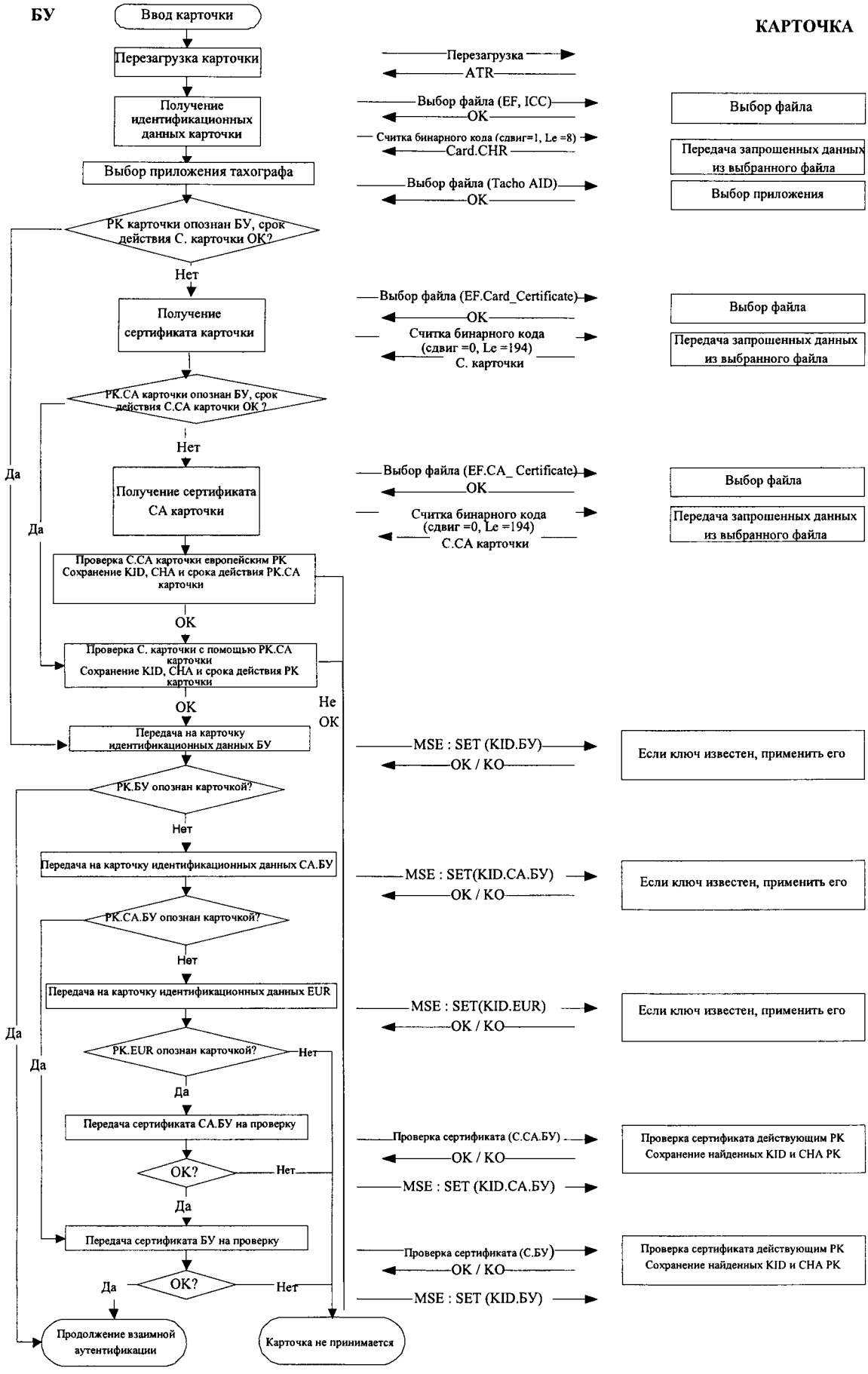
В основу механизма взаимной аутентификации карточек и БУ положен следующий принцип:

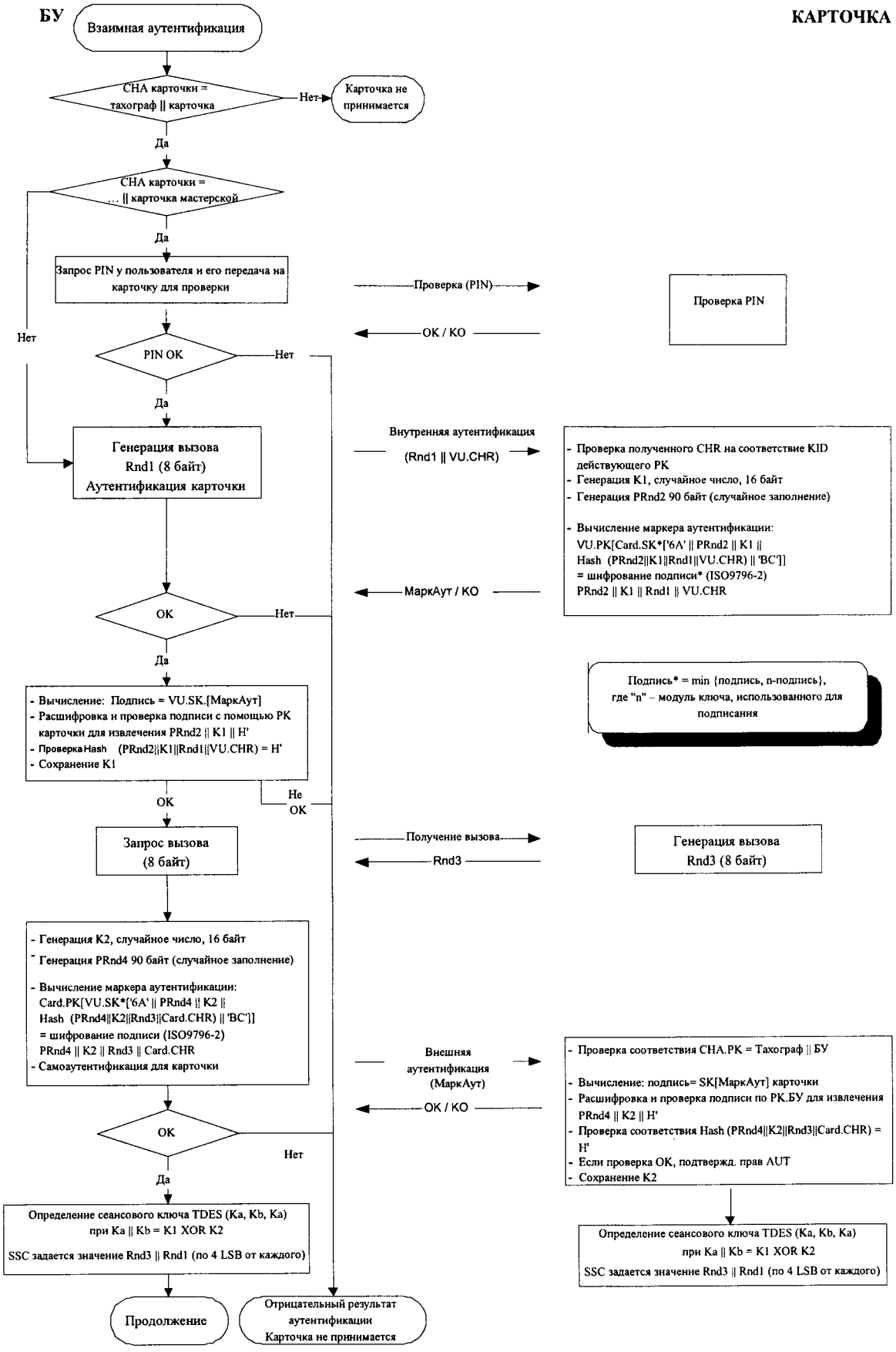
Каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован сертификационным органом Договаривающейся стороны, имеющим в свою очередь сертификат, выданный европейским сертификационным органом.

Доказательством служит подписание закрытым ключом случайной последовательности цифр, полученной от другой стороны, которая при проверке подписи должна восстановить из нее ту же последовательность цифр.

Данный механизм запускается со стороны БУ при вводе карточки в считывающее устройство. Процесс начинается с обмена сертификатами и извлечения открытых ключей и завершается созданием сеансового ключа.

CSM_020 При этом используется протокол, представленный ниже (стрелками показаны команды и передаваемые данные (см. подраздел II)):


БУ
КАРТОЧКА
Ввод карточки
Перезагрузка карточки
Перезагрузка
ATR
Получение идентификационных данных карточки
Выбор файла (EF, ICC)
OK
Выбор файла
Считка бинарного кода (сдвиг=1, Le =8)
Card.CHR
Передача запрошенных данных из выбранного файла
Выбор приложения тахографа
Выбор файла (Tacho AID)
OK
Выбор приложения
РК карточки опознан БУ, срок действия С. карточки ОК?
Нет
Получение сертификата карточки
Выбор файла (EF.Card_Certificate)
OK
Выбор файла
Считка бинарного кода (сдвиг =0, Le =194)
С. карточки
Передача запрошенных данных из выбранного файла
РК.СА карточки опознан БУ, срок действия С.СА карточки ОК ?
Нет
Да
Получение сертификата СА карточки
Выбор файла (EF.CA_ Certificate)
OK
Выбор файла
Считка бинарного кода (сдвиг =0, Le =194)
С.СА карточки
Передача запрошенных данных из выбранного файла
Да
Проверка С.СА карточки европейским РК
Сохранение KID, CHA и срока действия РК.СА карточки
OK
Проверка С. карточки с помощью РК.СА карточки
Сохранение KID, CHA и срока действия РК карточки
OK
Не ОК
Передача на карточку идентификационных данных БУ
MSE : SET (KID.БУ)
OK / KO
Если ключ известен, применить его
РК.БУ опознан карточкой?
Нет
Передача на карточку идентификационных данных СА.БУ
MSE : SET(KID.СА.БУ)
OK / KO
Если ключ известен, применить его
РК.СА.БУ опознан карточкой?
Нет
Передача на карточку идентификационных данных EUR
MSE : SET(KID.EUR)
OK / KO
Если ключ известен, применить его
Да
РК.EUR опознан карточкой?
Нет
Да
Передача сертификата СА.БУ на проверку
Проверка сертификата (С.СА.БУ)
OK / KO
Проверка сертификата действующим РК
Сохранение найденных KID и CHA РК
OK?
Нет
MSE : SET (KID.СА.БУ)
Да
Передача сертификата БУ на проверку
Проверка сертификата (С.БУ)
OK / KO
Проверка сертификата действующим РК
Сохранение найденных KID и CHA РК
Да
OK?
Нет
MSE : SET (KID.БУ)
Продолжение взаимной аутентификации
Карточка не принимается


БУ
КАРТОЧКА
Взаимная аутентификация
CHA карточки = тахограф || карточка
Нет
Карточка не принимается
Да
CHA карточки = ... || карточка мастерской
Да
Запрос PIN у пользователя и его передача на карточку для проверки
Проверка (PIN)
Проверка PIN
OK / KO
Нет
PIN OK
Нет
Да
Генерация вызова Rnd1 (8 байт) Аутентификация карточки
Внутренняя аутентификация
(Rnd1 || VU.CHR)
- Проверка полученного CHR на соответствие KID действующего PK
- Генерация K1, случайное число, 16 байт
- Генерация PRnd2 90 байт (случайное заполнение)
- Вычисление маркера аутентификации:
VU.PK[Card.SK*['6A' || PRnd2 || K1 ||
Hash (PRnd2||K1||Rnd1||VU.CHR) || 'BC']]
= шифрование подписи* (ISO9796-2)
PRnd2 || K1 || Rnd1 || VU.CHR
МаркАут / KO
OK
Нет
Да
Подпись* = min {подпись, n-подпись}, где "n" – модуль ключа, использованного для подписания
- Вычисление: Подпись = VU.SK.[МаркАут]
- Расшифровка и проверка подписи с помощью PK карточки для извлечения PRnd2 || K1 || H'
- Проверка Hash (PRnd2||K1||Rnd1||VU.CHR) = H'
- Сохранение K1
OK
Не OK
Запрос вызова (8 байт)
Получение вызова
Rnd3
Генерация вызова Rnd3 (8 байт)
- Генерация K2, случайное число, 16 байт
- Генерация PRnd4 90 байт (случайное заполнение)
- Вычисление маркера аутентификации:
Card.PK[VU.SK*['6A' || PRnd4 || K2 ||
Hash (PRnd4||K2||Rnd3||Card.CHR) || 'BC']]
= шифрование подписи (ISO9796-2)
PRnd4 || K2 || Rnd3 || Card.CHR
- Самоаутентификация для карточки
Внешняя аутентификация (МаркАут)
OK / KO
- Проверка соответствия CHA.PK = Тахограф || БУ
- Вычисление: подпись= SK[МаркАут] карточки
- Расшифровка и проверка подписи по PK.БУ для извлечения PRnd4 || K2 || H'
- Проверка соответствия Hash (PRnd4||K2||Rnd3||Card.CHR) = H'
- Если проверка OK, подтвержд. прав AUT
- Сохранение K2
OK
Нет
Да
Определение сеансового ключа TDES (Ka, Kb, Ka) при Ka || Kb = K1 XOR K2
SSC задается значение Rnd3 || Rnd1 (по 4 LSB от каждого)
Определение сеансового ключа TDES (Ka, Kb, Ka) при Ka || Kb = K1 XOR K2
SSC задается значение Rnd3 || Rnd1 (по 4 LSB от каждого)
Продолжение
Отрицательный результат аутентификации Карточка не принимается

5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками

5.1 Криптозащищенный обмен сообщениями

CSM_021 Неискаженность данных, передаваемых между БУ и карточками, обеспечивается благодаря криптозащите сообщений в соответствии с цитируемыми источниками [ISO/IEC 7816-4] и [ISO/IEC 7816-8].

CSM_022 При передаче данных, которые нуждаются в защите, к высылаемым в виде команды или ответа объектам данных добавляется объект, представляющий собой криптографическую контрольную сумму. Эта криптографическая контрольная сумма проверяется принимающим устройством.

CSM_023 В криптографической контрольной сумме данных, высылаемых в виде команды, учитываются заголовок команды и все содержащиеся в ней объекты данных (=>CLA = '0C', причем все эти объекты данных при их формировании снабжаются метками, где b1=1).

CSM_024 Байты ответа, несущие информацию о состоянии, защищаются с помощью криптографической контрольной суммы в тех случаях, когда ответ не содержит полей данных.

CSM_025 Криптографические контрольные суммы имеют длину 4 байта.

Таким образом, при криптозащищенном обмене сообщениями команды и ответы имеют структуру, показанную ниже.

Используемые здесь объекты данных представляют собой часть набора ОД для криптозащищенного обмена сообщениями, описание которого приводится в ISO/IEC 7816-4:

Метка	Мнемокод	Значение
'81'	T_{PV}	Простое значение: данные без кодировки BER-TLV (защищаются с помощью ККС)
'97'	T_{LE}	Значение Le в незащищенной команде (защищается с помощью ККС)
'99'	T_{SW}	Информация о состоянии (защищается с помощью ККС)
'8E'	T_{CC}	Криптографическая контрольная сумма
'87'	$T_{PI\,CG}$	Байт индикации заполнения || Криптограмма (Простое значение без кодировки BER-TLV)

Если незащищенная пара "команда-ответ" выглядит следующим образом:

Заголовок команды	Текст команды
CLA INS P1 P2	[поле L_c] [Поле данных] [поле L_e]
четыре байта	L байт, обозначаемые как байты от B_1 до B_L

Текст ответа	Концевая метка ответа	
[Поле данных]	SW1	SW2
L_r байт данных	два байта	

то соответствующая ей криптозащищенная пара "команда-ответ" имеет следующий вид:

Криптозащищенная команда:

Заголовок команды (CH)	Текст команды										
CLA INS P1 P2	[Новое поле L_c]	[Новое поле данных]									[Новое поле L_e]
'OC'	Длина нового поля данных	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
		'81'	L_c	Поле данных	'97'	'01'	L_e	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB, где

PB = заполняющие байты (80 .. 00) согласно стандартам ISO-IEC 7816-4 и ISO 9797 (метод 2).

Объекты данных PV и LE присутствуют лишь в случаях, когда незащищенная команда содержит соответствующие данные.

Криптозащищенный ответ:

1. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Текст ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Поле данных	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = T_{PV} || L_{PV} || PV || PB

2. Если поле данных ответа не является пустым и нуждается в защите конфиденциальности:

Текст ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Информация, передаваемая в виде криптограммы: данные без кодировки BER-TLV и заполняющие байты.

Данные, учитываемые в контрольной сумме = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Если поле данных ответа оставлено пустым:

Текст ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Новые SW1 SW2	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = T_{SW} || L_{SW} || SW || PB

5.2 Обработка ошибок при криптозащищенном обмене сообщениями

CSM_026 Когда карточка тахографа обнаруживает ошибку КЗОС при расшифровке команды, она возвращает соответствующие байты состояния, не используя КЗОС. В соответствии со стандартом ISO/IEC 7816-4 для указания на ошибки КЗОС предусматриваются следующие байты состояния:

'66 88': несоответствие криптографической контрольной суммы;

'69 87': отсутствие ожидаемых объектов данных КЗОС;

'69 88': неверные объекты данных КЗОС.

CSM_027 Если карточкой тахографа возвращены байты состояния без ОД КЗОС или с неверным ОД КЗОС, то БУ должно прервать сеанс обмена данными.

5.3 Алгоритм расчета криптографических контрольных сумм

CSM_028 Криптографические контрольные суммы вычисляются на основе алгоритма аутентификации сообщений retail-MAC в соответствии с ANSI X9.19 и системой DES:

- начальный этап: в качестве первого контрольного блока y0 используется E(Ka, SSC);
- последующие этапы: на основе Ka рассчитываются контрольные блоки y1, .. , yn;

- заключительный этап: по последнему контрольному блоку yn рассчитывается криптографическая контрольная сумма: E(Ka, D(Kb, yn)),

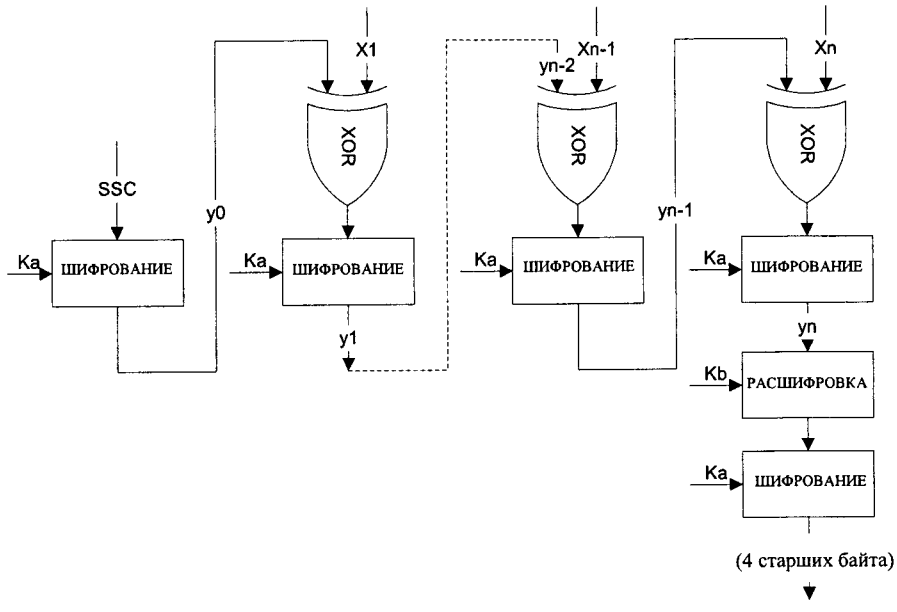
где E() означает шифрование по системе DES, а D() – расшифровка по системе DES.

Передаче подлежат четыре старших байта криптографической контрольной суммы.

CSM_029 В ходе процедуры согласования ключей счетчику исходящих сообщений (SSC) задаются следующие начальные значения: Initial SSC: Rnd3 (4 младших байта) || Rnd1 (4 младших байта).

CSM_030 Счетчик исходящих сообщений увеличивается на 1 единицу перед каждым вычислением MAC (кода аутентификации сообщения) (т.е. для первой команды значение SSC составляет Initial SSC + 1, а для первого ответа – Initial SSC + 2).

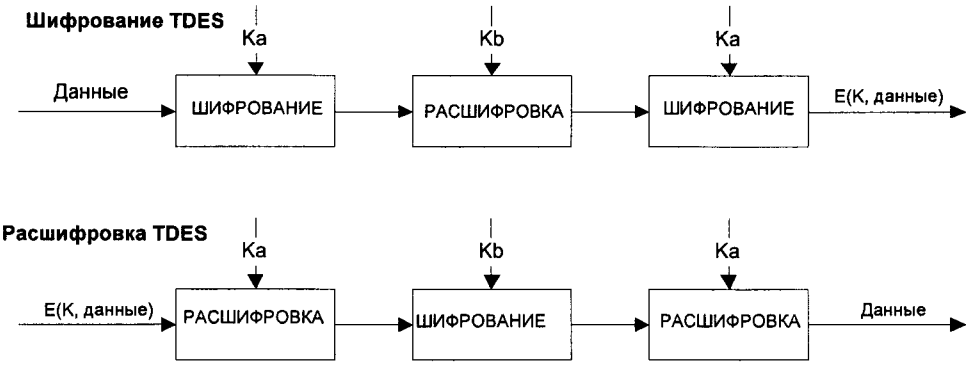
Способ вычисления retail-MAC изображен на диаграмме ниже.



5.4 Алгоритм расчета криптограмм для защиты конфиденциальности ОД

CSM_031 Криптограммы рассчитываются с помощью алгоритма TDEA в режиме TCBC, как указано в цитируемых источниках [TDES] и [TDES-OP], причем в качестве блока начальной величины используется нуль-вектор.

Применение ключей TDES показано на следующей диаграмме.



6. Механизмы цифровой подписи при загрузке данных

CSM_032 Данные, полученные из того или иного аппаратного источника (БУ или карточки) за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Этот файл должен заключать в себе сертификаты CP_i.C и EQT.C. Файл содержит цифровые подписи блоков данных в соответствии с указанным в подразделе VII (Протоколы загрузки данных).

CSM_033 Цифровые подписи загружаемых данных создаются по схеме, предполагающей добавление информации, которая позволяет при желании производить считку загруженных данных в нерасшифрованном виде.

6.1 Генерация подписей

CSM_034 Подписи данных генерируются аппаратурой согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1:

Подпись = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(данные))]

PS = Заполняющая октетная строка со значением ‘FF’, до общей длины 128.

DER(SHA-1(*M*)) – кодированное представление идентификатора алгоритма хеш-функции и значения хеш-функции в виде величины стандарта ASN.1 типа DigestInfo (правила однозначного шифрования):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||значение хеш-функции.

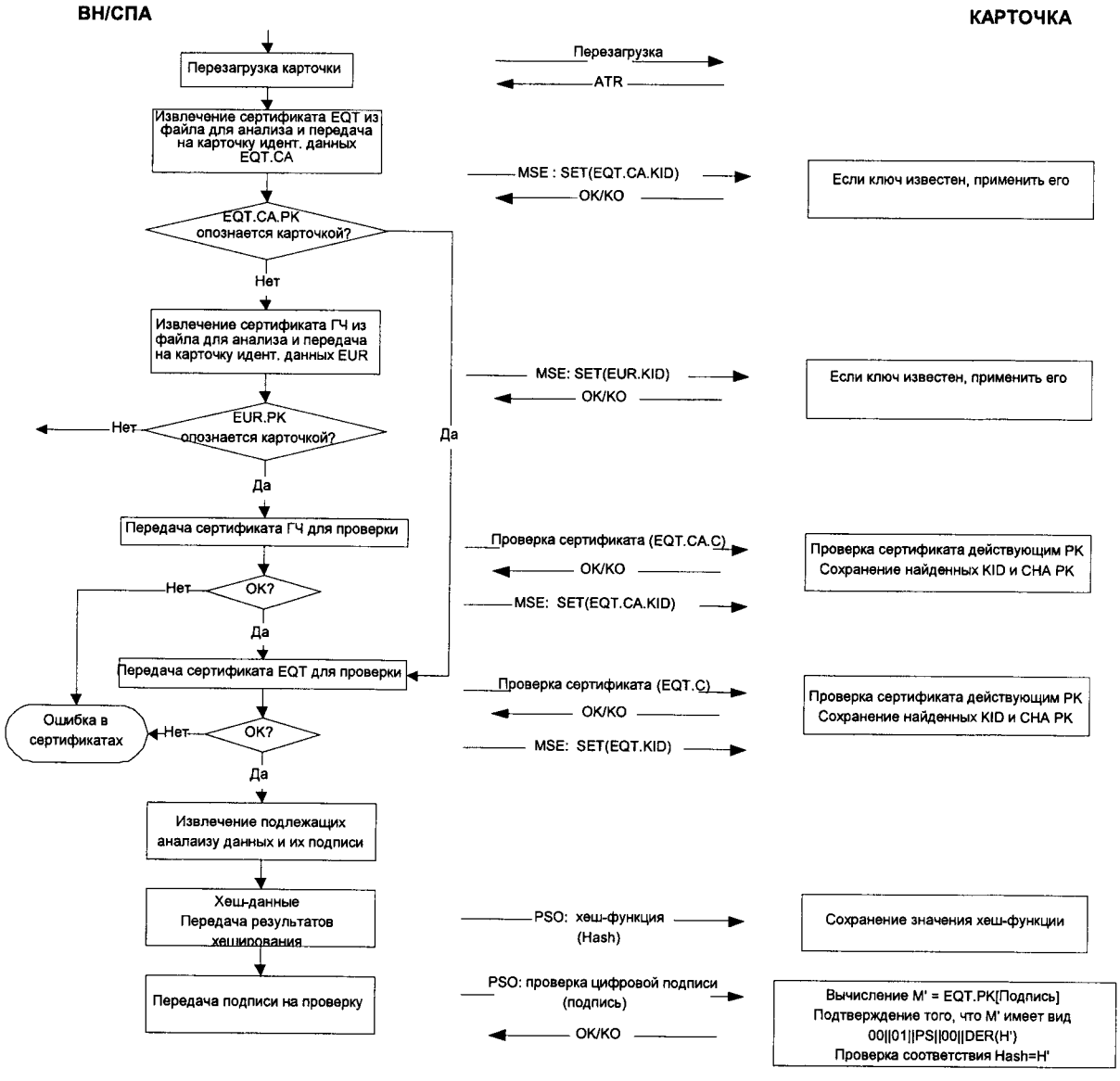
6.2 Проверка подписей

CSM_035 Проверка подписей загружаемых данных производится согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1.

Проверяющей стороне должен быть известен европейский открытый ключ EUR.PK, который она должна получить из независимого (и пользующегося доверием) источника.

В нижеследующей таблице представлен протокол, в соответствии с которым СПА после ввода в нее карточки контролера может проверять целостность загруженных данных, сохраненных на ВН (внешнем носителе). Для расшифровки цифровых подписей используется карточка контролера. В этом случае данная функция не обязательно должна быть предусмотрена в СПА.

Аппаратура, с помощью которой были загружены и подписаны подлежащие анализу данные, обозначена буквами EQT.


ВН/СПА
КАРТОЧКА
Перезагрузка карточки
Перезагрузка
ATR
Извлечение сертификата EQT из файла для анализа и передача на карточку идент. данных EQT.CA
MSE : SET(EQT.CA.KID)
OK/KO
Если ключ известен, применить его
EQT.CA.PK опознается карточкой?
Нет
Да
Извлечение сертификата ГЧ из файла для анализа и передача на карточку идент. данных EUR
MSE: SET(EUR.KID)
OK/KO
Если ключ известен, применить его
EUR.PK опознается карточкой?
Нет
Да
Передача сертификата ГЧ для проверки
Проверка сертификата (EQT.CA.C)
OK/KO
Проверка сертификата действующим PK
Сохранение найденных KID и CHA PK
Нет
OK?
MSE: SET(EQT.CA.KID)
Да
Передача сертификата EQT для проверки
Проверка сертификата (EQT.C)
OK/KO
Проверка сертификата действующим PK
Сохранение найденных KID и CHA PK
Ошибка в сертификатах
Нет
OK?
MSE: SET(EQT.KID)
Да
Извлечение подлежащих анализу данных и их подписи
Хеш-данные
Передача результатов хеширования
PSO: хеш-функция (Hash)
Сохранение значения хеш-функции
Передача подписи на проверку
PSO: проверка цифровой подписи (подпись)
OK/KO
Вычисление M' = EQT.PK[Подпись]
Подтверждение того, что M' имеет вид
00||01||PS||00||DER(H')
Проверка соответствия Hash=H'

- - - - -