Distr.: General
27 July 2018

Original: English/French

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

Group of Experts on European Agreement Concerning Work of Crews of Vehicles Engaged in International Road Transport (AETR)

Nineteenth session
Geneva, 15-16 October 2018
Item 2 (b) of the provisional agenda

Appendix 1C

Submitted by European Commission

This document, submitted by the European Commission, provides the amended text (in English and French) of Regulation (EU) 2016/799.

Official Journal of the European Union

L 85

English edition

Legislation

Volume 61

28 March 2018

Contents

[1] Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2018/502

of 28 February 2018

amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport ([1]), and in particular Articles 11 and 12(7) thereof,

Whereas:

(1) Regulation (EU) No 165/2014 has introduced smart tachographs, second-generation digital tachographs which include a connection to the global navigation satellite system ('GNSS') facility, a remote early detection communication facility, and an optional interface with intelligent transport systems.

(2) The technical requirements for the construction, testing, installation, operation and repair of tachographs and their components are set out in Commission Implementing Regulation (EU) 2016/799 ([2]).

(3) In accordance with Articles 8, 9 and 10 of Regulation (EU) No 165/2014, tachographs installed in vehicles registered for the first time on or after 15 June 2019 shall be smart tachographs. Implementing Regulation (EU) 2016/799 must therefore be amended so that the technical provisions laid down therein apply from that date.

(4) In order to comply with Article 8 of Regulation (EU) No 165/2014, which establishes that the position of the vehicle must be recorded every 3 hours of accumulated driving time, Implementing Regulation (EU) 2016/799 should be amended to enable information on the position of the vehicle to be stored with a 3-hour frequency, using a metric that cannot be reset, and to avoid confusion with 'continuous driving time', which is a metric with a different function.

(5) The vehicle unit may be a single unit or several units distributed in the vehicle. The GNSS and the Dedicated Short Range Communication ('DSRC') facilities could therefore be internal or external to the vehicle unit main body. When they are external, it should be possible that both facilities and the main body of the vehicle unit can be type-approved as components, in order to adapt the smart tachograph type-approval process to the needs of the market.

(6) The rules on the storage of time conflict events and time adjustments must be modified, in order to distinguish between the automatic time adjustments that are triggered following a possible tampering attempt or malfunctioning of the tachograph, and the time adjustments that are due to other reasons such as maintenance.

(7) The data identifiers should be able to distinguish between data downloaded from a smart tachograph and data downloaded from a tachograph of a previous generation.

([1]) OJ L 60, 28.2.2014, p. 1.

([2]) Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components (OJ L 139, 26.5.2016, p. 1).

(8) The validity period of the company card must be extended from 2 to 5 years, in order to align it with the validity period of the driver card.

(9) The description of certain faults and events, the validation of the entries of places where daily work period begins and/or end, the use of the driver consent for Intelligent Transport System ('ITS') interface regarding data transmitted by the vehicle unit through the vehicle network and other technical issues should be better defined.

(10) In order to ensure that the certification of tachograph seals is up to date, they need to be adjusted to the new standard on the security of the mechanical seals used on tachographs.

(11) This Regulation concerns the construction, testing, installation and operation of systems which are also comprised of radio equipment regulated by Directive 2014/53/EU of the European Parliament and of the Council [1]. This Directive regulates the placement on the market and putting into service of electronic and electrical equipment using radio waves for communication and/or radiodetermination at a horizontal level, with particular respect to electrical safety, compatibility with other systems, access to radio spectrum, access to emergency services and/or any additional delegated provisions. In order to guarantee the efficient use of radio spectrum, to prevent harmful radio interferences, to ensure the safety and the electromagnetic compatibility of the radio equipment and to allow any other specific delegated requirements, this Regulation should be without prejudice to that Directive.

(12) Implementing Regulation (EU) 2016/799 should therefore be amended.

(13) The measures provided for in this Regulation are in accordance with the opinion of the Committee referred to in Article 42(3) of Regulation (EU) No 165/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Implementing Regulation (EU) 2016/799 is amended as follows:

(1) Article 1 is amended as follows:

(a) the second and third paragraphs are replaced by the following:

'2. The construction, testing, installation, inspection, operation and repair of smart tachographs and their components, shall comply with the technical requirements set out in Annex IC to this Regulation.

3. Tachographs other than smart tachographs shall continue, as regards construction, testing, installation, inspection, operation and repair, to comply with the requirements of either Annex I to Regulation (EU) No 165/2014 or Annex IB to Council Regulation (EEC) No 3821/85 (*), as applicable;

(*) Council Regulation (EEC) No 3821/85 of 20 December 1985 on recording equipment in road transport (OJ L 370, 31.12.1985, p. 8).';

(b) the following paragraph 5 is added:

'5. This Regulation shall be without prejudice to Directive 2014/53/EU of the European Parliament and of the Council (*).

(*) Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).';

(2) Article 2 is amended as follows:

(a) definition (3) is replaced by the following:

'(3) "information folder" means the complete folder, in electronic or paper form, containing all the information supplied by the manufacturer or its agent to the type-approval authority for the purpose of the type-approval of a tachograph or a component thereof, including the certificates referred to in Article 12(3) of Regulation (EU) No 165/2014, the performance of the tests defined in Annex IC to this Regulation, as well as drawings, photographs, and other relevant documents;';

[1] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

(b) definition (7) is replaced by the following:

'(7) "smart tachograph" or "second generation tachograph" means a digital tachograph complying with Articles 8, 9 and 10 of Regulation (EU) No 165/2014 as well as with Annex IC to this Regulation;';

(c) definition (8) is replaced by the following:

'(8) "tachograph component" means any of the following elements: the vehicle unit, the motion sensor, the record sheet, the external GNSS facility and the external remote early detection facility;';

(d) the following definition (10) is added:

'(10) "vehicle unit" means the tachograph excluding the motion sensor and the cables connecting the motion sensor.

It may be a single unit or several units distributed in the vehicle and includes a processing unit, a data memory, a time measurement function, two smart card interface devices for driver and co-driver, a printer, a display, connectors and facilities for entering the user's inputs, a GNSS receiver and a remote communication facility.

The vehicle unit may be composed of the following components subject to type-approval:

— vehicle unit, as a single component (including GNSS receiver and remote communication facility),

— vehicle unit main body (including remote communication facility), and external GNSS facility,

— vehicle unit main body (including GNSS receiver), and external remote communication facility,

— vehicle unit main body, external GNSS facility, and external remote communication facility.

If the vehicle unit is composed of several units distributed in the vehicle, the vehicle unit main body is the unit containing the processing unit, the data memory, and the time measurement function.

"vehicle unit (VU)" is used for "vehicle unit" or "vehicle unit main body" ';

(3) in Article 6, the third paragraph is replaced by the following:

'However, Annex IC shall apply from 15 June 2019 with the exception of Appendix 16 which shall apply from 2 March 2016.';

(4) Annex IC is amended in accordance with Annex I to this Regulation;

(5) Annex II is amended in accordance with Annex II to this Regulation.

Article 2

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 28 February 2018.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX I

Annex IC to Regulation (EU) 2016/799 is amended as follows:

(1) the Table of Contents is amended as follows:

(a) point 3.12.5 is replaced by the following:

'3.12.5. Places and positions where daily work periods begin, end and/or where 3 hours accumulated driving time is reached';

(b) point 4.5.3.2.16 is replaced by the following:

'4.5.3.2.16 Three hours accumulated driving places data';

(c) point 4.5.4.2.14 is replaced by the following:

'4.5.4.2.14 Three hours accumulated driving places data';

(d) point 6.2 is replaced by the following:

'6.2 Check of new or repaired components';

(2) point 1 is amended as follows:

(a) definition (ll) is replaced by the following:

'(ll) "remote communication facility" or "remote early detection facility" means:

the equipment of the vehicle unit which is used to perform targeted roadside checks;';

(b) definition (tt) is replaced by the following:

'(tt) "time adjustment" means:

an adjustment of current time; this adjustment can be automatic at regular intervals, using the time provided by the GNSS receiver as a reference, or performed in calibration mode;';

(c) the first dash of definition (yy) is replaced by the following:

'— installed and used only in M1 and N1 type vehicles (as defined in Annex II to Directive 2007/46/EC of the European Parliament and of the Council (*), as last amended),';

(d) a new definition (fff) is added:

'(fff) "accumulated driving time" means:

a value representing the total accumulated number of minutes of driving of a particular vehicle.

The accumulated driving time value is a free running count of all minutes regarded as DRIVING by the monitoring of driving activities function of the recording equipment, and is only used for triggering the recording of the vehicle position, every time a multiple of three hours of accumulated driving is reached. The accumulation is started at the recording equipment activation. It is not affected by any other condition, like out of scope or ferry/train crossing.

The accumulated driving time value is not intended to be displayed, printed, or downloaded;';

(3) in point 2.3, the last indent of paragraph (13) is replaced by the following:

'— the vehicle units have a normal operations validity period of 15 years, starting with the vehicle unit certificates effective date, but vehicle units can be used for additional 3 months, for data downloading only.';

(4) in point 2.4, the first paragraph is replaced by the following:

'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 recording equipment and the tachograph cards, protecting the integrity and authenticity of data exchanged between the vehicle unit and the external GNSS facility, if any, protecting the confidentiality, integrity and authenticity of data exchanged through the remote early detection communication for control purposes, and verifying the integrity and authenticity of data downloaded.';

(5) in point 3.2, the second dash of paragraph (27) is replaced by the following:

'— positions where the accumulated driving time reaches a multiple of three hours;';

(6) in point 3.4, paragraph (49) is replaced by the following:

'(49) The first change of activity to BREAK/REST or AVAILABILITY 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).';

(7) in point 3.6.1, paragraph (59) is replaced by the following:

'(59) The driver shall then enter the current place of the vehicle, which shall be considered as a temporary entry.

Under the following conditions temporary entry made at last card withdrawal is validated (i.e. shall not be overwritten anymore):

— entry of a place where the current daily work period begins during manual entry according to requirement (61);

— the next entry of a place where the current daily work period begins if the card holder doesn't enter any place where the work period begins or ended during the manual entry according to requirement (61).

Under the following conditions temporary entry made at last card withdrawal is overwritten and the new value is validated:

— the next entry of a place where the current daily work period ends if the card holder doesn't enter any place where the work period begins or ended during the manual input according to requirement (61)';

(8) in point 3.6.2, the sixth and seventh dashes are replaced by the following:

'— a place where a previous daily work period ended, associated to the relevant time (thus overwriting and validating the entry made at the last card withdrawal),

— a place where the current daily work period begins, associated to the relevant time (thus validating a temporary entry made at last card withdrawal).';

(9) point 3.9.15 is replaced by the following:

'3.9.15 "Time conflict" event

(86) This event shall be triggered, **while not in calibration mode**, when the VU detects a discrepancy of more than 1 minute between the time of the vehicle unit's time measurement function and the time originating from the GNSS receiver. This event is recorded together with the internal clock value of the vehicle unit and comes together with an automatic time adjustment. After a time conflict event has been triggered, the VU will not generate other time conflict events for the next 12 hours. This event shall not be triggered in cases where no valid GNSS signal was detectable by the GNSS receiver for 30 days or more.';

(10) in point 3.9.17, the following dash is added:

'— ITS interface fault (if applicable)';

(11) point 3.10 is amended as follows:

(i) the text before the table in paragraph (89) is replaced by the following:

'The recording equipment shall detect faults through self-tests and built-in-tests, according to the following table:';

(ii) The following row is added to the table:

'ITS interface (optional)	Proper operation'	

(12) the second dash of point 3.12 is replaced by the following:

'— the average number of positions per day is defined as at least 6 positions where the daily work period begins, 6 positions when the accumulated driving time reaches a multiple of three hours, and 6 positions where the daily work period ends, so that "365 days" include at least 6570 positions,';

(13) point 3.12.5 is amended as follows:

(a) the heading and paragraph (108) are replaced by the following:

'3.12.5. Places and positions where daily work periods begin, end and/or where 3 hours accumulated driving time is reached

(108) The recording equipment shall record and store in its data memory:

— places and positions where the driver and/or co-driver begins his daily work period;

— positions where the accumulated driving time reaches a multiple of three hours;

— places and positions where the driver and/or the co-driver ends his daily work period.';

(b) the fourth dash of paragraph (110) is replaced by the following:

'— The type of entry (begin, end or 3 hours accumulated driving time),';

(c) paragraph (111) is replaced by the following:

'(111) The data memory shall be able to hold places and positions where daily work periods begin, end and/or where 3 hours accumulated driving time is reached for at least 365 days';

(14) in point 3.12.7, paragraph (116) is replaced by the following:

'(116) The recording equipment 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';

(15) the table in point 3.12.8 is amended as follows:

(a) the following item is inserted between the items 'Absence of position information from GNSS receiver' and 'Motion data error':

'Communication error with the external GNSS facility	— 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, — card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, — number of similar events that day.'

(b) The item 'Time conflict' is replaced by the following:

'Time conflict	— the most serious event for each of the 10 last days of occurrence (i.e. the ones with the greatest difference between recording equipment date and time, and GNSS date and time). — the 5 most serious events over the last 365 days.	— recording equipment date and time — GNSS date and time, — card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, — number of similar events that day.'

(16) in point 3.20 paragraph (200) is replaced by the following:

'(200) The recording equipment may also be equipped with standardised interfaces allowing the data recorded or produced by tachograph to be used in operational or calibration mode, by an external facility.

In Appendix 13, an optional ITS interface is specified and standardized. Other vehicle unit interfaces may co-exist, provided they fully comply with the requirements of Appendix 13 in term of minimum list of data, security and driver consent.

The driver consent doesn't apply to data transmitted by the recording equipment to the vehicle network. In case the personal data injected in the vehicle network are further processed outside the vehicle network, it is the responsibility of the vehicle manufacturer to have that personal data process compliant with Regulation (EU) 2016/679 ("General Data Protection Regulation").

The driver consent doesn't apply either to tachograph data downloaded to a remote company (requirement 193), as this scenario is monitored by the company card access right.

The following requirements apply to ITS data made available through that interface:

— these data are a set of selected existing data from the tachograph data dictionary (Appendix 1),

— a subset of these selected data are marked "personal data",

— the subset of "personal data" is only available if the verifiable consent of the driver, accepting his personal data can leave the vehicle network, is enabled,

— At any moment, the driver consent can be enabled or disabled through commands in the menu, provided the driver card is inserted,

— the set and subset of data will be broadcasted via Bluetooth wireless protocol in the radius of the vehicle cab, with a refresh rate of 1 minute,

— the pairing of the external device with the ITS interface will be protected by a dedicated and random PIN of at least 4 digits, recorded in and available through the display of each vehicle unit,

— in any circumstances, the presence of the ITS interface cannot disturb or affect the correct functioning and the security of the vehicle unit.

Other data may also be output in addition to the set of selected existing data, considered as the minimum list, provided they cannot be considered as personal data.

The recording equipment shall have the capacity to communicate the driver consent status to other platforms in the vehicle network.

When the ignition of the vehicle is ON, these data shall be permanently broadcasted.';

(17) in point 3.23, paragraph (211) is replaced by the following:

'(211) The time setting of the VU internal clock shall be automatically re-adjusted every 12 hours. When this re-adjustment is not possible because the GNSS signal is not available, the time setting shall be done as soon as the VU can access a valid time provided by GNSS receiver, according to the vehicle ignition conditions. The time reference for the automatic time setting of the VU internal clock shall be derived from the GNSS receiver.';

(18) in point 3.26, paragraphs (225) and (226) are replaced by the following:

'(225) A descriptive plaque shall be affixed to each separate component of the recording equipment and shall show the following details:

— name and address of the manufacturer,

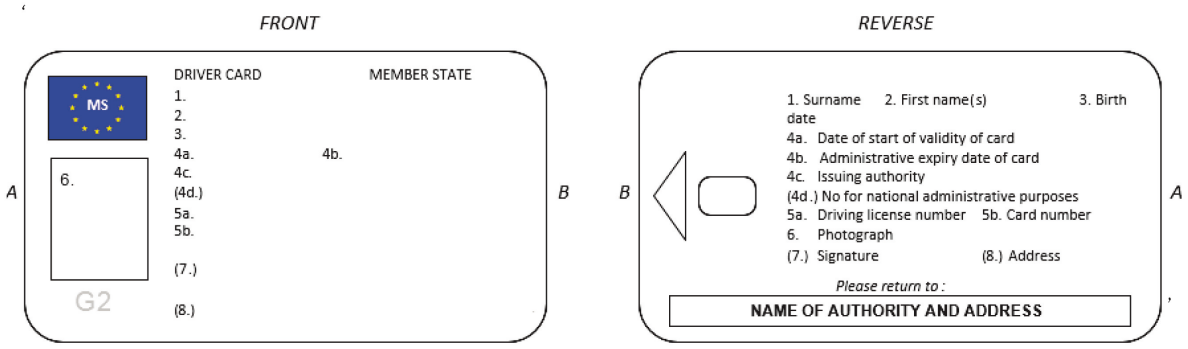
— manufacturer's part number and year of manufacture,

— serial number,

— type-approval mark.

(226) 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 part number.';

(19) in point 4.1, the drawing corresponding to the front and reverse of the driver card is replaced by the following:



(20) in point 4.5.3.1.8, the first dash in paragraph (263) is replaced by the following:

'— Card fault (where this card is the subject of the fault),';

(21) in point 4.5.3.2.8, the first dash in paragraph (288) is replaced by the following:

'— Card fault (where this card is the subject of the fault),';

(22) point 4.5.3.2.16 is replaced by the following:

'4.5.3.2.16 Three hours accumulated driving places data

(305) The driver card shall be able to store the following data related to the position of the vehicle where the accumulated driving time reaches a multiple of three hours:

— the date and time when the accumulated driving time reaches a multiple of three hours,

— the position of the vehicle,

— the GNSS accuracy, date and time when the position was determined,

— the vehicle odometer value.

(306) The driver card shall be able to store at least 252 such records.';

(23) point 4.5.4.2.14 is replaced by the following:

'4.5.4.2.14 Three hours accumulated driving places data

(353) The workshop card shall be able to store the following data related to the position of the vehicle where the accumulated driving time reaches a multiple of three hours:

— the date and time when the accumulated driving time reaches a multiple of three hours,

— the position of the vehicle,

— the GNSS accuracy, date and time when the position was determined,

— the vehicle odometer value.

(354) The workshop card shall be able to store at least 18 such records';

(24) in point 5.2, paragraph (396) is replaced by the following:

'(396) 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 recording equipment, 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 and the effective circumference of the wheel tyres were measured,

— the vehicle identification number,

— the presence (or not) of an external GNSS facility,

— the serial number of the external GNSS facility, if applicable,

— the serial number of the remote communication device, if any,

— the serial number of all the seals in place,

— the part of the vehicle where the adaptor, if any, is installed,

— the part of the vehicle where the motion sensor is installed, if not connected to the gear-box or an adaptor is not being used,

— a description of the colour of the cable between the adaptor and that part of the vehicle providing its incoming impulses,

— the serial number of the embedded motion sensor of the adaptor.';

(25) point 5.3 is amended as follows:

(a) a new paragraph (398a) is inserted after paragraph (398):

'(398a) The seals mentioned above shall be certified according to the standard EN 16882:2016.';

(b) in paragraph (401), the second sub-paragraph is replaced by the following:

'This unique identification number is defined as: MMNNNNNNNN by non-removable marking, with MM as unique manufacturer identification (database registration to be managed by EC) and NNNNNNNN seal alpha-numeric number, unique in the manufacturer domain.';

(c) paragraph (403) is replaced by the following:

'(403) Seals manufacturers shall be registered in a dedicated database when they get a seal model certified according to EN 16882:2016 and shall make their identification seals numbers public through a procedure to be established by the European Commission.';

(d) paragraph (404) is replaced by the following:

'(404) Approved workshops and vehicle manufacturers shall, in the frame of Regulation (EU) No 165/2014, only use seals certified according to EN 16882:2016 from those of the seals manufacturers listed in the database mentioned above.';

(26) point 6.2 is replaced by the following:

'6.2. Check of new or repaired components

(407) 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 3.2.1, 3.2.2, 3.2.3 and 3.3';

(27) in point 6.3, paragraph (408) is replaced by the following:

'(408) When being fitted to a vehicle, the whole installation (including the recording equipment) shall comply with the provisions relating to maximum tolerances laid down in Chapter 3.2.1, 3.2.2, 3.2.3 and 3.3. The whole installation shall be sealed in accordance with Chapter 5.3 and it shall include a calibration.';

(28) point 8.1 is amended as follows

(a) in point 8.1, the introduction text before paragraph (425) is replaced by the following:

'For the purpose of this chapter, the words "recording equipment" mean "recording equipment or its components". No type approval is required for the cable(s) linking the motion sensor to the VU, the external GNSS facility to the VU or the external remote communication facility to the VU. The paper, for use by the recording equipment, shall be considered as a component of the recording equipment.

Any manufacturer may ask for type approval of recording equipment component(s) with any other recording equipment component(s), provided each component complies with the requirements of this annex. Alternately, manufacturers may also ask for type approval of recording equipment.

As described in definition (10) in Article 2 of this Regulation, vehicle units have variants in components assembly. Whatever the vehicle unit components assembly, the external antenna and (if applicable) the antenna splitter connected to the GNSS receiver or to the remote communication facility are not part of the vehicle unit type approval.

Nevertheless, manufacturers having obtained type approval for recording equipment shall maintain a publicly available list of compatible antennas and splitters with each type approved vehicle unit, external GNSS facility and external remote communication facility.';

(b) paragraph (427) is replaced by the following:

'(427) Member States type approval authorities will not grant a type approval certificate as long as they do not hold:

— a security certificate (if requested by this Annex),

— a functional certificate,

— and an interoperability certificate (if requested by this Annex)

for the recording equipment or the tachograph card, subject of the request for type approval.';

(29) Appendix 1 is amended as follows:

(a) the Table of Content is amended as follows:

(i) point 2.63 is replaced by the following:

'2.63 Reserved for future use';

(ii) point 2.78 is replaced by the following:

'2.78 GNSSAccumulatedDriving';

(iii) point 2.79 is replaced by the following:

'2.79 GNSSAccumulatedDrivingRecord';

(iv) point 2.111 is replaced by the following:

'2.111 NoOfGNSSADRecords';

(v) point 2.160 is replaced by the following:

'2.160 Reserved for future use';

(vi) point 2.203 is replaced by the following:

'2.203 VuGNSSADRecord';

(vii) point 2.204 is replaced by the following:

'2.204 VuGNSSADRecordArray';

(viii) point 2.230 is replaced by the following:

'2.230 Reserved for future use';

(ix) point 2.231 is replaced by the following:

'2.231 Reserved for future use';

(b) in point 2, the following text is added before point 2.1:

'For card data types used for Generation 1 and Generation 2 applications, the size specified in this Appendix is the one for Generation 2 application. The size for Generation 1 application is supposed to be already known by the reader. The Annex IC requirement numbers related to such data types cover both Generation 1 and Generation 2 applications.';

(c) point 2.19 is replaced by the following:

'2.19. **CardEventData**

Generation 1:

Information, stored in a driver or workshop card, related to the events associated with the card holder (Annex IC requirements 260 and 318).

```
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).

Generation 2:

Information, stored in a driver or workshop card, related to the events associated with the card holder (Annex IC requirements 285 and 341).

```
CardEventData ::= SEQUENCE SIZE(11) 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).'

(d) point 2.30 is replaced by the following:

'2.30. **CardRenewalIndex**

A card renewal index (definition i)).

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Value assignment: (see this Annex chapter 7).

"0" First issue.

Order for increase: "0, …, 9, A, …, Z" ';

(e) in point 2.61, the text after the heading Generation 2 is replaced by the following:

```
'DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

In addition to generation 1 the following data elements are used:

noOfGNSSADRecords is the number of GNSS accumulated driving records the card can store.

noOfSpecificConditionRecords is the number of specific condition records the card can store.

noOfCardVehicleUnitRecords is the number of vehicle units used records the card can store.';

(f) point 2.63 is replaced by the following:

'2.63. **Reserved for future use**';

(g) in point 2.67, the text under the heading 'Generation 2' is replaced by the following:

'The same values as in generation 1 are used with the following additions:

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS interface module          (10),
--Plaque                        (11),--may be used in SealRecord
--M1/N1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Note 1: The generation 2 values for the Plaque, Adapter and the External GNSS connection as well as the generation 1 values for the Vehicle Unit and Motion Sensor may be used in SealRecord, i.e. if applicable.

Note 2: In the CardHolderAuthorisation (CHA) field of a generation 2 certificate, the values (1), (2), and (6) are to be interpreted as indicating a certificate for Mutual Authentication for the respective equipment type. For indicating the respective certificate for creating a digital signature, the values (17), (18) or (19) must be used.';

(h) in point 2.70, the text under the heading 'Generation 2' is replaced by the following:

'Generation 2:

'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	Vehicle Motion Conflict,
'0B'H	Time conflict (GNSS versus VU internal clock),
'0C'H	Communication error with the remote communication facility,
'0D'H	Absence of position information from GNSS receiver,
'0E'H	Communication error with the external GNSS facility,
'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	Tamper detection of GNSS,
'1A'H	External GNSS facility authentication failure,
'1B'H	External GNSS facility certificate expired,
'1C'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	Recording equipment 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	Internal GNSS receiver,
'37'H	External GNSS facility,
'38'H	Remote communication facility,
'39'H	ITS interface,
'3A'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.';

(i) Point 2.71 is replaced by the following:

'2.71. **ExtendedSealIdentifier**

Generation 2:

The extended seal identifier uniquely identifies a seal (Annex IC requirement 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode is a code of the manufacturer of the seal.

sealIdentifier is an identifier for the seal which is unique for the manufacturer.';

(j) points 2.78 and 2.79 are replaced by the following:

'2.78 **GNSSAccumulatedDriving**

Generation 2:

Information, stored in a driver or workshop card, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Annex IC requirement 306 and 354).

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord is the index of the last updated GNSS accumulated driving record.

Value assignment is the number corresponding to the numerator of the GNSS accumulated driving record, beginning with '0' for the first occurrence of the GNSS accumulated driving record in the structure.

gnssAccumulatedDrivingRecords is the set of records containing the date and time the accumulated driving reaches a multiple of three hours and information on the position of the vehicle.

2.79. **GNSSAccumulatedDrivingRecord**

Generation 2:

Information, stored in a driver or workshop card, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Annex IC requirement 305 and 353)

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

timeStamp is the date and time when the accumulated driving time reaches a multiple of three hours.

gnssPlaceRecord contains information related to the position of the vehicle.

vehicleOdometerValue is the odometer value when the accumulated driving time reaches a multiple of three hours.';

(k) point 2.86 is replaced by the following:

'2.86. **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, of a tachograph card or of an external GNSS facility.

The second choice is suitable to reference the public key of a Vehicle Unit (in cases where 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 Member State.';

(l) point 2.92 is replaced by the following:

'2.92. **MAC**

Generation 2:

A cryptographic check sum of 8, 12 or 16 bytes length corresponding to the cipher suites specified in Appendix 11.

```
MAC ::= CHOICE {
   Mac8                 OCTET STRING (SIZE(8)),
   Mac12                OCTET STRING (SIZE(12)),
   Mac16                OCTET STRING (SIZE(16)),
}';
```

(m) point 2.111 is replaced by the following:

'2.111. **NoOfGNSSADRecords**

Generation 2:

Number of GNSS accumulated driving records a card can store.

$$\texttt{NoOfGNSSADRecords ::= INTEGER (0..2}^{16}\texttt{-1)}$$

Value assignment: see Appendix 2.';

(n) in point 2.120, the value assignment '16H' is replaced by the following:

''16'H VuGNSSADRecord ';

(o) point 2.160 is replaced by the following:

'2.160. **Reserved for future use**';

(p) point 2.162 is replaced by the following:

'2.162. **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 UTC.

```
TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)
```

Value assignment – Octet aligned: Number of seconds since midnight 1 January 1970 UTC.

The max. possible date/time is in the year 2106.';

(q) point 2.179 is replaced by the following:

'2.179 **VuCardRecord**

Generation 2:

Information, stored in a vehicle unit, about a tachograph card used (Annex IC requirement 132).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation is the full card number and generation of the card used (data type 2.74).

cardExtendedSerialNumber as read from the file EF_ICC under the MF of the card.

cardStructureVersion as read from the file EF_Application_Identification under the DF_Tachograph_G2.

cardNumber as read from the file EF_Identification under the DF_Tachograph_G2.';

(r) points 2.203 and 2.204 are replaced by the following:

'2.203 **VuGNSSADRecord**

Generation 2:

Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Annex IC requirement 108, 110).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp is the date and time when the accumulated driving time reaches a multiple of three hours.

cardNumberAndGenDriverSlot identifies the card including its generation which is inserted in the driver slot.

cardNumberAndGenCodriverSlot identifies the card including its generation which is inserted in the co-driver slot.

gnssPlaceRecord contains information related to the position of the vehicle.

vehicleOdometerValue is the odometer value when the accumulated driving time reaches a multiple of three hours.

2.204 **VuGNSSADRecordArray**

Generation 2:

Information, stored in a vehicle unit, related to the GNSS position of the vehicle if the accumulated driving time reaches a multiple of three hours (Annex IC requirement 108 and 110).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType denotes the type of the record (VuGNSSADRecord).

Value Assignment: See RecordType.

recordSize is the size of the VuGNSSADRecord in bytes.

noOfRecords is the number of records in the set records.

records is a set of GNSS accumulated driving records.';

(s) points 2.230 and 2.231 are replaced by the following:

'2.230. Reserved for future use

2.231. Reserved for future use';

(t) in point 2.234, the text under the heading 'Generation 2' is replaced by the following:

```
'WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId               EquipmentType,
    cardStructureVersion                 CardStructureVersion,
    noOfEventsPerType                    NoOfEventsPerType,
    noOfFaultsPerType                    NoOfFaultsPerType,
    activityStructureLength              CardActivityLengthRange,
    noOfCardVehicleRecords               NoOfCardVehicleRecords,
    noOfCardPlaceRecords                 NoOfCardPlaceRecords,
    noOfCalibrationRecords               NoOfCalibrationRecords,
    noOfGNSSADRecords                    NoOfGNSSADRecords,
    noOfSpecificConditionRecords         NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords           NoOfCardVehicleUnitRecords
}
```

In addition to generation 1 the following data elements are used:

noOfGNSSADRecords is the number of GNSS accumulated driving records the card can store.

noOfSpecificConditionRecords is the number of specific condition records the card can store.

noOfCardVehicleUnitRecords is the number of vehicle units used records the card can store';

(30) Appendix 2 is amended as follows:

(a) in point 1.1, the following abbreviations are added:

'CHA Certificate Holder Authorisation

DO Data Object';

(b) point 3.3 is amended as follows:

(i) paragraph TCS_24 is replaced by the following:

'TCS_24 These security conditions can be linked in the following ways:

AND: All security conditions must be fulfilled

OR: At least one security condition must be fulfilled

The access rules for the file system, i.e. the SELECT, READ BINARY and UPDATE BINARY command, are specified in chapter 4. The access rules for the remaining commands are specified in the following tables. The term 'not applicable' is used if there is no requirement to support the command. In this case the command may or may not be supported, but the access condition is out of scope.';

(ii) in paragraph TCS_25, the table is replaced by the following:

'Command	Driver Card	Workshop Card	Control Card	Company Card
External Authenticate				
— For generation 1 authentication	ALW	ALW	ALW	ALW
— For generation 2 authentication	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Not applicable	Not applicable
PSO: Hash	Not applicable	Not applicable	ALW	Not applicable

Command	Driver Card	Workshop Card	Control Card	Company Card
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Not applicable	Not applicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Not applicable	Not applicable	ALW	Not applicable
Verify	Not applicable	ALW	Not applicable	Not applicable'

(iii) in paragraph TCS_26, the table is replaced by the following:

'Command	Driver Card	Workshop Card	Control Card	Company Card
External Authenticate				
— For generation 1 authentication	Not applicable	Not applicable	Not applicable	Not applicable
— For generation 2 authentication	ALW	PWD	ALW	ALW
Internal Authenticate	Not applicable	Not applicable	Not applicable	Not applicable
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Not applicable	ALW	ALW	Not applicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Not applicable	Not applicable
PSO: Hash	Not applicable	Not applicable	ALW	Not applicable
PERFORM HASH of FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Not applicable	Not applicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Not applicable	Not applicable	ALW	Not applicable
Verify	Not applicable	ALW	Not applicable	Not applicable'

(iv) in paragraph TCS_27, the table is replaced by the following:

'Command	Driver Card	Workshop Card	Control Card	Company Card
External Authenticate				
— For generation 1 authentication	Not applicable	Not applicable	Not applicable	Not applicable
— For generation 2 authentication	ALW	PWD	ALW	ALW
Internal Authenticate	Not applicable	Not applicable	Not applicable	Not applicable
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Compute Digital Signature	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Hash	Not applicable	Not applicable	Not applicable	Not applicable
PERFORM HASH of FILE	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Not applicable	Not applicable	Not applicable	Not applicable
Verify	Not applicable	ALW	Not applicable	Not applicable'

(c) in point 3.4, paragraph TCS_29 is replaced by the following:

'TCS_29 The status words 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	00	Authentication failed (Warning)
63	CX	Wrong CHV (PIN). Remaining attempts counter provided by "X".

SW1	SW2	Meaning
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)
68	83	Last command of the chain expected
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	80	Incorrect parameters in data field
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

Additional status words as defined in ISO/IEC 7816-4 can be returned, if their behaviour is not explicitly mentioned in this appendix.

For example the following status words can be optionally returned:

6881: Logical channel not supported

6882: Secure messaging not supported';

(d) in point 3.5.1.1, the last indent in paragraph TCS_38 is replaced by the following:

'— If the selected application is considered to be corrupted (integrity error is detected within the file attributes), the processing state returned is "**6400**" or "**6500**".';

(e) in point 3.5.1.2, the last indent in paragraph TCS_41 is replaced by the following:

'— If the selected file is considered to be corrupted (integrity error is detected within the file attributes), the processing state returned is "**6400**" or "**6500**".';

(f) in point 3.5.2.1, the sixth indent in paragraph TCS_43 is replaced by the following:

'— 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**".';

(g) point 3.5.2.1.1 is amended as follows:

(i) in paragraph TCS_45, the table is replaced by the following:

'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	"99h"	Tag for Processing Status (SW1-SW2) – optional for generation 1 secure messaging
#(3+L+NN)	1	"02h"	Length of Processing Status – optional for generation 1 secure messaging
#(4+L+NN) - #(5+L+NN)	2	"XX XXh"	Processing Status of the unprotected response APDU – optional for generation 1 secure messaging
#(6+L+NN)	1	"8Eh"	TCC: Tag for cryptographic checksum
#(7+L+NN)	1	"XXh"	LCC: Length of following cryptographic checksum "04h" for Generation 1 secure messaging (see Appendix 11 Part A) "08h", "0Ch" or "10h" depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)

'Byte	Length	Value	Description
#(8+L+NN)-#(7+M+L+NN)	M	"XX..XXh"	Cryptographic checksum
SW	2	"XXXXh"	Status Words (SW1,SW2)'

(ii) in paragraph TCS_46, the table is replaced by the following:

'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 LPI CG > 127 bytes.
#(2+L)-#(1+L+MM)	MM	"01XX..XXh"	Encrypted Data: Padding Indicator and cryptogram
#(2+L+MM)	1	"99h"	Tag for Processing Status (SW1-SW2) – optional for generation 1 secure messaging
#(3+L+MM)	1	"02h"	Length of Processing Status – optional for generation 1 secure messaging
#(4+L+MM) - #(5+L+MM)	2	"XX XXh"	Processing Status of the unprotected response APDU – optional for generation 1 secure messaging
#(6+L+MM)	1	"8Eh"	TCC: Tag for cryptographic checksum
#(7+L+MM)	1	"XXh"	LCC: Length of following cryptographic checksum "04h" for Generation 1 secure messaging (see Appendix 11 Part A) "08h", "0Ch" or "10h" depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)
#(8+L+MM)- #(7+N+L+MM)	N	"XX..XXh"	Cryptographic checksum
SW	2	"XXXXh"	Status Words (SW1,SW2)'

(h) in point 3.5.2.2, the sixth indent in paragraph TCS_50 is replaced by the following:

'— 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**".';

(i) in point 3.5.2.3, paragraph TCS_52 is amended as follows:

(i) the last row of the table is replaced by the following:

'Le	1	'XXh'	As specified in ISO/IEC 7816-4'

(ii) the following sentence is added:

'In case of T = 0 the card assumes the value Le = "00h" if no secure messaging is applied.

In case of T = 1 the processing state returned is "6700" if Le="01h".';

(j) in point 3.5.2.3, the sixth indent in paragraph TCS_53 is replaced by the following:

'— 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**".';

(k) in point 3.5.3.2, the sixth indent in paragraph TCS_63 is replaced by the following:

'— 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**".';

(l) in point 3.5.5, paragraph TCS_72 is replaced by the following:

'TCS_72 The PIN entered by the user must be ASCII encoded and right padded with "FFh" bytes up to a length of 8 bytes by the IFD, see also the data type WorkshopCardPIN in Appendix 1.';

(m) in point 3.5.8, paragraph TCS_95 is replaced by the following:

'TCS_95 If the INTERNAL AUTHENTICATE command is successful, the current generation 1 session key, if existing, is erased and no longer available. In order to have a new generation 1 session key available, the EXTERNAL AUTHENTICATE command for the generation 1 authentication mechanism must be successfully performed.

Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain INTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys.';

(n) in point 3.5.9, paragraph TCS_97 is replaced by the following:

'TCS_97 The command variant for the second generation VU-card mutual authentication can be performed in the MF, DF Tachograph and DF Tachograph_G2, see also TCS_34. If this generation 2 EXTERNAL AUTHENTICATE command is successful, the current generation 1 session key, if existing, is erased and no longer available.

Note: For generation 2 session keys see Appendix 11 CSM_193 and CSM_195. If generation 2 session keys are established and the tachograph card receives the plain EXTERNAL AUTHENTICATE command APDU, it aborts the generation 2 secure messaging session and destroys the generation 2 session keys.';

(o) in point 3.5.10, the following row is added to the table in paragraph TCS_101:

'5 + L + 1	1	"00h"	As specified in ISO/IEC 7816-4'

(p) in point 3.5.11.2.3, the following paragraphs are added in paragraph TCS_114:

'— If the currentAuthenticatedTime of the card is later than the Expiration Date of the selected public key, the processing state returned is **"6A88".**

Note: In the case of a MSE: SET AT for VU Authentication command, the referenced key is a VU_MA public key. The card shall set the VU_MA public key for use, if available in its memory, which matches the Certificate Holder Reference (CHR) given in the command data field (the card can identify VU_MA public keys by means of the certificate's CHA field). A card shall return "6A 88" to this command in case only the VU_Sign public key or no public key of the Vehicle Unit is available. See the definition of the CHA field in Appendix 11 and of data type equipmentType in Appendix 1.

Similarly, in case an MSE: SET DST command referencing an EQT (i.e. a VU or a card) is sent to a control card, according to CSM_234 the referenced key is always an EQT_Sign key that has to be used for the verification of a digital signature. According to Figure 13 in Appendix 11, the control card will always have stored the relevant EQT_Sign public key. In some cases, the control card may have stored the corresponding EQT_MA public key. The control card shall always set the EQT_Sign public key for use when it receives an MSE: SET DST command.';

(q) point 3.5.13 is amended as follows:

(i) paragraph TCS_121 is replaced by the following:

'TCS_121 The temporarily stored hash of file value shall be deleted if a new hash of file value is computed by means of the PERFORM HASH of FILE command, if a DF is selected, and if the tachograph card is reset.';

(ii) paragraph TCS_123 is replaced by the following:

'TCS_123 The Tachograph Generation 2 application shall support the SHA-2 algorithm (SHA-256, SHA-384 or SHA-512), specified by the cipher suite in Appendix 11 Part B for the card signature key Card_Sign.';

(iii) the table in paragraph TCS_124 is replaced by the following:

'Byte	Length	Value	Description
CLA	1	"80h"	CLA
INS	1	"2Ah"	Perform Security Operation
P1	1	"90h"	Tag: Hash
P2	1	"00h"	Algorithm implicitly known For the Tachograph Generation 1 application: SHA-1 For the Tachograph Generation 2 application: SHA-2 algorithm (SHA-256, SHA-384 or SHA-512) defined by the cipher suite in Appendix 11 Part B for the card signature key Card_Sign'

(r) point 3.5.14 is amended as follows:

the text below the heading and until paragraph TCS_126 is replaced by the following:

'This command is used to compute the digital signature of previously computed hash code (see PERFORM HASH of FILE, §3.5.13).

Only the driver card and the workshop card are required to support this command in the DF Tachograph and DF Tachograph_G2.

Other types of tachograph cards may or may not implement this command. In case of the Generation 2 tachograph application, only the driver card and the workshop card have a generation 2 signature key, other cards are not able to successfully perform the command and terminate with a suitable error code.

The command may or may not be accessible in the MF. If the command is not accessible in the MF, it shall terminate with a suitable error code.

This command is compliant with ISO/IEC 7816-8. The use of this command is restricted regarding the related standard.';

(s) point 3.5.15 is amended as follows:

(i) the table in paragraph TCS_133 is replaced by the following:

'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	"XXh"	Length Lc of the subsequent data field
#6	1	"9Eh"	Tag for Digital Signature
#7 or #7-#8	L	"NNh" or "81 NNh"	Length of digital signature (L is 2 bytes if the digital signature is longer than 127 bytes): 128 bytes coded in accordance with Appendix 11 Part A for Tachograph Generation 1 application. Depending on the selected curve for Tachograph Generation 2 application (see Appendix 11 Part B).
#(7+L)-#(6+L+NN)	NN	"XX..XXh"	Digital signature content'

(ii) the following indent is added to paragraph TCS_134:

'— If the selected public key (used to verify the digital signature) has a CHA.LSB (CertificateHolderAuthorisation.equipmentType) that is not suitable for the digital signature verification according to Appendix 11, the processing state returned is "**6985**".';

(t) point 3.5.16 is amended as follows:

(i) in paragraph TCS_138, the following row is added to the table:

'5 + L + 1	1	'00h'	As specified in ISO/IEC 7816-4'

(ii) the following sub-paragraph is added to paragraph TCS_139:

'— "**6985**" indicates that the 4-byte time stamp provided in the command data field is earlier than cardValidityBegin or later than cardExpiryDate.';

(u) point 4.2.2 is amended as follows:

(i) in the data structure in paragraph TCS_154, the lines from DF Tachograph G2 to EF CardMA_Certificate, and the lines from EF GNSS_Places to the end of this paragraph are replaced by the following:

'

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*20268*	*40316*	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*17*	*17*	
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		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
GNSSContinuousDriving		*4538*	*6050*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n_8	*18*	*18*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

,

(ii) in paragraph TCS_155, the item NoOfGNSSCDRecords of the table is replaced by the following:

‘n_8	NoOfGNSSADRecords	252	336’

(v) in point 4.3.1, the text corresponding to the abbreviation SC4 in paragraph TCS_156 is replaced by the following:

‘**SC4** For the READ BINARY command with even INS byte:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

For the READ BINARY command with odd INS byte (if supported): NEV’;

(w) point 4.3.2 is amended as follows:

(i) in the data structure in paragraph TCS_162, the lines from DF Tachograph G2 to EF CardMA_Certificate, the lines from EF Calibration to extendedSealIdentifier and the lines from EF GNSS_Places to vehicleOdometerValue are replaced by the following:

‘

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*18783*	*49787*	
EF Application_Identification		*19*	*19*	
WorkshopCardApplicationIdentification		*19*	*19*	
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		2	2	{00 00}
noOfCalibrationRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

…

EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
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}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

,

(ii) the item NoOfGNSSCDRecords of the table in paragraph TCS_163 is replaced by the following:

'n_8	NoOfGNSSADRecords	18	24'

(31) in Appendix 3, point 2 is amended as follows:

(a) the following line is inserted after the line with the pictograms 'Location start of daily work period' and 'Location end of daily work period':

'  Position after 3 hours accumulated driving time';

(b) the pictogram combination 'time adjustment (by workshop)', is replaced by the following:

 Time conflict or time adjustment (by workshop)';

(c) the following pictogram combinations are added to the Events list:

'  Absence of position information from GNSS receiver or Communication error with the external GNSS facility;

 Communication error with the remote communication facility ';

(32) Appendix 4 is amended as follows:

(a) point 2 is amended as follows:

(i) block number 11.4 is replaced by the following:

'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
longitude of the recorded position	lon ±DDD°MM.M'
latitude of the recorded position	lat ± DD°MM.M'
timestamp when position was determined	hh:mm
Odometer	x xxx xxx **km**'

(ii) block number 11.5 is replaced by the following:

'11.5	*Positions after 3 hours accumulated driving time* pi=position after 3 hours accumulated driving time longitude of the recorded position latitude of the recorded position timestamp when position was determined Odometer	pihh:mm lon ± DDD°MM.M' lat ± DD°MM.M ' hh:mm x xxx xxx **km**'

(b) in point 3.1, position 11.5 of the daily printout format is replaced by the following:

'11.5	Positions after 3 hours accumulated driving time in chronological order'

(c) in point 3.2, the daily printout format is replaced by the following:

'1	Date and time at which the document is printed
2	Type of printout
3	Card holder identification (for all cards inserted in VU + GEN)
4	Vehicle identification (vehicle from which printout is taken)
5	VU identification (VU from which printout is taken + GEN)
6	Last calibration of this VU
7	Last control on this tachograph
9	Driver activities delimiter
10	Driver slot delimiter (slot 1)
10a	Out of scope condition in the beginning of this day
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activities in chronological order (driver slot)
10	Co-driver slot delimiter (slot 2)
10a	Out of scope condition in the beginning of this day
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
11.5	Positions after 3 hours accumulated driving time in chronological order
11.7	Activity totals
11.2	Summary of periods without card in co-driver slot
11.4	Places entered in chronological order
11.5	Positions after 3 hours accumulated driving time in chronological order

11.8	Activity totals
11.3	Summary of activities for a driver both slots included
11.4	Places entered by this driver in chronological order
11.5	Positions after 3 hours accumulated driving time in chronological order
11.9	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)
22.1	Control place
22.2	Controller's signature
22.3	From time (space available for a driver without a card to indicate
22.4	To time which periods are relevant to himself)
22.5	Driver's signature'

(d) in point 3.7, paragraph PRT_014 is replaced by the following:

'PRT_014 The historic of inserted cards 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 identifications (of all cards inserted in the VU)
23	Most recent card inserted in the VU
23.1	Inserted cards (up to 88 records)
12.3	Faults delimiter'

(33) Appendix 7 is amended as follows:

(a) point 1.1 is replaced by the following:

'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 Appendix 11 Common Security Mechanisms. The source equipment (VU or card) identification and its security certificates (Member state and equipment) are also downloaded. The verifier of the data must possess independently a trusted European public key.

Data downloaded from a VU are signed using Appendix 11 Common Security Mechanisms Part B (Second-generation tachograph system), except when drivers' control is performed by a non EU control authority, using a first generation control card, in which case data are signed using Appendix 11 Common Security Mechanisms Part A (First-generation tachograph system), as requested by Appendix 15 Migration, requirement MIG_015.

This Appendix specifies therefore two types of data downloads from the VU:

— Generation 2 type of VU data download, providing the generation 2 data structure, signed using Appendix 11 Common Security Mechanisms Part B,

— Generation 1 type of VU data download, providing the generation 1 data structure, signed using Appendix 11 Common Security Mechanisms Part A.

Similarly, there are two types of data downloads from second generation driver cards inserted in a VU, as specified in paragraphs 3 and 4 of this Appendix.';

(b) point 2.2.2 is amended as follows:

(i) the table is replaced by the following:

'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 or 21		97
Activities	80	EE	F0	06	36	02 or 22	Date	CS
Events & Faults	80	EE	F0	02	36	03 or 23		99
Detailed Speed	80	EE	F0	02	36	04 or 24		9A
Technical Data	80	EE	F0	02	36	05 or 25		9B
Card download	80	EE	F0	02	36	06	Slot	CS

Message Structure	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte CheckSum
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
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'

(ii) the following indents are added to the Notes after the table:

'— TRTP 21 to 25 are used for Generation 2 type of VU data download requests, TRTP 01 to 05 are used for Generation 1 type of VU data download requests, which can only be accepted by the VU in the frame of drivers' control performed by a non EU control authority, using a first generation control card,

— TRTP 11 to 19 and 31 to 39 are reserved for manufacturer specific download requests.';

(c) point 2.2.2.9 is amended as follows:

(i) paragraph DDP_011 is replaced by the following:

'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. For VU data download, two different TRTP values can be used for each transfer type:

Data transfer type	TRTP value for generation 1 type of VU data download	TRTP value for generation 2 type of VU data download
Overview	01	21
Activities of a specified date	02	22
Events and faults	03	23
Detailed speed	04	24
Technical data	05	25

Data transfer type	TRTP value
Card download	06'

(ii) paragraph DDP_054 is replaced by the following:

'DDP_054 It is mandatory for the IDE to request the overview data transfer (TRTP 01 or 21) 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 or 22) the Transfer Data Request message includes the indication of the calendar day (`TimeReal` format) to be downloaded.';

(d) in point 2.2.2.10, paragraph DDP_055 is replaced by the following:

'DDP_055 In the first case (TREP 01 or 21), 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.';

(e) in point 2.2.2.16, the last dash in paragraph DDP_018 is replaced by the following:

'— FA data not available

The data object of a data transfer request are not available in the VU (e.g. no card is inserted, generation 1 type of VU data download requested outside the frame of a driver's control by a non EU control authority…).';

(f) point 2.2.6.1 is amended as follows:

(i) the first sub-paragraph in paragraph DDP_029 is replaced by the following:

'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 or 21 Hex and appropriate sub message splitting and counting:';

(ii) the heading 'Data structure generation 1' is replaced by the following:

'Data structure generation 1 (TREP 01 Hex)';

(iii) the heading "Data structure generation 2" is replaced by the following:

'Data structure generation 2 (TREP 21 Hex)';

(g) point 2.2.6.2 is amended as follows:

(i) the first sub-paragraph in paragraph DDP_030 is replaced by the following:

'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 or 22 Hex and appropriate sub message splitting and counting:';

(ii) the heading 'Data structure generation 1' is replaced by the following:

'Data structure generation 1 (TREP 02 Hex)';

(iii) the heading 'Data structure generation 2' is replaced by the following:

'Data structure generation 2 (TREP 22 Hex)';

(iv) the item VuGNSSCDRecordArray under the heading 'Data structure generation 2 (TREP 22 Hex)', is replaced by the following:

'VuGNSSADRecordArray	GNSS positions of the vehicle when the accumulated driving time of the vehicle reaches a multiple of three hours. If the section is empty, an array header with noOfRecords = 0 is sent.'

(h) point 2.2.6.3 is amended as follows:

(i) the first sub-paragraph in paragraph DDP_031 is replaced by the following:

'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 or 23 Hex and appropriate sub message splitting and counting:';

(ii) the heading 'Data structure generation 1' is replaced by the following:

'Data structure generation 1 (TREP 03 Hex)';

(iii) the heading 'Data structure generation 2' is replaced by the following:

'Data structure generation 2 (TREP 23 Hex)';

(iv) the item VuTimeAdjustmentGNSSRecordArray under the heading 'Data structure generation 2 (TREP 23 Hex)' is deleted;

(i) point 2.2.6.4 is amended as follows:

(i) the first sub-paragraph in paragraph DDP_032 is replaced by the following:

'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 or 24 Hex and appropriate sub message splitting and counting:';

(ii) the heading 'Data structure generation 1' is replaced by the following:

'Data structure generation 1 (TREP 04)';

(iii) the heading 'Data structure generation 2' is replaced by the following:

'Data structure generation 2 (TREP 24)';

(j) point 2.2.6.5 is amended as follows:

(i) the first sub-paragraph in paragraph DDP_033 is replaced by the following:

'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 or 25 Hex and appropriate sub message splitting and counting:';

(ii) the heading 'Data structure generation 1' is replaced by the following:

'Data structure generation 1 (TREP 05)';

(iii) the heading 'Data structure generation 2' is replaced by the following:

'Data structure generation 2 (TREP 25)';

(k) in point 3.3, paragraph DDP_035 is replaced by the following:

'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.

— (for first and second generation tachograph cards) Download EFs within Tachograph DF:

— 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, using Appendix 11 Common Security Mechanisms Part A.

— It is mandatory to download at least the EFs Application_Identification and Identification 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,

— (for second generation tacograph cards only) Except when a download of a driver card inserted in a VU is performed during drivers' control by a non EU control authority, using a first generation control card, download EFs within Tachograph_G2 DF:

— Download the EFs CardSignCertificate, CA_Certificate and Link_Certificate (if present). 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_G2 DF) except EF Card_Download. This information is secured with a digital signature, using Appendix 11 Common Security Mechanisms Part B.

— It is mandatory to download at least the EFs Application_Identification and Identification 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,
  — VehicleUnits_Used,
  — GNSS Places.
— When downloading a driver card, update the LastCardDownload date in EF Card_Download, in the Tachograph and, if applicable, Tachograph_G2 DFs.

— When downloading a workshop card, reset the calibration counter in EF Card_Download in the Tachograph and, if applicable, Tachograph_G2 DFs.

— When downloading a workshop card the EF `Sensor_Installation_Data` in the `Tachograph` and, if applicable, `Tachograph_G2` DFs shall not be downloaded.';

(l) in point 3.3.2, the first subparagraph in paragraph DDP_037 is replaced by the following:

'The sequence to download EFs ICC, IC, Card_Certificate (or CardSignCertificate for DF Tachograph_G2), CA_Certificate and Link_Certificate (for DF Tachograph_G2 only) is as follows:';

(m) in point 3.3.3, the table is replaced by the following:

'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 Appendix 11, part A or B. 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** 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'

(n) in point 3.4.2, paragraph DDP_046 is replaced by the following:

'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) in the Tachograph or for common information of the card	3 Bytes
FID (2 Bytes) || "01"	Tag for Signature of EF (FID) in the Tachograph DF	3 Bytes
FID (2 Bytes) || "02"	Tag for EF (FID) in the Tachograph_G2 DF	3 Bytes
FID (2 Bytes) || "03"	Tag for Signature of EF (FID) in the Tachograph_G2 DF	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 (in the Tachograph DF)
05 05 01	00 80	Signature of EF Vehicles_Used (in the Tachograph DF)
05 05 02	0A 2E	Data of EF Vehicles_Used in the Tachograph_G2 DF
05 05 03	xx xx	Signature of EF Vehicles_Used in the Tachograph_G2 DF'

(o) in point 4, paragraph DDP_049 is replaced by the following:

'DDP_049 First generation driver cards: Data shall be downloaded using the first generation data download protocol, and downloaded data shall have the same format as data downloaded from a first generation vehicle unit.

Second generation driver cards: the VU shall then download the whole card, file by file, in accordance with the card downloading protocol defined in paragraph 3, 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.';

(34) in point 2 of Appendix 8, the paragraph under the heading 'references' is replaced by the following:

'ISO 14230-2: Road Vehicles -Diagnostic Systems — Keyword Protocol 2000- Part 2: Data Link Layer.

First edition: 1999.';

(35) Appendix 9 is amended as follows:

(a) in the Table of Contents, point 6 is replaced by the following:

'6. EXTERNAL REMOTE COMMUNICATION FACILITY TESTS';

(b) in point 1.1, the first dash is replaced by the following:

'— a **security certification**, based on Common Criteria specifications, against a security target fully compliant with Appendix 10 to this Annex,';

(c) in point 2, the table of the vehicle unit functional tests is replaced by the following:

'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.	88, 89,91
2	**Visual inspection**		
2,1	Compliance with documentation		
2.2	Identification / markings		224 to 226
2.3	Materials		219 to 223
2.4	Sealing		398, 401 to 405
2.5	External interfaces		
3	**Functional tests**		
3.1	Functions provided		02, 03, 04, 05, 07, 382
3.2	Modes of operation		09 to 11*, 134, 135
3.3	Functions and data access rights		12* 13*, 382, 383, 386 to 389
3.4	Monitoring cards insertion and withdrawal		15, 16, 17, 18, 19*, 20*, 134
3.5	Speed and distance measurement		21 to 31
3.6	Time measurement (test performed at 20 °C)		38 to 43
3.7	Monitoring driver activities		44 to 53, 134
3.8	Monitoring driving status		54, 55, 134
3.9	Manual entries		56 to 62
3.10	Company locks management		63 to 68
3.11	Monitoring control activities		69, 70
3.12	Detection of events and/or faults		71 to 88, 134

No	Test	Description	Related requirements
3.13	Equipment identification data		93*, 94*, 97, 100
3.14	Driver card insertion and withdrawal data		102* to 104*
3.15	Driver activity data		105* to 107*
3.16	Places and positions data		108* to 112*
3.17	Odometer data		113* to 115*
3.18	Detailed speed data		116*
3.19	Events data		117*
3.20	Faults data		118*
3.21	Calibration data		119* to 121*
3.22	Time adjustment data		124*, 125*
3.23	Control activity data		126*, 127*
3.24	Company locks data		128*
3.25	Download activity data		129*
3.26	Specific conditions data		130*, 131*
3.27	Recording and storing on tachographs cards		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Displaying		90, 134, 151 to 168, PIC_001, DIS_001
3.29	Printing		90, 134, 169 to 181, PIC_001, PRT_001 to PRT_014
3.30	Warning		134, 182 to 191, PIC_001
3.31	Data downloading to external media		90, 134, 192 to 196
3.32	Remote communication for targeted roadside checks		197 to 199
3.33	Output data to additional external devices		200, 201
3.34	Calibration		202 to 206*, 383, 384, 386 to 391
3.35	Roadside calibration checking		207 to 209
3.36	Time adjustment		210 to 212*
3.37	Non-interference of additional functions		06, 425

No	Test	Description	Related requirements
3.38	Motion sensor interface		02, 122
3.39	External GNSS facility		03, 123
3.40	Verify that the VU detects, records and stores the event(s) and/or fault(s) defined by the VU manufacturer when a paired motion sensor reacts to magnetic fields disturbing vehicle motion detection.		217
3.41	Cypher suite and standardized domain parameters		CSM_48, CSM_50
4	**Environmental tests**		
4.1	Temperature	Verify functionality through: Test according to ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) This test refers to IEC 60068-2-1: Environmental testing - Part 2-1: Tests - Test A: Cold Test according to ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h at 70 °C) This test refers to IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Test according to ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cycles, dwell time 2h at each 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	213
4.2	Humidity	Verify that the vehicle unit can withstand a cyclic damp (heat test) through IEC 60068-2-30, 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	214
4.3	Mechanical	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 60068-2-6, test Fc, with a minimum test duration of 3 × 12 hours (12 hours per axis) ISO 16750-3 does not require a sinusoidal vibration test for devices located in the decoupled vehicle cab.	219

No	Test	Description	Related requirements
		2. Random vibrations: Test according to ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Random vibration test, 10…2000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 axes, 32 h per axis, including temperature cycle – 20…70 °C. This test refers to IEC 60068-2-64: Environmental testing - Part 2-64: Tests - Test Fh: Vibration, broadband random and guidance 3. Shocks: mechanical shock with 3 g half sinus according ISO 16750. The tests described above are performed on different samples of the equipment type being tested.	
4.4	Protection against water and foreign bodies	Test according to ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (No change in parameters); Minimum value IP 40	220, 221
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 12V versions: 17V at + 40 °C 1 hour(ISO 16750-2)	216
4.6	Reverse polarity protection	Verify that the vehicle unit can withstand an inversion of its power supply (ISO 16750-2)	216
4.7	Short-circuit protection	Verify that input output signals are protected against short circuits to power supply and ground (ISO 16750-2)	216
5	**EMC tests**		
5.1	Radiated emissions and susceptibility	Compliance with Regulation ECE R10	218
5.2	Electrostatic discharge	Compliance with ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for contact and +/– 8 kV for air discharge	218

No	Test	Description	Related requirements
5.3	Conducted transient susceptibility on power supply	For 24V versions: compliance with ISO 7637-2 + ECE Regulation No. 10 Rev. 3: pulse 1a: Vs=450V Ri=50 ohms pulse 2a: Vs=+37V Ri=2 ohms pulse 2b: Vs=+20V Ri=0,05 ohms pulse 3a: Vs=– 150V Ri=50 ohms pulse 3b: Vs=+150V 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 + ECE Regulation No. 10 Rev. 3: pulse 1: Vs=– 75V Ri=10 ohms pulse 2a: Vs=+37V Ri=2 ohms pulse 2b: Vs=+10V Ri=0,05 ohms pulse 3a: Vs=– 112V Ri=50 ohms pulse 3b: Vs=+75V Ri=50 ohms pulse 4: Vs=– 6V Va=– 5V t6=15ms pulse 5: Vs=+65V Ri=3ohms 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 For load dump proposal, refer to ISO 16750-2, 4th edition, chapter 4.6.4.	218’

(d) point 6 is replaced by the following:

‘6. EXTERNAL REMOTE COMMUNICATION FACILITY TEST

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		225, 226
2.3	Materials		219 to 223
3.	**Functional tests**		
3.1	Remote communication for targeted roadside checks		4, 197 to 199

No	Test	Description	Related requirements
3.2	Recording and storing in data memory		91
3.3	Communication with Vehicle Unit		Appendix 14 DSC_66 to DSC_70, DSC_71 to DSC_76
4.	**Environmental tests**		
4.1	Temperature	Verify functionality through: Test according to ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) This test refers to IEC 60068-2-1: Environmental testing - Part 2-1: Tests - Test A: Cold Test according to ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h @ 70 °C) This test refers to IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Test according to ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cycles, dwell time 1 h at each 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	213
4.2	Protection against water and foreign bodies	Test according to ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (targeted value IP40)	220, 221
5	**EMC tests**		
5.1	Radiated emissions and susceptibility	Compliance with Regulation ECE R10	218
5.2	Electrostatic discharge	Compliance with ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for contact and +/– 8 kV for air discharge	218

No	Test	Description	Related requirements
5.3	Conducted transient susceptibility on power supply	For 24V versions: compliance with ISO 7637-2 + ECE Regulation No. 10 Rev. 3: pulse 1a: Vs=– 450V Ri=50 ohms pulse 2a: Vs=+37V Ri=2 ohms pulse 2b: Vs=+20V Ri=0,05 ohms pulse 3a: Vs=– 150V Ri=50 ohms pulse 3b: Vs=+150V 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 + ECE Regulation No. 10 Rev. 3: pulse 1: Vs=-75V Ri=10 ohms pulse 2a: Vs=+37V Ri=2 ohms pulse 2b: Vs=+10V Ri=0,05 ohms pulse 3a: Vs=– 112V Ri=50 ohms pulse 3b: Vs=+75V Ri=50 ohms pulse 4: Vs=– 6V Va=– 5V t6=15ms pulse 5: Vs=+65V Ri=3ohms 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 For load dump proposal, refer to ISO 16750-2, 4th edition, chapter 4.6.4.	218’

(e) the table in point 8 on interoperability tests is replaced by the following:

‘No	Test	Description
8.1 Interoperability tests between vehicle units and tachograph cards		
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 vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through daily printouts that all corresponding recordings can be properly read

No	Test	Description
		8.2 Interoperability tests between vehicle units and motion sensors
1	Pairing	Check that the pairing between the vehicle units and the motion sensors runs normally
2	Activity tests	Execute a typical activity scenario on the motion sensor. The scenario shall involve a normal activity and creating as many events or faults as possible. Verify through a vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through a daily printout that all corresponding recordings can be properly read
		8.3 Interoperability tests between vehicle units and external GNSS facilities (when applicable)
1	Mutual authentication	Check that the mutual authentication (coupling) between the vehicle unit and the external GNSS module runs normally.
2	Activity tests	Execute a typical activity scenario on the external GNSS facility. The scenario shall involve a normal activity and creating as many events or faults as possible. Verify through a vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through a daily printout that all corresponding recordings can be properly read'

(36) Appendix 11 is amended as follows:

(a) in point 8.2.3, paragraph CSM_49 is replaced by the following:

'CSM_49 Vehicle units, tachograph cards and external GNSS facilities shall support the SHA-256, SHA-384 and SHA-512 algorithms specified in [SHS].';

(b) in point 9.1.2, the first sub-paragraph of paragraph CSM_58 is replaced by the following:

'CSM_58 Whenever it generates a new European root key pair, the ERCA shall create a link certificate for the new European public key and sign it with the previous European private key. The validity period of the link certificate shall be 17 years plus 3 months. This is shown in Figure 1 in section 9.1.7 as well.';

(c) in point 9.1.4, paragraph CSM_72 is replaced by the following:

'CSM_72 Two unique ECC key pairs shall be generated for each vehicle unit, designated as VU_MA and VU_Sign. This task is handled by VU manufacturers. Whenever a VU key pair is generated, the party generating the key shall send the public key to its MSCA, in order to obtain a corresponding VU certificate signed by the MSCA. The private key shall be used only by the vehicle unit.';

(d) point 9.1.5 is amended as follows:

(i) paragraph CSM_83 is replaced by the following:

'CSM_83 One unique ECC key pair, designated as Card_MA, shall be generated for each tachograph card. A second unique ECC key pair, designated as Card_Sign, shall additionally be generated for each driver card and each workshop card. This task may be handled by card manufacturers or card personalisers. Whenever a card key pair is generated, the party generating the key shall send the public key to its MSCA, in order to obtain a corresponding card certificate signed by the MSCA. The private key shall be used only by the tachograph card.';

(ii) paragraph CSM_88 is replaced by the following:

'CSM_88 The validity period of a Card_MA certificate shall be as follows:

— For driver cards: 5 years

— For company cards: 5 years

— For control cards: 2 years

— For workshop cards: 1 year';

(iii) the following text is added in paragraph CSM_91:

'— Additionally, for control cards, company cards and workshop cards only, and only if such cards are issued during the first three months of the validity period of a new EUR certificate: the EUR certificate that is two generations older, if existing.

Note to last bullet: For example, in the first three months of the ERCA(3) certificate (see Figure 1), the mentioned cards shall contain the ERCA(1) certificate. This is needed to ensure that these cards can be used to perform data downloads from ERCA(1) VUs whose normal 15-year life period plus the 3-months data downloading period expires during these months; see the last bullet of requirement 13) in Annex IC.';

(e) point 9.1.6 is amended as follows:

(i) paragraph CSM_93 is replaced by the following:

'CSM_93 One unique ECC key pair shall be generated for each external GNSS facility, designated as EGF_MA. This task is handled by external GNSS facility manufacturers. Whenever an EGF_MA key pair is generated, the party generating th e key shall send the public key to its MSCA in order to obtain a corresponding EGF_MA certificate signed by the MSCA. The private key shall be used only by the external GNSS facility.';

(ii) paragraph CSM_95 is replaced by the following:

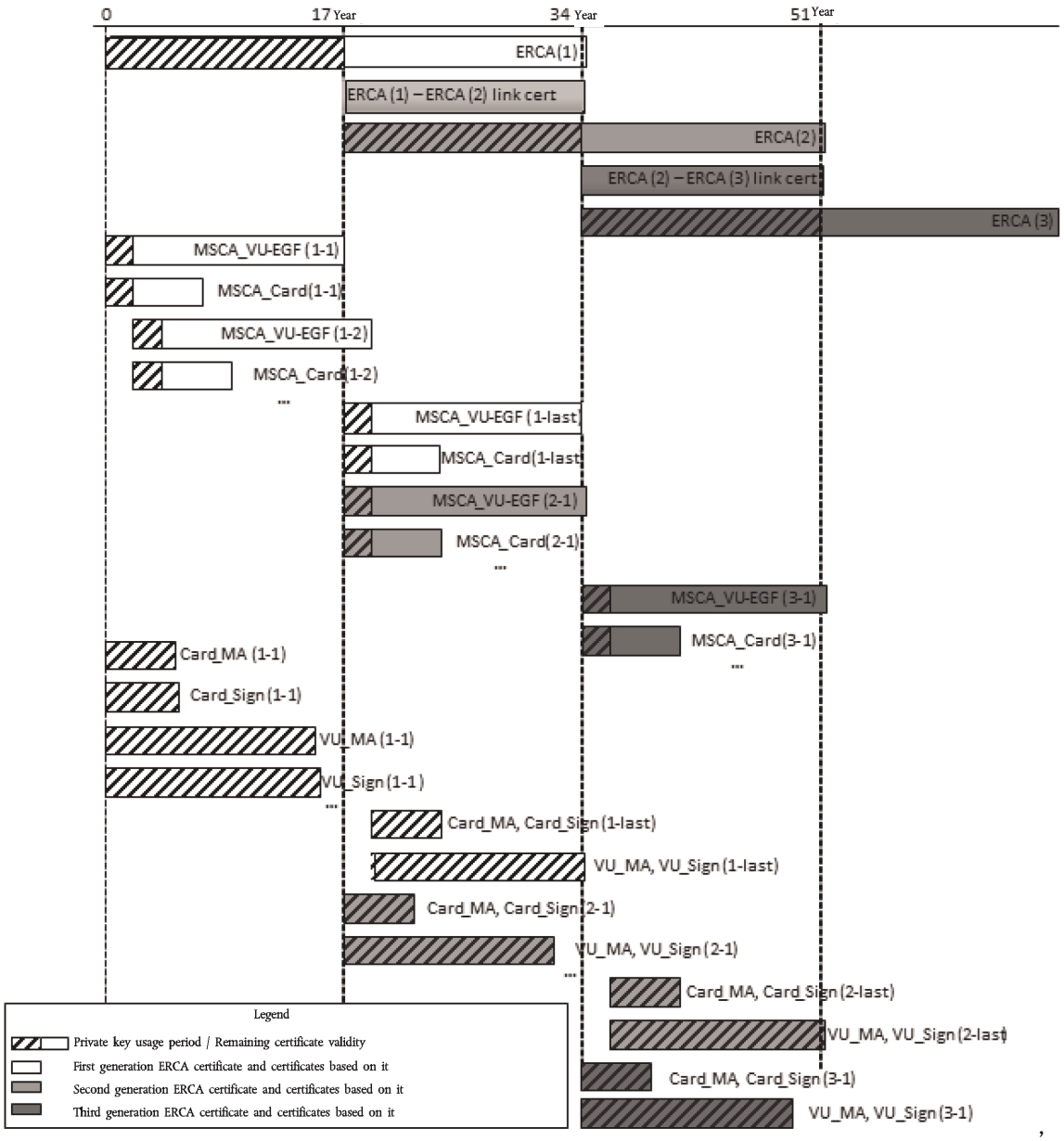
'CSM_95 An external GNSS facility shall use its EGF_MA key pair, consisting of private key EGF_MA.SK and public key EGF_MA.PK, exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in section 11.4 of this Appendix.';

(f) point 9.1.7 is amended as follows:

(i) Figure 1 is replaced by the following:

'Figure 1

Issuance and usage of different generations of ERCA root certificates, ERCA link certificates, MSCA certificates and equipment certificates



,

(ii) paragraph 6 in the Notes to Figure 1 is replaced by the following:

'6. To save space, the difference in validity period between the Card_MA and Card_Sign certificates is shown only for the first generation.';

(g) point 9.2.1.1 is amended as follows:

(i) in paragraph CSM_106, the first dash is replaced by the following:

'— For 128-bit motion sensor master keys: CV = "B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83" ';

(ii) in paragraph CSM_107, the first sub-paragraph is replaced by the following:

'Each Motion sensor manufacturer shall generate a random and unique pairing key K_P for every motion sensor, and shall send each pairing key to its Member State Certificate Authority. The MSCA shall encrypt each pairing key separately with the motion sensor master key K_M and shall return the encrypted key to the motion sensor manufacturer. For each encrypted key, the MSCA shall notify the motion sensor manufacturer of the version number of the associated K_M.';

(iii) paragraph CSM_108 is replaced by the following:

'CSM_108 Each motion sensor manufacturer shall generate a unique serial number for every motion sensor, and shall send all serial numbers to its Member State Certificate Authority. The MSCA shall encrypt each serial number separately with the identification key K_{ID} and shall return the encrypted serial number to the motion sensor manufacturer. For each encrypted serial number, the MSCA shall notify the motion sensor manufacturer of the version number of the associated K_{ID}.';

(h) point 9.2.2.1 is amended as follows:

(i) paragraph CSM_123 is replaced by the following:

'CSM_123 For every vehicle unit, the vehicle unit manufacturer shall create a unique VU serial number and shall send this number to its Member State Certificate Authority in a request to obtain a set of two VU-specific DSRC keys. The VU serial number shall have data type `VuSerialNumber`.

Note:

— This VU serial number shall be identical to the vuSerialNumber element of VuIdentification, see Appendix 1 and to the Certificate Holder Reference in the VU's certificates.

— The VU serial number may not be known at the moment a vehicle unit manufacturer requests the VU-specific DSRC keys. In this case, the VU manufacturer shall send instead the unique certificate request ID it used when requesting the VU's certificates; see CSM_153. This certificate request ID shall therefore be equal to the Certificate Holder Reference in the VU's certificates.';

(ii) in paragraph CSM_124, the info requirement in step 2 is replaced by the following:

'info = VU serial number or certificate request ID, as specified in CSM_123';

(iii) paragraph CSM_128 is replaced by the following:

'CSM_128 The MSCA shall keep records of all VU-specific DSRC keys it generated, their version number and the VU serial number or certificate request ID used in deriving them.';

(i) in point 9.3.1, the first sub-paragraph in paragraph CSM_135 is replaced by the following:

'The Distinguished Encoding Rules (DER) according to [ISO 8825-1] shall be used to encode the data objects within certificates. Table 4 shows the full certificate encoding, including all tag and length bytes.';

(j) in point 9.3.2.3, paragraph CSM_141 is replaced by the following:

'CSM_141 The Certificate Holder Authorisation shall be used to identify the type of certificate. It consists of the six most significant bytes of the Tachograph Application ID, concatenated with the equipment type, which indicates the type of equipment for which the certificate is intended. In the case of a VU certificate, a driver card certificate or a workshop card certificate, the equipment type is also used to differentiate between a certificate for Mutual Authentication and a certificate for creating digital signatures (see section 9.1 and Appendix 1, data type EquipmentType).';

(k) in point 9.3.2.5, the following sub-paragraph is added in paragraph CSM_146:

'*Note:* For a card certificate, the value of the CHR shall be equal to the value of the cardExtendedSerialNumber in EF_ICC; see Appendix 2. For an EGF certificate, the value of the CHR shall be equal to the value of the sensorGNSSSerialNumber in EF_ICC; see Appendix 14. For a VU certificate, the value of the CHR shall be equal to the vuSerialNumber element of VuIdentification, see Appendix 1, unless the manufacturer does not know the manufacturer-specific serial number at the time the certificate is requested.';

(l) in point 9.3.2.6, paragraph CSM_148 is replaced by the following:

'CSM_148 The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate.';

(m) point 9.3.3 is amended as follows:

(i) in paragraph CSM_151, the first sub-paragraph is replaced by the following:

'When requesting a certificate, an MSCA shall send the following data to the ERCA:';

(ii) paragraph CSM_153 is replaced by the following:

'CSM_153 An equipment manufacturer shall send the following data in a certificate request to an MSCA, allowing the MSCA to create the Certificate Holder Reference of the new equipment certificate:

— If known (see CSM_154), a serial number for the equipment, unique for the manufacturer, the equipment's type and the month of manufacturing. Otherwise, a unique certificate request identifier.

— The month and the year of equipment manufacturing or of the certificate request.

The manufacturer shall ensure that this data is correct and that the certificate returned by the MSCA is inserted in the intended equipment.';

(n) point 10.2.1 is amended as follows:

(i) in paragraph CSM_157, the text before the Notes to Figure 4 is replaced by the following:

'Vehicle units shall use the protocol depicted in Figure 4 for verifying a tachograph card's certificate chain. For every certificate it reads from the card, the VU shall verify that the Certificate Holder Authorisation (CHA) field is correct:

— The CHA field of the Card certificate shall indicate a card certificate for mutual authentication (see Appendix 1, data type EquipmentType).

— The CHA of the Card.CA certificate shall indicate an MSCA.

— The CHA of the Card.Link certificate shall indicate the ERCA.';

(ii) in paragraph CSM_159, the following sentence is added:

'Whereas storing of all other types of certificate is optional, it is mandatory for a VU to store a new link certificate presented by a card.';

(o) point 10.2.2 is amended as follows:

(i) in paragraph CSM_161, the text before the Figure 5 is replaced by the following:

'Tachograph cards shall use the protocol depicted in Figure 5 for verifying a VU's certificate chain. For every certificate presented by the VU, the card shall verify that the Certificate Holder Authorisation (CHA) field is correct:

— The CHA of the VU.Link certificate shall indicate the ERCA.

— The CHA of the VU.CA certificate shall indicate an MSCA.

— The CHA field of the VU certificate shall indicate a VU certificate for mutual authentication (see Appendix 1, data type EquipmentType).';

(ii) paragraph CSM_165 is replaced by the following:

'CSM_165 If the MSE: Set AT command is successful, the card shall set the indicated VU.PK for subsequent use during Vehicle Authentication, and shall temporarily store Comp(VU.PKeph). In case two or more successful MSE: Set AT commands are sent before session key agreement is performed, the card shall store only the last Comp(VU.PKeph) received. The card shall reset Comp(VU.PKeph) after a successful GENERAL AUTHENTICATE command.';

(p) point 10.3 is amended as follows:

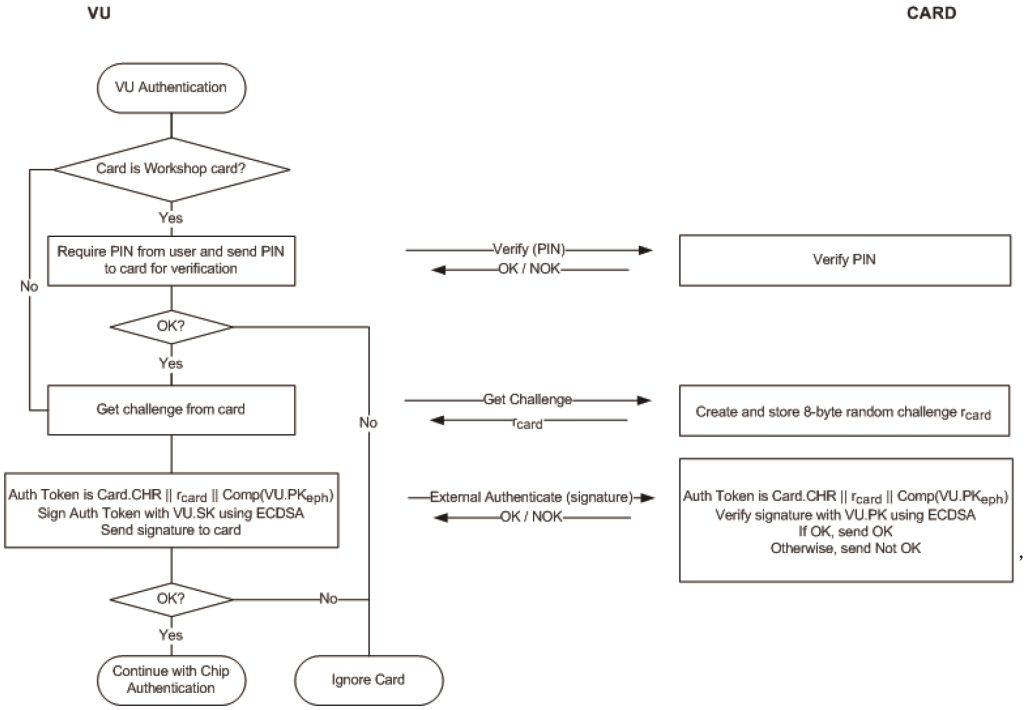
(i) the first sub-paragraph in paragraph CSM_170 is replaced by the following:

'Next to the card challenge, the VU shall include in the signature the certificate holder reference taken from the card certificate.';

(ii) in paragraph CSM_171, Figure 6 is replaced by the following:

'Figure 6

VU Authentication protocol



(iii) paragraph CSM_174 is replaced by the following:

'CSM_174 Upon receiving the VU's signature in an EXTERNAL AUTHENTICATE command, the card shall

— Calculate the authentication token by concatenating Card.CHR, the card challenge rcard and the identifier of the VU ephemeral public key Comp(VU.PKeph),

— Verify the VU's signature using the ECDSA algorithm, using the hashing algorithm linked to the key size of the VU's VU_MA key pair as specified in CSM_50, in combination with VU.PK and the calculated authentication token.';

(q) in point 10.4, paragraph CSM_176 is amended as follows:

(i) sub-paragraph 2 is replaced by the following:

'2. The VU sends the public point $VU.PK_{eph}$ of its ephemeral key pair to the card. The public point shall be converted to an octet string as specified in [TR-03111]. The uncompressed encoding format shall be used. As explained in CSM_164, the VU generated this ephemeral key pair prior to the verification of the VU certificate chain. The VU sent the identifier of the ephemeral public key Comp($VU.PK_{eph}$) to the card, and the card stored it.';

(ii) sub-paragraph 6 is replaced by the following:

'6. Using K_{MAC}, the card computes an authentication token over the VU ephemeral public point: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). The public point shall be in the format used by the VU (see bullet 2 above). The card sends N_{PICC} and T_{PICC} to the vehicle unit.';

(r) in point 10.5.2, paragraph CSM_191 is replaced by the following:

'CSM_191 Any data object to be encrypted shall be padded according to [ISO 7816-4] using padding-content indicator '01'. For the calculation of the MAC, data objects in the APDU shall be padded according to [ISO 7816-4].

Note: Padding for Secure Messaging is always performed by the secure messaging layer, not by the CMAC or CBC algorithms.

Summary and Examples

A command APDU with applied Secure Messaging will have the following structure, depending on the case of the respective unsecured command (DO is data object):

Case 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Case 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Case 3 (even INS byte): CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le

Case 3 (odd INS byte): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le

Case 4 (even INS byte): CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le

Case 4 (odd INS byte): CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

where Le = '00' or '00 00' depending on whether short length fields or extended length fields are used; see [ISO 7816-4].

A response APDU with applied Secure Messaging will have the following structure, depending on the case of the respective unsecured response:

Case 1 or 3: DO '99' || DO '8E' || SW1SW2

Case 2 or 4 (even INS byte) without encryption: DO '81' || DO '99' || DO '8E' || SW1SW2

Case 2 or 4 (even INS byte) with encryption: DO '87' || DO '99' || DO '8E' || SW1SW2

Case 2 or 4 (odd INS byte) without encryption: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Note: Case 2 or 4 (odd INS byte) with encryption is never used in the communication between a VU and a card.

Below are three example APDU transformations for commands with even INS code. Figure 8 shows an authenticated Case 4 command APDU, Figure 9 shows an authenticated Case 1/Case 3 response APDU, and Figure 10 shows an encrypted and authenticated Case 2/Case 4 response APDU.

Figure 8

Transformation of an authenticated Case 4 Command APDU

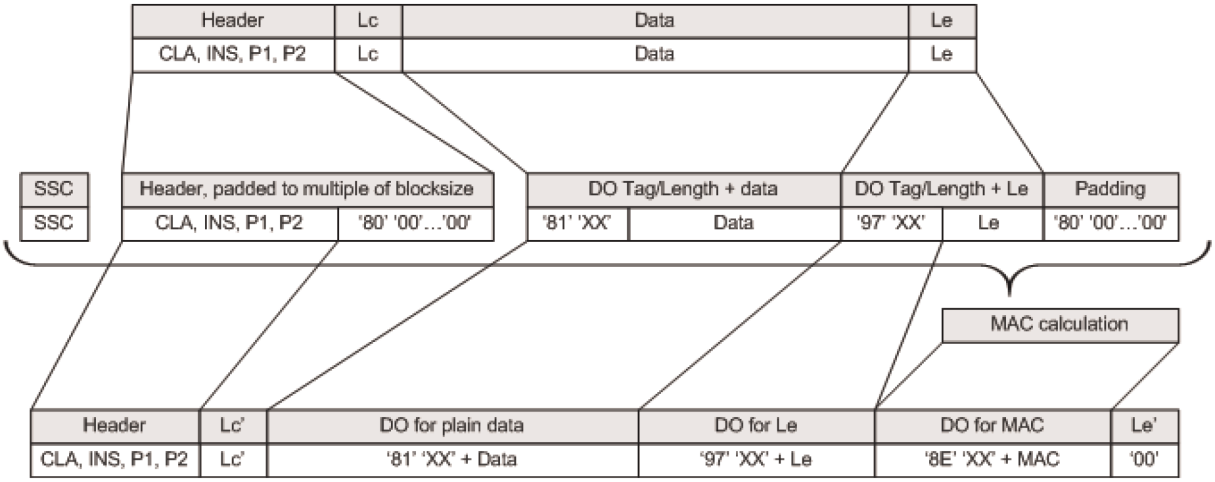


Figure 9

Transformation of an authenticated Case 1 / Case 3 Response APDU

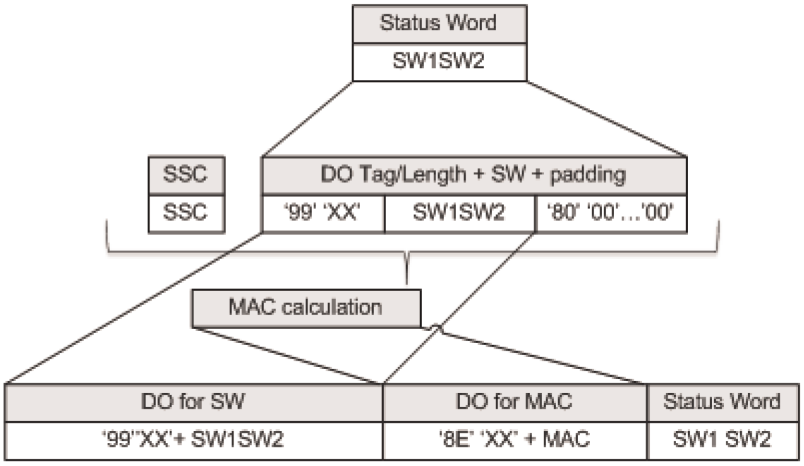
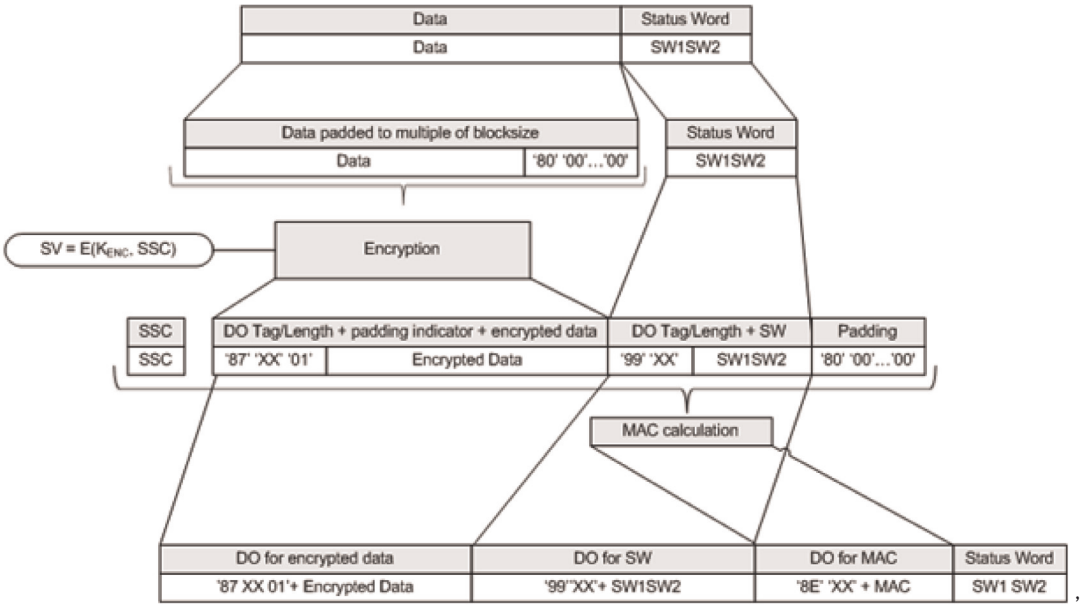


Figure 10

Transformation of an encrypted and authenticated Case 2/Case 4 Response APDU



(s) in point 10.5.3, paragraph CSM_193 is replaced by the following:

'CSM_193 A tachograph card shall abort an ongoing Secure Messaging session if and only if one of the following conditions occur:

— it receives a plain command APDU,

— it detects a Secure Messaging error in a command APDU:

— An expected Secure Messaging data object is missing, the order of data objects is incorrect, or an unknown data object is included.

— A Secure Messaging data object is incorrect, e.g. the MAC value is incorrect or the TLV structure is incorrect.

— it is depowered or reset,

— the VU starts the VU Authentication process,

— the limit for the number of commands and associated responses within the current session is reached. For a given card, this limit shall be defined by its manufacturer, taking into account the security requirements of the hardware used, with a maximum value of 240 SM commands and associated responses per session';

(t) point 11.3.2 is amended as follows:

(i) the first sub-paragraph of paragraph CSM_208 is replaced by the following:

'During the coupling to a VU, an external GNSS facility shall use the protocol depicted in Figure 5 (section 10.2.2) for verifying the VU's certificate chain';

(ii) paragraph CSM_210 is replaced by the following:

'CSM_210 Once it has verified the VU_MA certificate, the external GNSS facility shall store this certificate for use during normal operation; see section 11.3.3.';

(u) in point 11.3.3, the first sub-paragraph in paragraph CSM_211, is replaced by the following:

'During normal operation, a vehicle unit and an EGF shall use the protocol depicted in Figure 11 for verifying the temporal validity of the stored EGF_MA certificate and for setting the VU_MA public key for subsequent VU Authentication. No further mutual verification of the certificate chains shall take place during normal operation.';

(v) in point 12.3, Table 6 is replaced by the following:

'Table 6

Number of plaintext and encrypted data bytes per instruction defined in [ISO 16844-3]

Instruction	Request / reply	Description of data	# of plaintext data bytes according to [ISO 16844-3]	# of plaintext data bytes using AES keys	# of encrypted data bytes when using AES keys of bitlength		
					128	192	256
10	request	Authentication data + file number	8	8	16	16	16
11	reply	Authentication data + file contents	16 or 32, depend on file	16 or32, depend on file	32 / 48	32 / 48	32 / 48
41	request	MoS serial number	8	8	16	16	16
41	reply	Pairing key	16	16 / 24 / 32	16	32	32
42	request	Session key	16	16 / 24 / 32	16	32	32
43	request	Pairing information	24	24	32	32	32
50	reply	Pairing information	24	24	32	32	32
70	request	Authentication data	8	8	16	16	16
80	reply	MoS counter value + auth. data	8	8	16	16	16'

(w) in point 13.1, the requirement on the VU serial number in subparagraph CSM_224 is replaced by the following:

'**VU serial number** the VU's serial number or certificate request ID (data type VuSerialNumber or CertificateRequestID) – see CSM_123';

(x) in point 13.3, the second indent in paragraph CSM_228 is replaced by the following:

'2. The control card shall use the indicated DSRC master key in combination with the VU serial number or the certificate request ID in the DSRC security data to derive the VU-specific DSRC keys K_VU_{DSRC}_ENC and K_VU_{DSRC}_MAC, as specified in CSM_124.';

(y) point 14.3 is amended as follows:

(i) in paragraph CSM_234, the text before the Notes to figure 13 is replaced by the following:

'An IDE may perform verification of a signature over downloaded data itself or it may use a control card for this purpose. In case it uses a control card, signature verification shall take place as shown in Figure 13. For verifying the temporal validity of a certificate presented by the IDE, the control card shall use its internal current time, as specified in CSM_167. The control card shall update its current time if the Effective Date of an authentic 'valid source of time' certificate is more recent than the card's current time. The card shall accept only the following certificates as a valid source of time:

— Second-generation ERCA link certificates

— Second-generation MSCA certificates

— Second-generation VU_Sign or Card_Sign certificates issued by the same country as the control card's own card certificate.

In case it performs signature verification itself, the IDE shall verify the authenticity and validity of all certificates in the certificate chain in the data file, and it shall verify the signature over the data following the signature scheme defined in [DSS]. In both cases, for every certificate read from the data file, it is necessary to verify that the Certificate Holder Authorisation (CHA) field is correct:

— The CHA field of the EQT certificate shall indicate a VU or Card (as applicable) certificate for signing (see Appendix 1, data type EquipmentType).

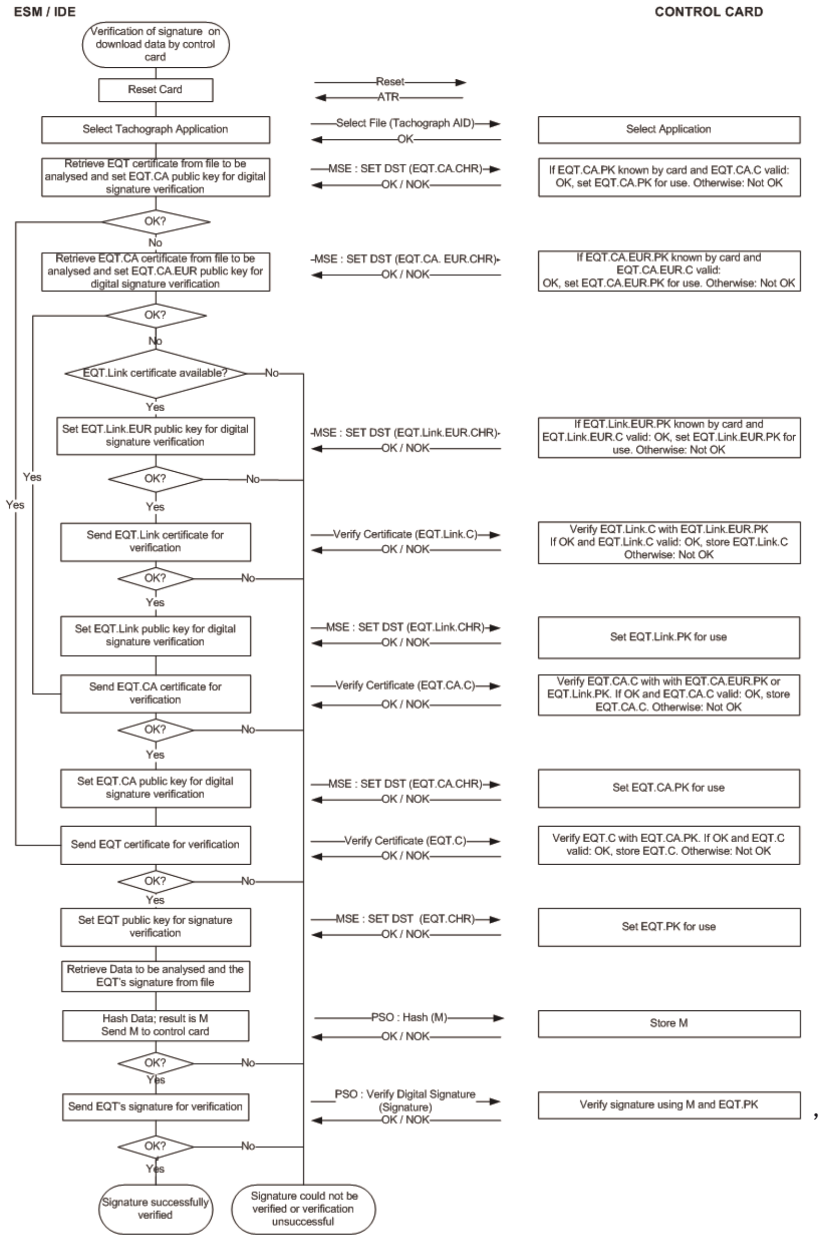
— The CHA of the EQT.CA certificate shall indicate an MSCA.

— The CHA of the EQT.Link certificate shall indicate the ERCA.';

(ii) Figure 13 is replaced by the following:

'Figure 13

Protocol for verification of the signature over a downloaded data file



,

(37) Appendix 12 is amended as follows:

(a) point 3 is amended as follows:

(i) in paragraph GNS_4, the second sub-paragraph after Figure 2 is replaced by the following:

'The resolution of the position is based on the format of the RMC sentence described above. The first part of the fields 3) and 5) are used to represent the degrees. The rest are used to represent the minutes with three decimals. So the resolution is 1/1000 of minute or 1/60000 of degree (because one minute is 1/60 of a degree).';

(ii) Paragraph GNS_5 is replaced by the following:

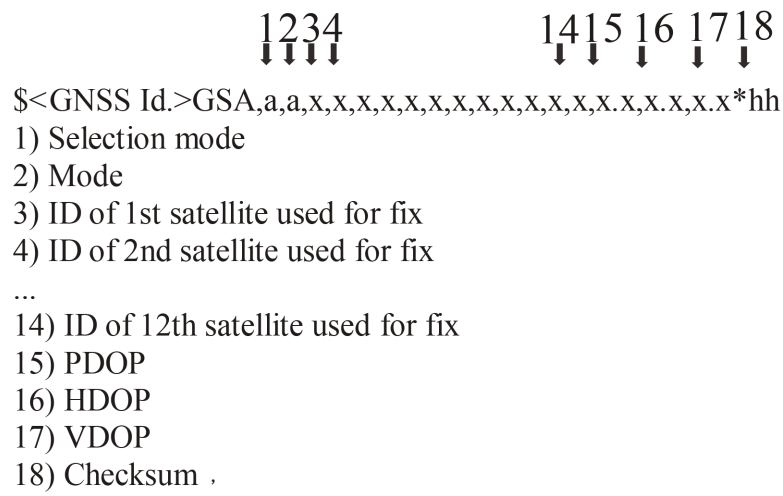
'GNS_5 The Vehicle Unit shall store in the VU database the position information for latitude and longitude with a resolution of 1/10 of minute or 1/600 of a degree as described in Appendix 1 for type GeoCoordinates.

The GPS DOP and active satellites (GSA) command can be used by the VU to determine and record the signal availability and accuracy. In particular the HDOP is used to provide an indication on the level of accuracy of the recorded location data (see 4.2.2). The VU will store the value of the Horizontal Dilution of Precision (HDOP) calculated as the minimum of the HDOP values collected on the available GNSS systems.

The GNSS Id. indicates the corresponding NMEA Id. for every GNSS constellation and Satellite-Based Augmentation System (SBAS).

Figure 3

Structure of the GSA sentence



(iii) paragraph GNS_6 is replaced by the following:

'GNS_6 The *GSA* sentence shall be stored with record number '02' to '06";

(b) point 4.2.1 is amended as follows:

(i) paragraph GNS_16 is replaced by the following:

'GNS_16 In the communication protocol, extended length fields shall not be supported.';

(ii) paragraph GNS_18 is replaced by the following:

'GNS_18 Regarding the functions 1) the collection and distribution of GNSS data and 2) the collection of the configuration data of the external GNSS facility and 3) management protocol, the GNSS Secure Transceiver shall simulate a smart card with a file system architecture composed by a Master File (MF), a Dedicated File (DF) with Application Identifier specified in Appendix 1 chapter 6.2 ('FF 44 54 45 47 4D') and with 3 EFs containing certificates and one single Elementary File (EF.EGF) with file identifier equal to '2F2F' as described in Table 1.';

(iii) paragraph GNS_20 is replaced by the following:

'GNS_20 The GNSS Secure Transceiver shall use a memory to store the data and be able to perform at least 20 millions write/read cycles. Apart from this aspect, the internal design and implementation of the GNSS Secure Transceiver is left to the manufacturers.

The mapping of record numbers and data is provided in Table 1. Note that there are five GSA sentences for the GNSS constellations and Satellite-Based Augmentation System (SBAS).';

(c) in point 4.2.2, sub-paragraph 5 in paragraph GNS_23 is replaced by the following:

'5. The VU processor checks the received data extracting the information (e.g., latitude, longitude, time) from the RMC NMEA sentence. The RMC NMEA sentence includes the information if the position is valid. If the position is not valid, the location data is not available yet and it cannot be used to record the position of the vehicle. If the position is valid, the VU processor also extracts the values of HDOP from GSA NMEA sentences and calculate the minimum value on the available satellite systems (i.e., when the fix is available).';

(d) In point 4.4.1, paragraph GNS_28 is replaced by the following:

'GNS_28 If the VU does not manage to communicate to the coupled external GNSS facility for more than 20 continuous minutes, the VU shall generate and record in the VU an event of type EventFaultType with the value of enum '0E'H Communication error with the external GNSS facility and with the timestamp set to the current time. The event will be generated only if the following two conditions are satisfied: (a) the Smart Tachograph is not in calibration mode and (b) the vehicle is moving. In this context, a communication error is triggered when the VU Secure Transceiver does not receive a response message after a request message as described in 4.2.';

(e) in point 4.4.2, paragraph GNS_29 is replaced by the following:

'GNS_29 If the external GNSS facility has been breached, the GNSS Secure Transceiver shall erase all its memory including cryptographic material. As described in GNS_25 and GNS_26, the VU shall detect tampering if the Response has status '6690'. The VU shall then generate an event of type EventFaultType enum '19'H Tamper detection of GNSS. Alternately, the external GNSS facility may not respond to any external request anymore.';

(f) in point 4.4.3, paragraph GNS_30 is replaced by the following:

'GNS_30 If the GNSS Secure Transceiver does not receive data from the GNSS receiver for more than 3 continuous hours, the GNSS Secure Transceiver shall generate a response message to the READ RECORD command with RECORD number equal to '01' with a Data Field of 12 bytes all set to 0xFF. Upon reception of the Response message with this value of the data field, the VU shall generate and record an event of type EventFaultType enum '0D'H Absence of position information from GNSS receiver event with a timestamp equal to the current value of time only if the following two conditions are satisfied: a) the Smart Tachograph is not in calibration mode and b) the vehicle is moving.';

(g) in point 4.4.4, the text in paragraph GNS_31 until Figure 4, is replaced by the following:

'If the VU detects that the EGF certificate used for mutual authentication is not valid any longer, the VU shall generate and record a recording equipment event of type EventFaultType enum '*1B'H External GNSS facility certificate expired* with a timestamp equal to the current value of time. The VU shall still use the received GNSS position data.';

(h) in point 5.2.1, paragraph GNS_34 is replaced by the following:

'GNS_34 If the VU does not receive data from the GNSS receiver for more than 3 continous hours, the VU shall generate and record an event of type EventFaultType enum '0D'H Absence of position information from GNSS receiver event with a timestamp equal to the current value of time only if the following two conditions are satisfied: (a) the Smart Tachograph is not in calibration mode and (b) the vehicle is moving.';

(i) point 6 is replaced by the following:

'6. GNSS TIME CONFLICT

If the VU detects a discrepancy of more than 1 minute between the time of the vehicle unit's time measurement function and the time originating from the GNSS receiver, the VU will record an event of type EventFaultType enum '*0B'H Time conflict (GNSS versus VU internal clock)*. After a time conflict event has been triggered, the VU will not check the time discrepancy for the next 12 hours. This event shall not be triggered in cases no valid GNSS signal was detectable by the GNSS receiver within the last 30 days.';

(38) Appendix 13 is amended as follows:

(a) in point 2, the fourth paragraph is replaced by the following:

'For clarification, this Appendix does <u>not</u> specify:

— The collection of *the Data* operation and management within the VU (which shall be specified elsewhere within *the Regulation* or otherwise shall be a function of product design).

— The form of presentation of collected data to application hosted on the external device.

— Data security provisions above what provides Bluetooth® (such as encryption) concerning the content of *the Data* (which shall be specified elsewhere within *the Regulation* [Appendix 11 Common Security Mechanisms]).

— The Bluetooth® protocols used by the ITS interface';

(b) in point 4.2, the third paragraph is replaced by the following:

'When an external device comes within range of the VU for the first time, the Bluetooth® pairing process can be initiated (see also annex 2). The devices share their addresses, names, and profiles and common secret key, which allows them to bond whenever they are together in the future. Once this step is completed, the external device is trusted and is in state to initiate requests to download data from the tachograph. It is not foreseen to add encryption mechanisms beyond what Bluetooth® provides. However, if additional security mechanisms are needed, this will be done in accordance with Appendix 11 Common Security Mechanisms.';

(c) point 4.3 is amended as follows:

(i) the first paragraph is replaced by the following:

'For security reasons, the VU will require a PIN code authorization system separated from the Bluetooth pairing. Each VU shall be able to generate PIN codes for authentication purposes composed of at least 4 digits. Every time an external device pairs with the VU, it must provide the correct PIN code before receiving any data.';

(ii) the third paragraph after Table 1 is replaced by the following:

'While the manufacturer may offer an option to change the PIN code directly through the VU, the PUC code shall not be alterable. Modifying the PIN code, if possible, shall require to enter the current PIN code directly in the VU.';

(d) in point 4.4, the second paragraph after the heading "Data Field" is replaced by the following:

'If the data to be handled is larger than the available space in one message, it will be split in several submessages. Each submessage shall have the same Header and SID, but will contain a 2-bytes counter, Counter Current (CC) and Counter Max (CM), to indicate the submessage number. To enable error checking and abort the receiving device acknowledges every submessage. The receiving device can accept the submessage, ask for it to be re-transmitted, request the sending device to start again or abort the transmission.';

(e) Annex 1 is amended as follows:

(i) the heading is replaced by the following:

'(1) LIST OF AVAILABLE DATA THROUGH THE ITS INTERFACE';

(ii) the following item is inserted in the table in point (3), after the item 'Absence of position information from GNSS receiver':

'Communication error with the external GNSS facility	— 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, — card(s) type, number, issuing Member State and generation of any card inserted at beginning and/or end of the event, — number of similar events that day.'

(iii) in point (5), the following dash is added:

'— ITS interface fault (if applicable)';

(f) the ASN.1 specifications in Annex 3 are amended as follows:

(i) the following lines 206a to 206e are inserted after line 206:

```
'206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }';
```

(ii) lines 262 to 264 are replaced by the following:

```
'262    driveRecognize BIT STRING ('00'B UNION '01'B),
263    driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264    driverCardDriver2 BIT STRING ('00'B UNION '01'B), ';
```

(iii) line 275 is replaced by the following:

```
‘275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),‘;
```

(iv) lines 288 to 310 are replaced by the following:

```
‘288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310’
```

(v) lines 362 and 363 are replaced by the following:

```
‘362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),’;
```

(vi) the following lines 410a and 410b are inserted after line 410:

```
‘410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,’;
```

(vii) the following lines 539a to 539j are inserted after line 539:

```
‘539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j’;
```

(39) Appendix 14 is amended as follows:

(a) item 5.5 in the Table of Contents is replaced by the following:

'5.5 Support for Directive (EU) 2015/719 ..... 490';

(b) in point 2, the third paragraph is replaced by the following:

'In this scenario, the time available for communication is limited, because *the Communication* is targeted and of a short- range design. Further, the same communication means for remote tachograph monitoring (RTM) may also be used by the competent control authorities for other applications (such as the maximal weights and dimensions for heavy goods vehicles defined in Directive (EU) 2015/719) and such operations may be separate or sequential at the discretion of the competent control authorities.';

(c) point 5.1 is amended as follows:

(i) in paragraph DSC_19, the twelfth dash is replaced by the following:

'— The DSRC-VU antenna shall be positioned at a location where it optimizes the DSRC communication between the vehicle and the roadside reader antenna, when the reader is installed 15 meters distance in front of the vehicle and 2 meters height, targeting the horizontal and vertical centre of the windscreen. For light vehicles an installation corresponding to the upper part of the windscreen is suitable. For all the other vehicles the DSRC antenna shall be installed either near the lower or near the upper part of the windscreen.';

(ii) in paragraph DSC_22, the first sub-paragraph is replaced by the following:

'The form factor of the antenna is not defined and shall be a commercial decision, so long as the fitted DSRC-VU meets the conformance requirements defined in section 5 below. The antenna shall be positioned as determined in DSC_19 and efficiently support the use cases described in in 4.1.2 and 4.1.3.';

(d) in point 5.4.3, sequence 7 is replaced by the following:

'7 REDCR > DSRC-VU Sends GET.request for data of other Attribute (if appropriate)'

(e) in point 5.4.4, the ASN.1 module definition in paragraph DCS_40 is amended as follows:

(i) the first line of the sequence for `TachographPayload` is replaced by the following:

```
'tp15638VehicleRegistrationPlate LPN - Vehicle Registration Plate as per EN 15509[1]'
```

(ii) the following footnote 1 is added:

'1. if a LPN contains an AlphabetIndicator LatinAlphabetNo2 or latinCyrillicAlphabet, the special characters are remapped at the road interrogator unit applying special rules according to Annex E of ISO/DIS 14 906,2';

(iii) the superscript 2 is removed from the line where the Timestamp of current record is defined;

(iv) the ASN.1 module definition for `RtmTransferAck` is replaced by the following:

```
'RtmTransferAck ::= INTEGER {
                    Ok (1),
                    NoK (2)
                    } (1..255)';
```

(f) in point 5.4.5, item RTM12 in table 14.3 is replaced by the following:

‘**RTM12** **Sensor Fault**	The VU shall generate an integer value for data element RTM12. The VU shall assign to the variable sensorFault a value of: — 1 if an event of type ‘35H’ Sensor fault has been recorded in the last 10 days, — 2 if an event of type GNSS receiver fault (either internal or external with enum values ‘36’H or ‘37’ H) has been recorded in the last 10 days. — 3 if an event of type ‘0E’H Communication error with the external GNSS facility event has been recorded in the last 10 days. — 4 If both Sensor Fault and GNSS receiver faults have been recorded in the last 10 days — 5 If both Sensor Fault and Communication error with the external GNSS facility event have been recorded in the last 10 days — 6 If both GNSS receiver fault and Communication error with the external GNSS facility event have been recorded in the last 10 days — 7 If all three sensor faults, have been recorded in the last 10 days ELSE it shall assign a value of 0 if no events have been recorded in the last 10 days	– sensor fault one octet as per data dictionary	`sensorFault INTEGER (0..255),;` ’

(g) in point 5.4.6, DSC_43 is replaced by the following:

‘DSC_43 For all DSRC exchanges, data shall be encoded using PER (Packed Encoding Rules) UNALIGNED, apart from `TachographPayload` and `OwsPayload`;, which shall be encoded using OER (Octet Encoding Rules) defined in ISO/IEC 8825-7, Rec. ITU-T X.696.’;

(h) in point 5.4.7, in the Fourth column of Table 14.9, the text in the cell describing `Rtm-ContextMark`; is replaced by the following:

‘Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1).

First octet is 06H, which is the Object Identifier. Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier.’;

(i) points 5.5 and 5.5.1 are replaced by the following:

‘5.5. **Support for Directive (EU) 2015/719**

5.5.1. *Overview*

DSC_59 To support the Directive (EU) 2015/719 on the maximal weights and dimensions for heavy goods vehicles, the transaction protocol to download OWS data across the 5,8 GHz DSRC interface link will be the same as that used for the RTM data (see 5.4.1), the only difference being that the Object Identifier that relates to the TARV standard will be addressing the ISO 15638 standard (TARV) Part 20 related to WOB/OWS.’;

(j) in point 5.6.1, sub-paragraph (a) in paragraph DSC_68 is replaced by the following:

'(a) In order that different suppliers may be contracted to supply the VU and the DSRC-VU, and indeed different batches of DSRC-VU, the connection between the VU and the DSRC-VU not internal to the VU shall be an open standard connection. The VU shall connect with the DSRC-VU either';

(k) in point 5.7.1, paragraph DSC_77 is replaced by the following:

'DSC_77 *The Data* shall be provided, already secured , by the *VUSM* function to the *DSRC-VU*. The *VUSM* shall verify that data recorded in the *DSRC-VU* has been recorded correctly. The recording and reporting of any errors in the transfer of data from the *VU* to the memory of the *DSRC-VU* shall be recorded with type EventFaultType and enum value set to '0C'H Communication error with the remote communication facility event together with the timestamp.';

(40) Appendix 15 is amended as follows:

(a) the first paragraph of point 2.2 is replaced by the following:

'It is understood that first generation tachograph cards are interoperable with first generation vehicle units in compliance with Annex IB to Regulation (EEC) No 3821/85, while second generation tachograph cards are interoperable with second generation vehicle units in compliance with Annex IC to this Regulation. In addition, the requirements below shall apply.';

(b) in point 2.4.1, paragraph MIG_11 is amended as follows:

(i) the first indent is replaced by the following:

'— non signed EFs IC and ICC (optional),';

(ii) the third indent is replaced by the following:

'— the other application data EFs (within DF Tachograph) requested by the first generation card download protocol. This information shall be secured with a digital signature, according to the first generation security mechanisms.

Such download shall not include application data EFs only present in second generation driver (and workshop) cards (application data EFs within DF Tachograph_G2).';

(c) In point 2.4.3, paragraphs MIG_014 and MIG_015 are replaced by the following:

'MIG_014 Outside the frame of drivers' control by non EU control authorities, data shall be downloaded from second generation vehicle units using the second generation security mechanisms, and the data download protocol specified in Appendix 7 of this Annex.

MIG_015 To allow drivers' control by non EU control authorities, it may optionally also be possible to download data from second generation vehicle units using the first generation security mechanisms. Downloaded data shall then have the same format as data downloaded from a first generation vehicle unit. This capability may be selected through commands in the menu.';

ANNEX II

Annex II to Regulation (EU) 2016/799 is amended as follows:

(1) in Chapter I, paragraph b) in point 1 is replaced by the following:

'(b) an approval number corresponding to the number of the approval certificate drawn up for the prototype of the recording equipment or the record sheet or the tachograph card, placed at any point within the immediate proximity of that rectangle.';

(2) in Chapter III, point 5 is replaced by the following:

'5. Submitted for approval on .....';

(3) in Chapter IV, point 5 is replaced by the following:

'5. Submitted for approval on .....'.

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN

II

(Actes non législatifs)

RÈGLEMENTS

RÈGLEMENT D'EXÉCUTION (UE) 2018/502 DE LA COMMISSION

du 28 février 2018

modifiant le règlement d'exécution (UE) 2016/799 fixant les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) n° 165/2014 du Parlement européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers ([1]), et notamment son article 11 et son article 12, paragraphe 7,

considérant ce qui suit:

(1) Le règlement (UE) n° 165/2014 a instauré le tachygraphe intelligent, tachygraphe numérique de deuxième génération connecté au système mondial de navigation par satellite (ci-après «GNSS») et comprenant un dispositif de communication à distance à des fins de détection précoce et une interface facultative avec les systèmes de transport intelligents.

(2) Les exigences techniques applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants sont définies dans le règlement d'exécution (UE) 2016/799 de la Commission ([2]).

(3) Conformément aux articles 8, 9 et 10 du règlement (UE) n° 165/2014, les tachygraphes installés dans les véhicules immatriculés pour la première fois le 15 juin 2019 ou après cette date doivent être des tachygraphes intelligents. Il convient, dès lors, de modifier le règlement d'exécution (UE) 2016/799 afin que les dispositions techniques qu'il arrête s'appliquent à partir de cette date.

(4) Pour assurer la conformité avec l'article 8 du règlement (UE) n° 165/2014, qui prévoit que la position du véhicule doit être enregistrée toutes les trois heures de temps de conduite accumulé, le règlement d'exécution (UE) 2016/799 devrait être modifié de manière à permettre le stockage d'informations sur la position du véhicule à intervalles de trois heures, au moyen d'une métrique qui ne peut pas être réinitialisée, et à éviter toute confusion avec le «temps de conduite sans interruption», qui est une métrique remplissant une autre fonction.

(5) L'unité embarquée sur le véhicule peut se présenter sous la forme d'un seul élément ou de plusieurs composants répartis dans le véhicule. Par conséquent, le GNSS et la communication spécialisée à courte portée (DSRC) pourraient être pris en charge par des dispositifs internes ou externes à l'élément principal de l'unité embarquée. Lorsque ces deux dispositifs sont externes, il devrait être possible de les homologuer, ainsi que l'élément principal de l'unité embarquée sur le véhicule, en tant que composants afin d'adapter le processus d'homologation du tachygraphe intelligent aux besoins du marché.

(6) Il convient de modifier les règles relatives au stockage des événements «Conflit temporel» et les remises à l'heure afin d'établir une distinction entre, d'une part, les remises à l'heure automatiques déclenchées par d'éventuelles tentatives de manipulation ou un dysfonctionnement du tachygraphe et, d'autre part, les remises à l'heure provoquées par d'autres interventions, comme un entretien.

(7) Les identificateurs de données devraient pouvoir opérer une distinction entre les données téléchargées depuis un tachygraphe intelligent et les données téléchargées depuis un tachygraphe d'une génération antérieure.

([1]) JO L 60 du 28.2.2014, p. 1.

([2]) Règlement d'exécution (UE) 2016/799 de la Commission du 18 mars 2016 mettant en œuvre le règlement (UE) n° 165/2014 du Parlement européen et du Conseil en ce qui concerne les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants (JO L 139 du 26.5.2016, p. 1).

(8) La période de validité d'une carte d'entreprise doit être portée à cinq ans, au lieu de deux, pour qu'elle corresponde à celle de la carte de conducteur.

(9) La description de certaines anomalies et événements, la validation de la saisie du lieu de début et/ou de fin de la période de travail journalière, l'utilisation du consentement du conducteur pour l'interface ITS (système de transport intelligent) en ce qui concerne les données transmises par l'unité embarquée sur le véhicule par l'intermédiaire du réseau du véhicule, ainsi que d'autres aspects techniques, devraient être mieux circonscrits.

(10) Pour garantir que la certification des scellements du tachygraphe est à jour, il y a lieu de les adapter à la nouvelle norme de sécurité des scellements mécaniques apposés sur les tachygraphes.

(11) Le présent règlement s'applique à la construction, aux essais, à l'installation et à l'utilisation de systèmes comprenant également des équipements radioélectriques relevant de la directive 2014/53/UE du Parlement européen et du Conseil ([1]). Cette dernière régit de manière horizontale la mise sur le marché et la mise en service d'équipements électriques et électroniques utilisant des ondes radioélectriques à des fins de communication et/ou de radiorepérage, notamment en ce qui concerne la sécurité électrique, la compatibilité avec les autres systèmes, l'accès au spectre radioélectrique, l'accès aux services d'urgence et/ou d'autres dispositions de délégation. Pour garantir l'utilisation efficiente du spectre radioélectrique, prévenir les perturbations radioélectriques, assurer la sécurité et la compatibilité électromagnétique des équipements radioélectriques et satisfaire à toute autre exigence spécifique faisant l'objet d'une délégation, le présent règlement devrait être sans préjudice de ladite directive.

(12) Il y a lieu, dès lors, de modifier le règlement d'exécution (UE) 2016/799.

(13) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 42, paragraphe 3, du règlement (UE) n° 165/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Le règlement d'exécution (UE) 2016/799 est modifié comme suit:

1) l'article 1er est modifié comme suit:

a) les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. La construction, les essais, l'installation, l'inspection, l'utilisation et la réparation des tachygraphes intelligents et de leurs composants sont conformes aux exigences techniques énoncées à l'annexe IC du présent règlement.

3. Les tachygraphes autres que les tachygraphes intelligents continuent, en matière de construction, d'essais, d'installation, d'inspection, d'utilisation et de réparation, de satisfaire aux exigences de l'annexe I du règlement (UE) n° 165/2014 ou de l'annexe IB du règlement (CEE) n° 3821/85 du Conseil (*), selon le cas.

(*) Règlement (CEE) n° 3821/85 du Conseil du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des transports par route (JO L 370 du 31.12.1985, p. 8).»;

b) le paragraphe 5 suivant est ajouté:

«5. Le présent règlement est sans préjudice de l'application de la directive 2014/53/UE du Parlement européen et du Conseil (*).

(*) Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).»;

2) l'article 2 est modifié comme suit:

a) la définition 3 est remplacée par le texte suivant:

«3. "dossier fabricant", le dossier complet, sous forme électronique ou imprimée, contenant toutes les informations fournies par le fabricant ou son mandataire à l'autorité d'homologation aux fins de l'homologation d'un tachygraphe ou d'un composant de tachygraphe, y compris les certificats visés à l'article 12, paragraphe 3, du règlement (UE) n° 165/2014, l'exécution des essais définis à l'annexe IC du présent règlement, ainsi que les dessins, photographies et autres documents pertinents;»;

([1]) Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).

b) la définition 7 est remplacée par le texte suivant:

«7. "tachygraphe intelligent" ou "tachygraphe de deuxième génération", un tachygraphe numérique conforme aux articles 8, 9 et 10 du règlement (UE) n° 165/2014 ainsi qu'à l'annexe IC du présent règlement;»;

c) la définition 8 est remplacée par le texte suivant:

«8. "composant de tachygraphe", l'un des éléments suivants: l'unité embarquée sur le véhicule, le capteur de mouvement, la feuille d'enregistrement, le dispositif GNSS externe et le dispositif externe de détection précoce à distance;»;

d) la définition suivante est ajoutée:

«10. "unité embarquée sur le véhicule", le tachygraphe à l'exclusion du capteur de mouvement et des câbles de connexion de ce capteur.

Elle peut se présenter sous la forme d'un seul élément ou de plusieurs composants répartis dans le véhicule et comprend une unité de traitement, une mémoire électronique, une fonction de mesure du temps, deux interfaces pour cartes à mémoire pour le conducteur et le convoyeur, une imprimante, un écran, des connecteurs ainsi que des dispositifs permettant la saisie de données par l'utilisateur, un récepteur GNSS et un dispositif de communication à distance.

L'unité embarquée sur le véhicule peut se composer des éléments suivants soumis à homologation:

— une unité composée d'un seul élément (intégrant un récepteur GNSS et un dispositif de communication à distance),

— un élément principal (intégrant un dispositif de communication à distance) et un récepteur GNSS externe,

— un élément principal (intégrant un récepteur GNSS) et un dispositif de communication à distance externe,

— un élément principal, un récepteur GNSS externe et un dispositif de communication à distance externe.

Si l'unité embarquée sur le véhicule se présente sous la forme de plusieurs éléments répartis dans le véhicule, son élément principal est celui qui comprend l'unité de traitement, la mémoire électronique et la fonction de mesure du temps.

Le terme "unité embarquée sur le véhicule (VU)" désigne l'"unité embarquée sur le véhicule" ou l'"élément principal de l'unité embarquée sur le véhicule"»;

3) à l'article 6, le troisième alinéa est remplacé par le texte suivant:

«Toutefois, l'annexe IC s'applique à compter du 15 juin 2019, à l'exception de l'appendice 16, qui s'applique à compter du 2 mars 2016.»;

4) l'annexe IC est modifiée conformément à l'annexe I du présent règlement;

5) l'annexe II est modifiée conformément à l'annexe II du présent règlement.

Article 2

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 28 février 2018.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE I

L'annexe I C du règlement (UE) 2016/799 est modifiée comme suit:

1) la table des matières est modifiée comme suit:

a) le point 3.12.5 est remplacé par le point suivant:

«3.12.5. Lieux et positions des lieux où les périodes de travail journalières commencent et se terminent et/ou où les 3 heures de temps de conduite accumulé sont atteintes»;

b) le point 4.5.3.2.16 est remplacé par le texte suivant:

«4.5.3.2.16 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes»;

c) le point 4.5.4.2.14 est remplacé par le texte suivant:

«4.5.4.2.14 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes»;

d) le point 6.2 est remplacé par le texte suivant:

«6.2 Vérification de composants neufs ou réparés»;

2) le point 1 est modifié comme suit:

a) La définition ll) est remplacée par la définition suivante:

«ll) "dispositif de communication à distance" ou "dispositif de détection précoce à distance":

l'équipement de l'unité embarquée sur le véhicule utilisé pour les contrôles routiers ciblés;»;

b) la définition tt) est remplacée par la définition suivante:

«tt) "remise à l'heure":

un réglage de l'heure actuelle; ce réglage peut être exécuté de manière automatique à intervalles réguliers, sur la base de l'heure fournie par le récepteur GNSS, ou être effectué en mode "étalonnage";»;

c) le premier tiret de la définition yy) est remplacé par le texte suivant:

«— installé et utilisé uniquement sur les types de véhicules M1 et N1 (tels que définis à l'annexe II de la directive 2007/46/CE du Parlement européen et du Conseil (*), telle que modifiée en dernier lieu),»;

d) une nouvelle définition fff) est ajoutée:

«fff) "temps de conduite accumulé":

valeur représentant le nombre total de minutes de temps de conduite accumulé d'un véhicule donné.

La valeur du temps de conduite accumulé est un comptage libre de l'ensemble des minutes comptabilisées comme de la CONDUITE par la fonction de suivi des activités de conduite de l'appareil de contrôle. Elle n'est utilisée que pour déclencher l'enregistrement de la position du véhicule à chaque fois qu'un multiple de trois heures de conduite accumulé est atteint. L'accumulation débute au moment de l'activation de l'appareil de contrôle. Elle n'est affectée par aucune autre condition (p. ex. "hors champ" ou "trajet en ferry/train").

La valeur du temps de conduite accumulé n'est pas destinée à être affichée, imprimée ou téléchargée;»;

3) au point 2.3, le paragraphe 13, dernier tiret, est remplacé par le texte suivant:

«— les unités embarquées ont une période de validité opérationnelle normale de 15 ans à partir de la date effective de leurs certificats mais peuvent être utilisées pendant 3 mois supplémentaires, uniquement aux fins du téléchargement de données.»;

4) au point 2.4, le premier paragraphe est remplacé par le texte suivant:

«La sécurité du système vise à protéger la mémoire de manière à empêcher l'accès non autorisé et la manipulation de données, et à détecter les tentatives de manipulation, à préserver l'intégrité et l'authenticité des données échangées entre le capteur de mouvement et l'unité embarquée sur le véhicule ainsi qu'entre l'appareil de contrôle et les cartes tachygraphiques, à préserver l'intégrité et l'authenticité des données échangées entre l'unité embarquée sur véhicule et le dispositif GNSS externe, le cas échéant, à préserver la confidentialité, l'intégrité et l'authenticité des données échangées via la communication de détection précoce à distance à des fins de contrôle, et enfin à vérifier l'intégrité et l'authenticité des données téléchargées.»;

5) au point 3.2, le paragraphe 27, deuxième tiret, est remplacé par le texte suivant:

«— des positions correspondant aux lieux où le temps de conduite accumulé atteint un multiple de trois heures,»;

6) au point 3.4, le paragraphe 49 est remplacé par le texte suivant:

«49) Le premier changement d'activité vers PAUSE/REPOS ou DISPONIBILITÉ intervenant dans les 120 secondes qui suivent la sélection automatique de l'activité TRAVAIL en raison de l'arrêt du véhicule doit être considéré comme étant intervenu au moment de l'arrêt du véhicule (et peut par conséquent annuler le passage à l'activité TRAVAIL).»;

7) au point 3.6.1, le paragraphe 59 est remplacé par le texte suivant:

«59) Le conducteur indique alors l'emplacement actuel du véhicule, ce qui est considéré comme une saisie temporaire.

Dans les conditions suivantes, la saisie temporaire effectuée lors du dernier retrait de la carte est validée (c'est-à-dire qu'elle n'est plus écrasée):

— saisie d'un lieu où débute la période de travail journalière actuelle lors de la saisie manuelle en application de l'exigence 61,

— saisie suivante d'un lieu où débute la période de travail journalière actuelle si le détenteur de la carte n'indique aucun emplacement de début ou de fin de la période de travail lors de la saisie manuelle en application de l'exigence 61.

Dans les conditions suivantes, la saisie temporaire effectuée lors du dernier retrait de la carte est écrasée et la nouvelle valeur est validée:

— saisie suivante d'un lieu où s'achève la période de travail journalière actuelle si le détenteur de la carte n'indique aucun emplacement de début ou de fin de la période de travail lors de la saisie manuelle en application de l'exigence 61.»;

8) au point 3.6.2, les sixième et septième tirets sont remplacés par le texte suivant:

«— un lieu où s'est achevée une période de travail journalière précédente, associé à l'heure correspondante (qui écrase et valide la saisie effectuée lors du dernier retrait de la carte),

— un lieu où débute la période de travail journalière actuelle, associé à l'heure correspondante (qui valide une saisie temporaire effectuée lors du dernier retrait de la carte).»;

9) le point 3.9.15 est remplacé par le texte suivant:

«3.9.15 Événement "Conflit temporel"

86) Cet événement est déclenché **en mode autre qu'étalonnage** lorsque la VU détecte un écart de plus d'une minute entre le temps fourni par sa fonction de mesure du temps et le temps fourni par le récepteur GNSS. Cet événement est enregistré avec la valeur de l'horloge interne de l'unité embarquée sur le véhicule et s'accompagne d'une remise à l'heure automatique. Après le déclenchement d'un événement "Conflit temporel", la VU ne générera plus d'autres événements "Conflit temporel" pendant les 12 heures suivantes. Cet événement n'est pas déclenché lorsqu'aucun signal GNSS valable n'a pu être détecté par le récepteur GNSS depuis au moins 30 jours.»;

10) au point 3.9.17, le tiret suivant est ajouté:

«— anomalie sur l'interface ITS (le cas échéant)»;

11) le point 3.10 est modifié comme suit:

i) le texte précédant le tableau figurant au paragraphe 89 est remplacé par ce qui suit:

«L'appareil de contrôle détecte les anomalies par des autotests et des tests intégrés, selon le tableau suivant:»;

ii) la ligne suivante est ajoutée au tableau:

«Interface ITS (facultatif)	Fonctionnement correct»	

12) au point 3.12, le deuxième tiret est remplacé par le texte suivant:

«— le nombre moyen de positions par jour est défini comme au moins 6 positions correspondant aux lieux où commence la période de travail journalière, 6 positions correspondant aux lieux où le temps de conduite accumulé atteint un multiple de trois heures et 6 positions correspondant aux lieux où se termine la période de travail journalière, de sorte qu'au moins 6570 positions sont comprises dans ces "365 jours",»;

13) le point 3.12.5 est modifié comme suit:

a) le titre et le paragraphe 108 sont remplacés par le texte suivant:

«3.12.5. Lieux et positions des lieux où les périodes de travail journalières commencent et se terminent et/ou où les 3 heures de temps de conduite accumulé sont atteintes

108) L'appareil de contrôle doit enregistrer et stocker dans sa mémoire:

— les lieux et positions des lieux où le conducteur et/ou le convoyeur commencent leur période de travail journalière;

— les positions des lieux où le temps de conduite accumulé atteint un multiple de trois heures;

— les lieux et positions des lieux où le conducteur et/ou le convoyeur terminent leur période de travail journalière.»;

b) le paragraphe 110, quatrième tiret, est remplacé par le texte suivant:

«— le type de saisie (début, fin ou 3 heures de temps de conduite accumulé),»;

c) le paragraphe 111 est remplacé par le texte suivant:

«111) La mémoire doit être en mesure de conserver pendant au moins 365 jours les lieux et les positions des lieux où les périodes de travail journalières commencent et se terminent, et/ou où les 3 heures de temps de conduite accumulé sont atteintes.»;

14) au point 3.12.7, le paragraphe 116 est remplacé par le texte suivant:

«116) L'appareil de contrôle enregistre et stocke dans sa mémoire la vitesse instantanée du véhicule et la date et l'heure correspondante à chaque seconde d'au moins les 24 dernières heures au cours desquelles le véhicule était en mouvement.»;

15) le tableau figurant au point 3.12.8 est modifié comme suit:

a) l'élément suivant est inséré entre les éléments «Absence d'informations de positionnement en provenance du récepteur GNSS» et «Erreur sur les données de mouvement»:

«Erreur de communication avec le dispositif GNSS externe	— l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, — les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	— la date et l'heure du début de l'événement, — la date et l'heure de fin de l'événement, — le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, — le nombre d'événements semblables survenus le même jour.»

b) l'élément «Conflit temporel» est remplacé par le texte suivant:

«Conflit temporel	— l'événement le plus grave (c'est-à-dire celui présentant l'écart le plus important entre la date et l'heure de l'appareil de contrôle et la date et l'heure du GNSS) des 10 derniers jours d'occurrence, — les 5 événements les plus graves au cours des 365 derniers jours.	— la date et l'heure de l'appareil de contrôle — la date et l'heure du GNSS, — le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, — le nombre d'événements semblables survenus le même jour.»

16) au point 3.20, le paragraphe 200 est remplacé par le texte suivant:

«200) L'appareil de contrôle peut également être équipé d'interfaces normalisées permettant l'utilisation par un dispositif externe, en mode opérationnel ou "étalonnage", des données enregistrées ou produites par le tachygraphe.

Dans l'appendice 13, une interface ITS facultative est spécifiée et normalisée. D'autres interfaces d'unité embarquée sur le véhicule peuvent coexister, à condition qu'elles respectent pleinement les exigences de l'appendice 13 en termes de liste minimale de données, de sécurité et de consentement du conducteur.

Le consentement du conducteur ne s'applique pas aux données transmises par l'appareil de contrôle au réseau du véhicule. En cas de traitement ultérieur, hors du réseau du véhicule, des données à caractère personnel introduites dans le réseau du véhicule, il relève de la responsabilité du constructeur du véhicule de s'assurer que ce traitement de données à caractère personnel est conforme au règlement (UE) 2016/679 (le "règlement général sur la protection des données").

Le consentement du conducteur ne s'applique pas non plus aux données tachygraphiques téléchargées vers une entreprise à distance (exigence 193), ce cas de figure étant contrôlé par le droit d'accès de la carte d'entreprise.

Les exigences suivantes sont applicables aux données ITS mises à disposition par l'intermédiaire de cette interface:

— ces données constituent un ensemble de données existantes sélectionnées qui proviennent du dictionnaire de données du tachygraphe (appendice 1),

— un sous-ensemble de ces données sélectionnées constitue des "données à caractère personnel",

— ce sous-ensemble de "données à caractère personnel" n'est disponible que si le consentement vérifiable du conducteur, qui accepte que ses données personnelles puissent quitter le réseau du véhicule, est activé,

— l'accord du conducteur peut être activé ou désactivé à tout moment, à l'aide de commandes se trouvant dans le menu, à condition que la carte du conducteur soit insérée,

— l'ensemble et le sous-ensemble de données seront diffusés via le protocole sans fil Bluetooth dans le rayon de la cabine du véhicule, avec une fréquence de rafraîchissement d'une minute,

— le couplage du dispositif externe avec l'interface ITS sera protégé par un code PIN dédié et aléatoire d'au moins 4 chiffres, enregistré et affichable dans chaque VU,

— en aucun cas la présence de l'interface ITS ne peut perturber ou affecter le fonctionnement correct et la sécurité de la VU.

D'autres données peuvent également être transmises en plus de l'ensemble de données existantes sélectionnées, considérées comme la liste minimale, à condition qu'elles ne puissent pas être considérées comme des données à caractère personnel.

L'appareil de contrôle permet de communiquer le statut du consentement du conducteur aux autres plateformes du réseau du véhicule.

Lorsque le contact du véhicule est en position MARCHE, ces données sont transmises en permanence.»;

17) au point 3.23, le paragraphe 211 est remplacé par le texte suivant:

«211) Le réglage de l'heure de l'horloge interne de la VU est automatiquement réajusté toutes les 12 heures. Lorsque ce réajustement est impossible en raison de l'indisponibilité du signal GNSS, le réglage de l'heure se fait dès que la VU est en mesure d'accéder à une heure valable fournie par le récepteur GNSS, selon les conditions d'allumage du véhicule. La base temps pour le réglage automatique de l'heure de l'horloge interne de la VU doit être déterminée à partir du récepteur GNSS.»;

18) au point 3.26, les paragraphes 225 et 226 sont remplacés par le texte suivant:

«225) Une plaque signalétique doit être fixée sur chaque composant séparé de l'appareil de contrôle et doit comporter les indications suivantes:

— nom et adresse du fabricant,

— numéro de pièce du fabricant et année de fabrication,

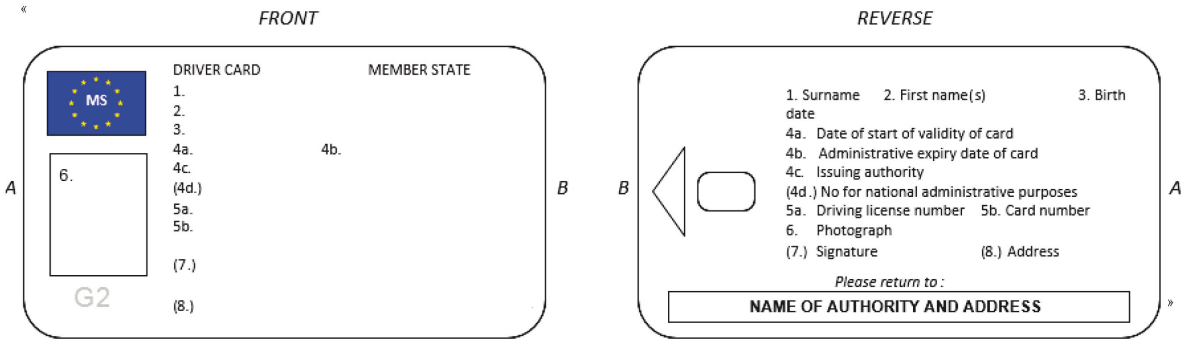
— numéro de série,

— marque d'homologation.

226) Lorsque l'espace disponible est insuffisant pour faire figurer l'ensemble des indications précitées, la plaque signalétique doit indiquer au moins: le nom ou le logo du fabricant, et le numéro de la pièce.»;

19) au point 4.1, le dessin correspondant au recto et au verso de la carte de conducteur est remplacé par le dessin suivant:

«



»

20) au point 4.5.3.1.8, le paragraphe 263, premier tiret, est remplacé par le texte suivant:

«— anomalie de la carte (lorsque la carte est à l'origine de l'anomalie),»;

21) au point 4.5.3.2.8, le paragraphe 288, premier tiret, est remplacé par le texte suivant:

«— anomalie de la carte (lorsque la carte est à l'origine de l'anomalie),»;

22) le point 4.5.3.2.16 est remplacé par le texte suivant:

«4.5.3.2.16 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes

305) La carte de conducteur doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures:

— la date et l'heure où le temps de conduite accumulé atteint un multiple de trois heures,

— la position du véhicule,

— la précision GNSS, la date et l'heure de détermination de la position,

— le kilométrage du véhicule.

306) La carte de conducteur doit pouvoir stocker au moins 252 enregistrements de ce type.»;

23) le point 4.5.4.2.14 est remplacé par le texte suivant:

«4.5.4.2.14 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes

353) La carte d'atelier doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures:

— la date et l'heure où le temps de conduite accumulé atteint un multiple de trois heures,

— la position du véhicule,

— la précision GNSS, la date et l'heure de détermination de la position,

— le kilométrage du véhicule.

354) La carte d'atelier doit permettre le stockage d'au moins 18 enregistrements de ce type.»;

24) au point 5.2, le paragraphe 396 est remplacé par le texte suivant:

«396) La plaquette doit comporter au moins les indications suivantes:

— le nom, l'adresse ou la raison sociale de l'installateur ou de l'atelier agréé,

— le coefficient caractéristique du véhicule, sous la forme 'w = … imp/km',

— la constante de l'appareil de contrôle, sous la forme 'k = … imp/km',

— les circonférences effectives des pneumatiques, sous la forme 'l = … mm',

— la taille des pneumatiques,

— la date à laquelle le coefficient caractéristique du véhicule et la circonférence effective des pneumatiques ont été mesurés,

— le numéro d'identification du véhicule,

— la présence (ou non) d'un dispositif GNSS externe,

— le numéro de série du dispositif GNSS externe, le cas échéant,

— le numéro de série de l'appareil de communication à distance, le cas échéant,

— le numéro de série de tous les scellements en place,

— la partie du véhicule où l'adaptateur, le cas échéant, est installé,

— la partie du véhicule où le capteur de mouvement est installé, s'il n'est pas connecté à la boîte de vitesses ou si un adaptateur n'est pas utilisé,

— une description de la couleur du câble entre l'adaptateur et la partie du véhicule qui fournit ses impulsions entrantes,

— le numéro de série du capteur de mouvement intégré de l'adaptateur.»;

25) le point 5.3 est modifié comme suit:

a) un nouveau paragraphe 398 *bis*) est ajouté après le paragraphe 398)

«398 *bis*) Les scellements susmentionnés sont certifiés sur la base de la norme EN 16882:2016.»;

b) au paragraphe 401, le deuxième alinéa est remplacé par le texte suivant:

«Ce numéro d'identification unique est défini comme suit: MMNNNNNNNN, faisant l'objet d'un marquage indélébile, où MM est l'identifiant unique du fabricant (enregistrement dans une base de données qui sera gérée par la CE) et NNNNNNNN est le numéro alphanumérique du scellement, unique dans le domaine du fabricant.»;

c) le paragraphe 403 est remplacé par le texte suivant:

«403) Les fabricants de scellements doivent être enregistrés dans une base de données dédiée lorsqu'ils obtiennent la certification d'un modèle de scellement selon la norme EN 16882:2016 et rendre publics leurs numéros d'identification de scellements par une procédure établie par la Commission européenne.»;

d) le paragraphe 404 est remplacé par le texte suivant:

«404) Les ateliers et constructeurs de véhicules agréés doivent, dans le cadre du règlement (UE) n° 165/2014, n'utiliser que des scellements certifiés selon la norme EN 16882:2016 issus des fabricants de scellements répertoriés dans la base de données mentionnée ci-dessus.»;

26) le point 6.2 est remplacé par le texte suivant:

«6.2. Vérification de composants neufs ou réparés

407) Chaque dispositif, neuf ou réparé, doit être vérifié pour s'assurer de son fonctionnement correct et de la précision de ses relevés et de ses enregistrements, dans les limites fixées au chapitre 3, points 2.1, 2.2, 2.3 et 3.»;

27) au point 6.3, le paragraphe 408 est remplacé par le texte suivant:

«408) Lors de son montage sur un véhicule, l'ensemble de l'installation (y compris l'appareil de contrôle) doit respecter les dispositions en matière de tolérances maximales fixées au chapitre 3, points 2.1, 2.2, 2.3 et 3. L'ensemble de l'installation doit être scellé conformément au chapitre 5.3 et comprendre un étalonnage.»;

28) le point 8.1) est modifié comme suit

a) au point 8.1, le texte introductif précédant le paragraphe 425 est remplacé par le texte suivant:

«Aux fins du présent chapitre, on entend par "appareil de contrôle", l'"appareil de contrôle ou ses composants". Aucune homologation n'est exigée pour le(s) câble(s) reliant le capteur de mouvement à la VU, le dispositif GNSS externe à la VU ou le dispositif externe de communication à distance à la VU. Le papier utilisé pour l'appareil de contrôle est considéré comme un composant de l'appareil.

Tout fabricant peut demander l'homologation de son ou ses composants d'appareil de contrôle avec tout autre composant d'appareil de contrôle, pour autant que chaque composant soit conforme aux exigences contenues dans la présente annexe. Les fabricants peuvent également demander l'homologation de l'appareil de contrôle.

Comme décrit dans la définition 10 de l'article 2 du présent règlement, les unités embarquées ont des variantes en ce qui concerne l'assemblage des composants. Quel que soit l'assemblage des composants de l'unité embarquée sur véhicule, l'antenne externe et (le cas échéant) du coupleur d'antenne connecté au récepteur GNSS ou au dispositif de communication à distance ne sont pas couverts par l'homologation de l'unité embarquée sur véhicule.

Les fabricants ayant obtenu l'homologation de leur appareil de contrôle doivent néanmoins tenir une liste publique des antennes et coupleurs compatibles avec chaque unité embarquée sur véhicule, dispositif GNSS externe et équipement externe de communication à distance homologués.»;

b) le paragraphe 427 est remplacé par le texte suivant:

«427) Les autorités d'homologation des États membres n'accorderont pas de certificat d'homologation tant qu'elles ne sont pas en possession:

— d'un certificat de sécurité (s'il est requis au titre de la présente annexe),

— d'un certificat de fonctionnement,

— et d'un certificat d'interopérabilité (s'il est requis au titre de la présente annexe)

pour l'appareil de contrôle ou la carte tachygraphique faisant l'objet de la demande d'homologation.»;

29) l'appendice 1 est modifié comme suit:

a) la table des matières est modifiée comme suit:

i) le point 2.63 est remplacé par le texte suivant:

«2.63 Réservé pour une utilisation future»;

ii) le point 2.78 est remplacé par le texte suivant:

«2.78 GNSSAccumulatedDriving»;

iii) le point 2.79 est remplacé par le texte suivant:

«2.79 GNSSAccumulatedDrivingRecord»;

iv) le point 2.111 est remplacé par le texte suivant:

«2.111 NoOfGNSSADRecords»;

v) le point 2.160 est remplacé par le texte suivant:

«2.160 Réservé pour une utilisation future»;

vi) le point 2.203 est remplacé par le texte suivant:

«2.203 VuGNSSADRecord»;

vii) le point 2.204 est remplacé par le texte suivant:

«2.204 VuGNSSADRecordArray»;

viii) le point 2.230 est remplacé par le texte suivant:

«2.230 Réservé pour une utilisation future»;

ix) le point 2.231 est remplacé par le texte suivant:

«2.231 Réservé pour une utilisation future»;

b) au point 2, le texte suivant est ajouté avant le point 2.1:

«Pour les types de données de carte utilisés pour les applications de génération 1 et 2, la taille indiquée dans le présent appendice est celle relative à l'application de génération 2. La taille relative à l'application de génération 1 est censée être déjà connue du lecteur. Les numéros des exigences de l'annexe IC relatives à ces types de données couvrent à la fois les applications de génération 1 et de génération 2.»;

c) le point 2.19 est remplacé par le texte suivant:

«2.19. **CardEventData**

Génération 1:

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 260 et 318 de l'annexe IC).

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

CardEventData consiste en une séquence de cardEventRecords (à l'exception des relevés portant sur les tentatives éventuelles d'atteinte à la sécurité, lesquels sont regroupés dans le dernier ensemble de données de la séquence) dont l'agencement correspond à celui des EventFaultType rangés par ordre croissant.

cardEventRecords consiste en un jeu de relevés d'événements correspondant à un type d'événement donné (ou à cette catégorie d'événements dans laquelle se rangent les tentatives d'atteinte à la sécurité).

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 285 et 341 de l'annexe IC).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
  cardEventRecords                    SET SIZE(NoOfEventsPerType) OF
                                      CardEventRecord
}
```

CardEventData consiste en une séquence de cardEventRecords (à l'exception des relevés portant sur les tentatives éventuelles d'atteinte à la sécurité, lesquels sont regroupés dans le dernier ensemble de données de la séquence) dont l'agencement correspond à celui des EventFaultType rangés par ordre croissant.

cardEventRecords consiste en un jeu de relevés d'événements correspondant à un type d'événement donné (ou à cette catégorie d'événements dans laquelle se rangent les tentatives d'atteinte à la sécurité).»;

d) le point 2.30 est remplacé par le texte suivant:

«2.30. **CardRenewalIndex**

Indice de renouvellement d'une carte [définition i)].

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Attribution de valeur: (cf. chapitre 7 de la présente annexe).

"0" Première édition.

Ordre croissant: "0, …, 9, A, …, Z" »;

e) au point 2.61, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

```
«DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

Outre la génération 1, les éléments de données suivants sont utilisés:

noOfGNSSADRecords indique le nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

noOfSpecificConditionRecords indique le nombre de relevés de conditions particulières que la carte est susceptible de mémoriser.

noOfCardVehicleUnitRecords indique le nombre de relevés utilisés par les unités embarquées sur le véhicule que la carte est susceptible de mémoriser.»;

f) le point 2.63 est remplacé par le texte suivant:

«2.63. **Réservé pour une utilisation future**»;

g) au point 2.67, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

«Les mêmes valeurs que pour la génération 1 servent pour les ajouts suivants:

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS interface module          (10),
--Plaque                        (11),--may be used in SealRecord
--M1/N1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Note 1: Les valeurs de génération 2 pour la plaque, l'adaptateur et la connexion externe GNSS ainsi que les valeurs de génération 1 pour l'unité embarquée sur véhicule et le capteur de mouvement peuvent servir en SealRecord, le cas échéant.

Note 2: Dans le champ CardHolderAuthorisation (CHA) d'un certificat de génération 2, les valeurs (1), (2) et (6) doivent être interprétées comme indiquant un certificat d'authentification mutuelle du type d'équipement concerné. Pour indiquer le certificat à utiliser pour la création d'une signature numérique, les valeurs (17), (18) ou (19) doivent être utilisées.»;

h) au point 2.70, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

«Génération 2:

'0x'H	événements généraux,
'00'H	absence d'informations complémentaires,
'01'H	insertion d'une carte non valable,
'02'H	conflit de carte,
'03'H	chevauchement temporel,
'04'H	conduite sans carte appropriée,
'05'H	insertion de carte en cours de conduite,
'06'H	dernière session incorrectement clôturée,
'07'H	excès de vitesse,
'08'H	Coupure d'alimentation électrique,
'09'H	erreur sur les données de mouvement,
'0A'H	conflit concernant le mouvement du véhicule,
'0B'H	conflit temporel (GNSS contre l'horloge interne de la VU),
'0C'H	erreur de communication avec l'équipement de communication à distance,
'0D'H	absence d'informations de positionnement en provenance du récepteur GNSS,
'0E'H	erreur de communication avec le dispositif GNSS externe,
'0F'H	RFU,
'1x'H	tentatives d'atteinte à la sécurité en rapport avec l'unité embarquée sur véhicule,
'10'H	absence d'informations complémentaires,
'11'H	défaut d'authentification du capteur de mouvement,
'12'H	défaut d'authentification d'une carte tachygraphique,
'13'H	remplacement sans autorisation du capteur de mouvement,
'14'H	défaut d'intégrité affectant l'entrée de données sur la carte,
'15'H	défaut d'intégrité affectant les données utilisateur mémorisées,
'16'H	erreur de transfert de données internes,
'17'H	ouverture illicite d'un boîtier,
'18'H	sabotage du matériel,
'19'H	détection de violation du dispositif GNSS,
'1A'H	défaut d'authentification du dispositif GNSS externe,
'1B'H	expiration du certificat du dispositif GNSS externe,
'1C'H à '1F'H	RFU,
'2x'H	tentatives d'atteinte à la sécurité en rapport avec le capteur de mouvement,
'20'H	absence d'informations complémentaires,
'21'H	échec d'une authentification,
'22'H	défaut d'intégrité affectant les données mémorisées,
'23'H	erreur de transfert de données internes,
'24'H	ouverture illicite d'un boîtier,
'25'H	sabotage du matériel,
'26'H à '2F'H	RFU,
'3x'H	anomalies affectant l'appareil de contrôle,
'30'H	absence d'informations complémentaires,
'31'H	anomalie interne affectant la VU,
'32'H	anomalie affectant l'imprimante,
'33'H	anomalie affectant l'affichage,
'34'H	anomalie affectant le téléchargement,
'35'H	anomalie affectant le capteur de mouvement,
'36'H	récepteur du dispositif GNSS interne,
'37'H	dispositif GNSS externe,
'38'H	dispositif de communication à distance,
'39'H	interface ITS,
'3A'H à '3F'H	RFU,
'4x'H	anomalies affectant une carte,
'40'H	absence d'informations complémentaires,
'41'H à '4F'H	RFU,
'50'H à '7F'H	RFU,
'80'H à 'FF'H	propre au fabricant.»;

i) le point 2.71 est remplacé par le texte suivant:

«2.71. **ExtendedSealIdentifier**

Génération 2:

L'identifiant de scellement étendu identifie un scellement de manière unique (exigence 401, annexe IC).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode correspond au code du fabricant du scellement.

sealIdentifier désigne l'identifiant du scellement, unique pour le fabricant.»;

j) les points 2.78 et 2.79 sont remplacés par le texte suivant:

«2.78 **GNSSAccumulatedDriving**

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier, relatives à la position GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 306 et 354, annexe IC).

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord désigne l'indice du dernier relevé de temps de conduite accumulé GNSS actualisé par le système.

Attribution de valeur est le nombre correspondant au numérateur du relevé de temps de conduite accumulé GNSS, commençant par une série de '0' pour la première occurrence d'un relevé de temps de conduite accumulé GNSS dans la structure considérée.

gnssContinuousDrivingRecords désigne le jeu de relevés contenant la date et l'heure lorsque le temps de conduite accumulé atteint un multiple de trois heures, ainsi que les informations relatives à la position du véhicule.

2.79. **GNSSAccumulatedDrivingRecord**

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier, relatives à la position GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 305 et 353, annexe IC).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

timeStamp désigne la date et l'heure lorsque le temps de conduite accumulé du détenteur de la carte atteint un multiple de trois heures.

gnssPlaceRecord contient les informations relatives à la position du véhicule.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique pour laquelle le temps de conduite accumulé atteint un multiple de trois heures.»;

k) le point 2.86 est remplacé par le texte suivant:

«2.86. **KeyIdentifier**

Identificateur unique d'une clé publique permettant de la désigner et de la sélectionner. Cet identificateur identifie également le titulaire de la clé.

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

La première option permet de désigner la clé publique d'une unité embarquée sur véhicule, d'une carte tachygraphique ou d'un dispositif GNSS externe.

La seconde option permet de désigner la clé publique d'une unité embarquée sur véhicule (en cas de méconnaissance du numéro de série de l'unité embarquée, lors de l'élaboration du certificat).

La troisième option permet de désigner la clé publique d'un État membre.»;

l) le point 2.92 est remplacé par le texte suivant:

«2.92. **MAC**

Génération 2:

Un total de contrôle cryptographique sur une longueur de 8, 12 ou 16 octets correspondant à des suites chiffrées spécifiées dans l'appendice 11.

```
MAC ::= CHOICE {
   Mac8                 OCTET STRING (SIZE(8)),
   Mac12                OCTET STRING (SIZE(12)),
   Mac16                OCTET STRING (SIZE(16)),
}
```

»;

m) le point 2.111 est remplacé par le texte suivant:

«2.111. **NoOfGNSSADRecords**

Génération 2:

Nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

$$\text{NoOfGNSSADRecords ::= INTEGER (0..2}^{16}\text{-1)}$$

Assignation de valeur: cf. appendice 2.»;

n) au point 2.120, l'assignation de valeur «16H» est remplacée par le texte suivant:

«'16'H VuGNSSADRecord »;

o) le point 2.160 est remplacé par le texte suivant:

«2.160. **Réservé pour une utilisation future**»;

p) le point 2.162 est remplacé par le texte suivant:

«2.162. **TimeReal**

Code associé à un champ combinant date et heure exprimées en secondes à compter de 00h00m00s TUC le 1er janvier 1970 (UTC).

```
TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)
```

Assignation de valeur — Octet aligné: nombre de secondes écoulées depuis minuit TUC, le 1er janvier 1970.

La date/heure future la plus avancée se situe en l'an 2106.»;

q) le point 2.179 est remplacé par le texte suivant:

«2.179 **VuCardRecord**

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à la carte tachygraphique utilisée (exigence 132, annexe IC).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation est le numéro complet et la génération de la carte utilisée (type de données 2.74).

cardExtendedSerialNumber tel qu'extrait du fichier EF_ICC sous le FM de la carte.

cardStructureVersion telle qu'extraite du fichier élémentaire EF_Application_Identification sous le fichier spécialisé DF_Tachograph_G2.

cardNumber tel qu'extrait du fichier élémentaire FE_Identification sous le fichier spécialisé DF_Tachograph_G2.»;

r) les points 2.203 et 2.204 sont remplacés par le texte suivant:

«2.203 **VuGNSSADRecord**

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule relatives à la position GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 108 et 110, annexe IC).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp désigne la date et l'heure où le temps de conduite accumulé atteint un multiple de trois heures.

cardNumberAndGenDriverSlot identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération.

cardNumberAndGenCodriverSlot identifie la carte insérée dans le lecteur réservé au convoyeur ainsi que sa génération.

gnssPlaceRecord contient les informations relatives à la position du véhicule.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique pour laquelle le temps de conduite accumulé atteint un multiple de trois heures.

2.204. **VuGNSSADRecordArray**

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule relatives à la position GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 108 et 110, annexe IC).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType indique le type de relevé (VuGNSSADRecord).

Assignation de valeur: Cf. RecordType

recordSize indique la taille des VuGNSSADRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés de temps de conduite accumulé GNSS.»;

s) les points 2.230 et 2.231 sont remplacés par le texte suivant:

«2.230. Réservé pour une utilisation future.

2.231. Réservé pour une utilisation future»;

t) au point 2.234, le texte qui suit le titre «Génération 2» est remplacé par le texte suivant:

```
«WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfEventsPerType                   NoOfEventsPerType,
    noOfFaultsPerType                   NoOfFaultsPerType,
    activityStructureLength             CardActivityLengthRange,
    noOfCardVehicleRecords              NoOfCardVehicleRecords,
    noOfCardPlaceRecords                NoOfCardPlaceRecords,
    noOfCalibrationRecords              NoOfCalibrationRecords,
    noOfGNSSADRecords                   NoOfGNSSADRecords,
    noOfSpecificConditionRecords        NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords          NoOfCardVehicleUnitRecords
}
```

Outre la génération 1, les éléments de données suivants sont utilisés:

noOfGNSSADRecords indique le nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

noOfSpecificConditionRecords indique le nombre de relevés de conditions particulières que la carte est susceptible de mémoriser.

noOfCardVehicleUnitRecords indique le nombre de relevés utilisés par les unités embarquées sur le véhicule que la carte est susceptible de mémoriser»;

30) l'appendice 2 est modifié comme suit:

a) au point 1.1, les abréviations suivantes sont ajoutées:

«CHA Autorisation d'un titulaire de certificat

DO Objet de données»;

b) le point 3.3 est modifié comme suit:

i) le paragraphe TCS_24 est remplacé par le texte suivant:

«TCS_24 Ces conditions de sécurité peuvent être liées selon les manières suivantes:

ET: Toutes les conditions de sécurité doivent être remplies

OU: Au moins l'une des conditions de sécurité doit être remplie

Les conditions d'accès au système de fichiers, à savoir les commandes SELECT, READ BINARY et UPDATE BINARY sont spécifiées au chapitre 4. Les conditions d'accès des autres commandes sont spécifiées dans les tableaux suivants. Le terme "non applicable" est utilisé s'il n'est pas exigé de prendre en charge cette commande. Dans ce cas, la commande est ou n'est pas prise en charge, mais la condition d'accès est hors champ.»;

ii) au paragraphe TCS_25, le tableau est remplacé par le tableau suivant:

«Commande	Carte du conducteur	Carte atelier	Carte de contrôle	Carte d'entreprise
External Authenticate				
— Pour l'authentification de génération 1	ALW	ALW	ALW	ALW
— Pour l'authentification de génération 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Compute Digital Signature	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Hash	Sans objet	Sans objet	ALW	Sans objet

Commande	Carte du conducteur	Carte atelier	Carte de contrôle	Carte d'entreprise
PERFORM HASH of FILE	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	ALW	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet»

iii) au paragraphe TCS_26, le tableau est remplacé par le tableau suivant:

«Commande	Carte du conducteur	Carte atelier	Carte de contrôle	Carte d'entreprise
External Authenticate				
— Pour l'authentification de génération 1	Sans objet	Sans objet	Sans objet	Sans objet
— Pour l'authentification de génération 2	ALW	PWD	ALW	ALW
Internal Authenticate	Sans objet	Sans objet	Sans objet	Sans objet
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Sans objet	ALW	ALW	Sans objet
PSO: Compute Digital Signature	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Hash	Sans objet	Sans objet	ALW	Sans objet
PERFORM HASH of FILE	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	ALW	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet»

iv) au paragraphe TCS_27, le tableau est remplacé par le tableau suivant:

«Commande	Carte du conducteur	Carte atelier	Carte de contrôle	Carte d'entreprise
External Authenticate				
— Pour l'authentification de génération 1	Sans objet	Sans objet	Sans objet	Sans objet
— Pour l'authentification de génération 2	ALW	PWD	ALW	ALW
Internal Authenticate	Sans objet	Sans objet	Sans objet	Sans objet
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Compute Digital Signature	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Hash	Sans objet	Sans objet	Sans objet	Sans objet
PERFORM HASH of FILE	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	Sans objet	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet»

c) au point 3.4, le paragraphe TCS_29 est remplacé par le texte suivant:

«TCS_29 Les mots d'état SW1 et SW2 accompagnent tout message de réponse. Ils indiquent l'état de traitement de la commande correspondante.

SW1	SW2	Signification
90	00	Traitement normal.
61	XX	Traitement normal. XX = nombre d'octets de réponse disponibles.
62	81	Traitement d'avertissement. Une partie des données renvoyées peut être corrompue
63	00	Échec de l'authentification (Avertissement)
63	CX	CHV erronées (PIN). Compteur de tentatives restantes assuré par "X"

SW1	SW2	Signification
64	00	Erreur d'exécution - État de la mémoire rémanente inchangé. Erreur d'intégrité
65	00	Erreur d'exécution - État de la mémoire rémanente modifié.
65	81	Erreur d'exécution - État de la mémoire rémanente modifié - Défaillance de la mémoire.
66	88	Erreur de sécurité: Total de contrôle cryptographique erroné (en cours de messagerie sécurisée) ou Certificat erroné (pendant la vérification du certificat) ou Cryptogramme erroné (pendant l'authentification externe) ou Signature erronée (pendant la vérification de la signature)
67	00	Longueur erronée (Lc ou Le erronée)
68	83	Dernière commande de la chaîne prévisible
69	00	Commande interdite (pas de réponse disponible en T=0)
69	82	État de sécurité non satisfait
69	83	Méthode d'authentification bloquée
69	85	Conditions d'utilisation non satisfaites
69	86	Commande non autorisée (pas d'EF actif)
69	87	Absence des objets informatifs SM prévus
69	88	Objets informatifs SM incorrects
6A	80	Paramètres incorrects dans les zones de données
6A	82	Fichier introuvable.
6A	86	Paramètres P1-P2 erronés
6A	88	Données désignées introuvables
6B	00	Paramètres erronés (déplacement hors de l'EF)
6C	XX	Longueur erronée, le SW2 indique la longueur exacte. Aucune zone de données n'est renvoyée.
6D	00	Code d'instruction non pris en charge ou incorrect
6E	00	Classe non prise en charge
6F	00	— Autres erreurs de contrôle

Les mots d'état supplémentaires au sens de la norme ISO/IEC 7816-4 peuvent être renvoyés si leur comportement n'est pas explicitement mentionné dans le présent appendice.

Par exemple, les mots d'état suivants peuvent éventuellement être renvoyés:

6881: Canal logique non pris en charge

6882: Messagerie sécurisée non prise en charge»;

d) au point 3.5.1.1, le paragraphe TCS_38, dernier tiret, est remplacé par le texte suivant:

«— Si l'application sélectionnée est considérée comme altérée (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

e) au point 3.5.1.2, le paragraphe TCS_41, dernier tiret, est remplacé par le texte suivant:

«— Si le fichier sélectionné est considéré comme altéré (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

f) au point 3.5.2.1, le paragraphe TCS_43, sixième tiret, est remplacé par le texte suivant:

«— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable et le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

g) le point 3.5.2.1.1 est modifié comme suit:

i) au paragraphe TCS_45, le tableau est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
#1	1	"81h"	T_{PV}: balise indiquant la valeur des données ordinaires
#2	L	"NNh" ou "81 NNh"	L_{PV}: longueur des données renvoyées (=Le original). L équivaut à 2 octets si L_{PV}> 127 octets.
#(2+L) - #(1+L+NN)	NN	"XX..XXh"	Valeur des données ordinaires
#(2+L+NN)	1	"99h"	Balise d'état de traitement (SW1-SW2) - facultatif pour la messagerie sécurisée de génération 1
#(3+L+NN)	1	"02h"	Longueur de l'état de traitement – facultatif pour la messagerie sécurisée de génération 1
#(4+L+NN) - #(5+L+NN)	2	"XX XXh"	État de traitement de l'APDU de réponse non protégée - facultatif pour la messagerie sécurisée de génération 1
#(6+L+NN)	1	"8Eh"	TCC: balise indiquant le total de contrôle cryptographique
#(7+L+NN)	1	"XXh"	LCC: longueur du total de contrôle cryptographique suivant "04h" pour la messagerie sécurisée de génération 1 (cf. appendice 11, partie A) "08h", "0Ch" ou "10h" selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11, partie B)

Octet	Longueur	Valeur	Description
#(8+L+NN)-#(7+M+L+NN)	M	"XX..XXh"	Total de contrôle cryptographique
SW	2	"XXXXh"	Mots d'état (SW1, SW2)»

ii) au paragraphe TCS_46, le tableau est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
#1	1	"87h"	$T_{PI\ CG}$: balise indiquant des données codées (cryptogramme)
#2	L	"MMh" ou "81 MMh"	$L_{PI\ CG}$: longueur des données chiffrées renvoyées (différentes du Le original de la commande en raison du remplissage). L équivaut à 2 octets si LPI CG > 127 octets
#(2+L)-#(1+L+MM)	MM	"01XX..XXh"	Données codées: cryptogramme et indicateur de remplissage
#(2+L+MM)	1	"99h"	Balise d'état de traitement (SW1-SW2) – facultatif pour la messagerie sécurisée de génération 1
#(3+L+MM)	1	"02h"	Longueur de l'état de traitement - facultatif pour la messagerie sécurisée de génération 1
#(4+L+MM) - #(5+L+MM)	2	"XX XXh"	État de traitement de l'APDU de réponse non protégée – facultatif pour la messagerie sécurisée de génération 1
#(6+L+MM)	1	"8Eh"	TCC: balise indiquant le total de contrôle cryptographique
#(7+L+MM)	1	"XXh"	LCC: longueur du total de contrôle cryptographique suivant "04h" pour la messagerie sécurisée de génération 1 (cf. appendice 11, partie A) "08h", "0Ch" ou "10h" selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11, partie B)
#(8+L+MM)-#(7+N+L+MM)	N	"XX..XXh"	Total de contrôle cryptographique
SW	2	"XXXXh"	Mots d'état (SW1, SW2)»

h) au point 3.5.2.2, le paragraphe TCS_50, sixième tiret, est remplacé par le texte suivant:

«— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable et le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

i) le point 3.5.2.3, paragraphe TCS_52, est modifié comme suit:

i) la dernière ligne du tableau est remplacée par la suivante:

«Le	1	"XXh"	Conformément à la norme ISO/IEC 7816-4»

ii) la phrase suivante est ajoutée:

«Si T=0, la carte suppose la valeur Le = "00h" si aucune messagerie sécurisée n'est appliquée.

Si T=1, l'état de traitement renvoyé est "6700" si Le="01h".»;

j) au point 3.5.2.3, le paragraphe TCS_53, sixième tiret, est remplacé par le texte suivant:

«— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable et le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

k) au point 3.5.3.2, le paragraphe TCS_63, sixième tiret, est remplacé par le texte suivant:

«— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable et le logiciel renvoie l'état de traitement "**6400**" ou "**6500**".»;

l) au point 3.5.5, le paragraphe TCS_72 est remplacé par le texte suivant:

«TCS_72 Le PIN indiqué par l'utilisateur doit être codé en code ASCII et complété à droite d'une série d'octets "FFh" jusqu'à atteindre une longueur de 8 octets, par l'IFD; cf. le type de données WorkshopCardPIN en appendice 1.»;

m) au point 3.5.8, le paragraphe TCS_95 est remplacé par le texte suivant:

«TCS_95 Si la commande INTERNAL AUTHENTICATE aboutit, la clé de session active de génération 1, pour autant qu'elle existe, est effacée et cesse d'être disponible. Pour disposer d'une nouvelle clé de session de génération 1, il convient d'exécuter avec succès la commande EXTERNAL AUTHENTICATE pour le mécanisme d'authentification de génération 1.

Remarque: Pour les clés de session de génération 2, voir l'appendice 11, paragraphes CSM_193 et CSM_195. Si les clés de session de génération 2 sont établies et que la carte tachygraphique reçoit la commande INTERNAL AUTHENTICATE en clair APDU, elle abandonne la session de messagerie sécurisée de génération 2 et détruit les clés de session de génération 2.»;

n) au point 3.5.9, le paragraphe TCS_97 est remplacé par le texte suivant:

«TCS_97 La variante de la commande pour l'authentification mutuelle de la carte VU de deuxième génération est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. également TCS_34. Si cette commande EXTERNAL AUTHENTICATE de génération 2 aboutit, la clé de session active de génération 1, pour autant qu'elle existe, est effacée et cesse d'être disponible.

Remarque: Pour les clés de session de génération 2, voir l'appendice 11, paragraphes CSM_193 et CSM_195. Si les clés de session de génération 2 sont établies et que la carte tachygraphique reçoit la commande EXTERNAL AUTHENTICATE en clair APDU, elle abandonne la session de messagerie sécurisée de génération 2 et détruit les clés de session de génération 2.»;

o) au point 3.5.10, la ligne suivante est ajoutée au tableau du paragraphe TCS_101:

«5 + L + 1	1	"00h"	Conformément à la norme ISO/IEC 7816-4»

p) au point 3.5.11.2.3, les paragraphes suivants sont ajoutés au paragraphe TCS_114:

«— Si le currentAuthenticatedTime de la carte est ultérieur à la date d'expiration de la clé publique sélectionnée, le logiciel renvoie l'état de traitement "**6A88**".

Remarque: En cas de MSE: SET AT pour authentification de VU, la clé mentionnée est une clé publique VU_MA. La carte définit la clé publique VU_MA pour utilisation, si elle est disponible dans sa mémoire, correspondant à la référence du titulaire du certificat (CHR) indiquée dans la zone de données de la commande (la carte peut identifier les clés publiques VU_MA au moyen du champ CHA du certificat). Une carte ne renvoie "6A 88" à cette commande que lorsque seule la clé publique VU_Sign est disponible ou lorsqu'aucune clé publique de l'unité embarquée sur véhicule n'est disponible. Voir la définition du champ CHA à l'appendice 11 et la définition du type de données EquipmentType à l'appendice 1.

De même, en cas de commande MSE: SET DST indiquant un EQT (une VU ou une carte) est envoyée à une carte de contrôle, aux termes du paragraphe CSM_234, la clé mentionnée est toujours une clé EQT_Sign à utiliser lors de la vérification d'une signature numérique. Selon la figure 13 de l'appendice 11, la carte de contrôle enregistre toujours la clé publique EQT_Sign pertinente. Dans certains cas, la carte de contrôle peut avoir enregistré la clé publique EQT_MA correspondante. La carte de contrôle définit toujours la clé publique EQT_Sign pour utilisation lorsqu'elle reçoit une commande MSE: SET DST.»;

q) le point 3.5.13 est modifié comme suit:

(i) le paragraphe TCS_121 est remplacé par le texte suivant:

«TCS_121 La valeur de hachage du fichier enregistrée temporairement doit être supprimée si une nouvelle valeur de hachage de fichier est calculée à l'aide de la commande PERFORM HASH of FILE, si un DF est sélectionné et si la carte tachygraphique est réinitialisée.»;

ii) le paragraphe TCS_123 est remplacé par le texte suivant:

«TCS_123 L'application tachygraphique de génération 2 doit prendre en charge l'algorithme SHA-2 (SHA-256, SHA-384 ou SHA-512), spécifié par la méthode de cryptage à l'appendice 11, partie B, pour la clé de signature de carte Card_Sign.»;

iii) le tableau figurant au paragraphe TCS_124 est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
CLA	1	"80h"	CLA
INS	1	"2Ah"	Exécution d'une opération de sécurité
P1	1	"90h"	Balise: Hash
P2	1	"00h"	Algorithme implicitement connu Pour l'application tachygraphique de génération 1: SHA-1 Pour l'application tachygraphique de génération 2: l'algorithme SHA-2 (SHA-256, SHA-384 ou SHA-512), défini par la méthode de cryptage à l'appendice 11, partie B, pour la clé de signature de carte Card_Sign»

r) le point 3.5.14 est modifié comme suit:

le texte suivant l'intitulé, jusqu'au paragraphe TCS_126, est remplacé par le texte suivant:

«Cette commande permet de calculer la signature numérique du code de hachage préalablement calculé (cf. commande PERFORM HASH of FILE, paragraphe 3.5.13).

Seules les cartes de conducteur et d'atelier doivent prendre en charge cette commande dans le DF Tachograph et le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non exécuter cette commande. Pour l'application tachygraphique de génération 2, seule la carte du conducteur et la carte d'atelier possèdent une clé de signature de génération 2; les autres cartes ne peuvent pas exécuter cette commande, mais l'abandonnent avec un code d'erreur approprié.

La commande peut ou non être accessible dans le MF. Si la commande n'est pas accessible dans le MF, le logiciel doit interrompre la commande avec un code d'erreur adapté.

Cette commande est conforme à la norme ISO/IEC 7816-8. Son usage est restreint relativement à la norme en question.»;

s) le point 3.5.15 est modifié comme suit:

i) le tableau figurant au paragraphe TCS_133 est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
CLA	1	"00h"	CLA
INS	1	"2Ah"	Exécution d'une opération de sécurité
P1	1	"00h"	
P2	1	"A8h"	Balise: zone de données contenant les DO pertinents pour la vérification
Lc	1	"XXh"	Longueur Lc de la zone de données suivante
#6	1	"9Eh"	Balise indiquant une signature numérique
#7 ou #7-#8	L	"NNh" ou "81 NNh"	Longueur de la signature numérique (L équivaut à 2 octets si la signature numérique est plus longue que 127 octets): 128 octets codés conformément à l'appendice 11 partie A pour l'application tachygraphique de génération 1. Selon la courbe retenue pour l'application tachygraphique de génération 2 (cf. appendice 11 partie B).
#(7+L)-#(6+L+NN)	NN	"XX..XXh"	Contenu de la signature numérique»

ii) au paragraphe TCS_134, le tiret suivant est ajouté:

«— Si la clé publique sélectionnée (utilisée pour vérifier la signature numérique) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) inadapté à la vérification de la signature numérique telle que prévue par l'appendice 11, le logiciel renvoie l'état de traitement "**6985**".»;

t) le point 3.5.16 est modifié comme suit:

i) au paragraphe TCS_138, la ligne suivante est ajoutée au tableau:

«5 + L + 1	1	"00h"	Conformément à la norme ISO/IEC 7816-4»

ii) l'alinéa suivant est ajouté au paragraphe TCS_139:

«— "**6985**" indique que le timbre horodateur sur 4 octets indiqué dans la zone de données de la commande est antérieur à cardValidityBegin ou postérieur à cardExpiryDate.»;

u) le point 4.2.2 est modifié comme suit:

i) dans la structure de données du paragraphe TCS_154, les lignes allant de DF Tachograph G2 à EF CardMA_Certificate et de EF GNSS_Places à la fin du paragraphe sont remplacées par le texte suivant:

«

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*20268*	*40316*	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*17*	*17*	
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		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
GNSSContinuousDriving		*4538*	*6050*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n_8	*18*	*18*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»;

ii) au paragraphe TCS_155, l'élément NoOfGNSSCDRecords du tableau est remplacé par l'élément suivant:

«n_8	NoOfGNSSADRecords	252	336»

v) au point 4.3.1, le texte correspondant à l'abréviation SC4 au paragraphe TCS_156 est remplacé par le texte suivant:

«**SC4** Concernant la commande READ BINARY avec des octets pairs INS:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OU

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Pour la commande READ BINARY avec octet impair INS (si pris en charge): NEV»;

w) le point 4.3.2 est modifié comme suit:

i) dans la structure de données du paragraphe TCS_162, les lignes allant de DF Tachograph G2 à EF CardMA_Certificate, de EF Calibration à extendedSealIdentifier et de EF GNSS_Places à vehicleOdometerValue sont remplacées par le texte suivant:

«

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
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	2		2	{00 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
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}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»

ii) l'élément NoOfGNSSCDRecords du tableau inclus au paragraphe TCS_163 est remplacé par l'élément suivant:

«n_8	NoOfGNSSADRecords	18	24»

31) dans l'appendice 3, le point 2 est modifié comme suit:

a) la ligne suivante est insérée après la ligne incluant les pictogrammes «Site de début de la période de travail journalière» et «Site de fin de la période de travail journalière»:

«  Position après trois heures de temps de conduite accumulé»;

b) la combinaison de pictogrammes «Réglage de l'heure (en atelier)» est remplacée par la combinaison suivante:

«  Conflit temporel ou réglage de l'heure (en atelier)»;

c) les combinaisons de pictogrammes suivantes sont ajoutées à la liste des événements:

«  Absence d'informations de positionnement en provenance du récepteur GNSS ou Erreur de communication avec le dispositif GNSS externe;

 Erreur de communication avec le dispositif de communication à distance»;

32) l'appendice 4 est modifié comme suit:

a) le point 2 est modifié comme suit:

i) le numéro de bloc 11.4 est remplacé par le numéro suivant:

«11.4 *Saisie du lieu de début et/ou de fin d'une période de travail journalière*

pi = pictogramme du lieu de départ/d'arrivée, heure, pays, région	pihh:mm Cou Reg
longitude de la position enregistrée	lon ±DDD°MM.M'
latitude de la position enregistrée	lat ± DD°MM.M'
horodatage de la détermination de la position	hh:mm
Compteur kilométrique	x xxx xxx **km**»

ii) le numéro de bloc 11.5 est remplacé par le numéro suivant:

«11.5 *Positions après trois heures de temps de conduite accumulé*
pi=position après trois heures de temps de conduite accumulé

heure	pihh:mm
longitude de la position enregistrée	lon ± DDD°MM.M'
latitude de la position enregistrée	lat ± DD°MM.M '
horodatage de la détermination de la position	hh:mm
Compteur kilométrique	x xxx xxx **km**»

b) au point 3.1, la position 11.5 du format du tirage quotidien est remplacée par ce qui suit:

«11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique»

c) au point 3.2, le format du tirage quotidien est remplacé comme suit:

«1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans la VU + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
5	Identification de la VU (à partir de laquelle le tirage est exécuté + GEN)
6	Dernier étalonnage de cette VU
7	Dernier contrôle auquel ce tachygraphe a été soumis
9	Délimiteur des activités du conducteur
10	Délimiteur de lecteur de carte du conducteur (lecteur 1)
10a	Condition hors champ au début de cette journée
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activités par ordre chronologique (lecteur conducteur)
10	Délimiteur de lecteur de carte du convoyeur (lecteur 2)
10a	Condition hors champ au début de cette journée
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activités par ordre chronologique (lecteur convoyeur)
11	Délimiteur de synthèse quotidienne
11.1	Synthèse des périodes sans carte dans le lecteur du conducteur
11.4	Lieux saisis par ordre chronologique
11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique
11.7	Totaux par activité
11.2	Synthèse des périodes sans carte dans le lecteur du convoyeur
11.4	Lieux saisis par ordre chronologique
11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique

11.8	Totaux par activité
11.3	Synthèse des activités par conducteur, les deux lecteurs étant inclus
11.4	Lieux saisis par ce conducteur, par ordre chronologique
11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique
11.9	Totaux par activité pour ce conducteur
13.1	Délimiteur d'événements et d'anomalies
13.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans la VU)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.3	De (heure)
22.4	À (heure) (espace disponible pour un conducteur dépourvu de carte lui permettant d'indiquer les périodes qui correspondent à ses prestations)
22.5	Signature du conducteur»

d) au point 3.7, le paragraphe PRT_014 est remplacé par le texte suivant:

«PRT_014 Le tirage de l'historique des cartes insérées doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identifications du titulaire de la carte (pour toutes les cartes insérées dans la VU)
23	Cartes les plus récentes insérées dans la VU
23.1	Cartes insérées (jusqu'à 88 enregistrements)
12.3	Délimiteur des anomalies»

33) l'appendice 7 est modifié comme suit:

a) le point 1.1 est remplacé par le texte suivant:

«1.1. **Champ d'application**

Certaines données sont susceptibles d'être téléchargées vers un support de mémoire externe (ESM):

— à partir d'une unité embarquée sur véhicule (VU) par l'intermédiaire d'un équipement spécialisé intelligent (IDE) raccordé à la VU,

— à partir d'une carte tachygraphique par l'intermédiaire d'un IDE équipé d'un périphérique de lecture de carte (IFD),

— à partir d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur véhicule et par le biais d'un IDE raccordé à la VU.

Afin de permettre la vérification de l'authenticité et de l'intégrité des données téléchargées qui auraient été sauvegardées sur un ESM, ces données s'accompagnent d'une signature conforme à l'appendice 11 (Mécanismes de sécurité communs). L'identification de l'équipement source (VU ou carte) et ses certificats de sécurité (État membre et équipement) sont également téléchargés. Le vérificateur doit être en possession d'une clé publique européenne sécurisée.

Les données téléchargées à partir d'une VU sont signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B (tachygraphe de deuxième génération), excepté lorsque le contrôle des conducteurs est effectué par des autorités de contrôle autres que celles de l'UE, au moyen d'une carte de contrôle de première génération, auquel cas les données sont signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A (tachygraphe de première génération), conformément à l'appendice 15 Migration, exigence MIG_015.

Cet appendice spécifie dès lors deux types de téléchargements de données à partir de la VU:

— téléchargement de données de la VU de génération 2, fournissant la structure de données de génération 2 et signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B,

— téléchargement de données de la VU de génération 1, fournissant la structure de données de génération 1 et signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A,

De même, on distingue deux types de téléchargements de données à partir de cartes de conducteur de deuxième génération insérées dans une VU, comme indiqué aux paragraphes 3 et 4 du présent appendice.»;

b) le point 2.2.2 est modifié comme suit:

i) le tableau est remplacé par le tableau suivant:

«Structure du message	4 octets max. En-tête				255 octets max. Données			1 octet Total de contrôle
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DONNÉES	CS
Demande d'établissement de la communication	81	EE	F0		81			E0
Réponse positive à une demande d'établissement de la communication	80	F0	EE	03	C1		EA, 8F	9B
Demande d'ouverture d'une session de diagnostic	80	EE	F0	02	10	81		F1
Réponse positive à une demande d'ouverture de session de diagnostic	80	F0	EE	02	50	81		31
Service de contrôle de liaison Vérification du débit en bauds (étape 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
Réponse positive à une demande de vérification du débit en bauds	80	F0	EE	02	C7		01	28
Débit de transition en bauds (étape 2)	80	EE	F0	03	87		02.03	ED
Demande de téléchargement (upload)	80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99
Réponse positive à une demande de téléchargement	80	F0	EE	03	75		00,FF	D5
Demande de transfert de données								
Récapitulatif	80	EE	F0	02	36	01 ou 21		97
Activités	80	EE	F0	06	36	02 ou 22	Date	CS
Événements et anomalies	80	EE	F0	02	36	03 ou 23		99
Vitesse instantanée	80	EE	F0	02	36	04 ou 24		9A
Données techniques	80	EE	F0	02	36	05 ou 25		9B
Téléchargement (download) d'une carte	80	EE	F0	02	36	06	Lecteur	CS

Structure du message	4 octets max. En-tête				255 octets max. Données			1 octet Total de contrôle
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DONNÉES	CS
Réponse positive à une demande de transfert de données	80	F0	EE	Len	76	TREP	Données	CS
Demande de fin de transfert	80	EE	F0	01	37			96
Réponse positive à une demande de fin de transfert	80	F0	EE	01	77			D6
Demande d'arrêt de la communication	80	EE	F0	01	82			E1
Réponse positive à une demande d'arrêt de la communication	80	F0	EE	01	C2			21
Accusé de réception d'un sous-message	80	EE	F0	Len	83		Données	CS
Réponses négatives								
Téléchargement (général) refusé	80	F0	EE	03	7F	Sid Req	10	CS
Service incompatible	80	F0	EE	03	7F	Sid Req	11	CS
Sous-fonction incompatible	80	F0	EE	03	7F	Sid Req	12	CS
Longueur du message incorrecte	80	F0	EE	03	7F	Sid Req	13	CS
Conditions non correctes ou erreur affectant la séquence d'interrogation	80	F0	EE	03	7F	Sid Req	22	CS
Demande excessive	80	F0	EE	03	7F	Sid Req	31	CS
Téléchargement (upload) refusé	80	F0	EE	03	7F	Sid Req	50	CS
Réponse en suspens	80	F0	EE	03	7F	Sid Req	78	CS
Données indisponibles	80	F0	EE	03	7F	Sid Req	FA	CS»

ii) les tirets suivants sont ajoutés aux remarques suivant le tableau:

«— Les TRTP 21 à 25 sont utilisés pour les demandes de téléchargement de données de la VU de génération 2, les TRTP 01 à 05 sont utilisés pour les demandes de téléchargement de données de la VU de génération 1, qui ne peuvent être acceptées par la VU que dans le cadre des contrôles des conducteurs effectués par des autorités de contrôle autres que celles de l'UE, au moyen d'une carte de contrôle de première génération.

— Les TRTP 11 à 19 et 31 à 39 sont réservés aux demandes de téléchargement propres au fabricant.»;

c) le point 2.2.2.9 est modifié comme suit:

i) le paragraphe DDP_011 est remplacé par le texte suivant:

«DDP_011 L'IDE émet une demande de transfert de données afin de préciser à la VU la nature des données à télécharger. Un paramètre de demande de transfert (TRTP) d'un octet indique de quel type de transfert il s'agit.

Il existe six types de transfert de données. Pour les téléchargements de données de la VU, deux différentes valeurs TRTP peuvent être utilisées pour chaque type de transfert:

Type de transfert de données	Valeur de TRTP pour les téléchargements de données de la VU de génération 1	Valeur de TRTP pour les téléchargements de données de la VU de génération 2
Récapitulatif	01	21
Activités associées à une date précise	02	22
Événements et anomalies	03	23
Vitesse instantanée	04	24
Données techniques	05	25

Type de transfert de données	Valeur de TRTP
Téléchargement de carte	06»

ii) le paragraphe DDP_054 est remplacé par le texte suivant:

«DDP_054 Il est obligatoire pour l'IDE de demander un transfert de données du type "récapitulatif" (TRTP 01 ou 21) au cours d'une session de téléchargement, car cela seul garantit que les certificats de la VU sont enregistrés sur le fichier téléchargé (et permet ainsi la vérification de la signature numérique).

Dans le deuxième cas de figure (TRTP 02 ou 22), le message de demande de transfert de données comporte l'indication du jour civil (format `TimeReal`) auquel le téléchargement est associé.»;

d) au point 2.2.2.10, le paragraphe DDP_055 est remplacé par le texte suivant:

«DDP_055 Dans le premier cas (TREP 01 ou 21), la VU enverra des données destinées à aider l'opérateur de l'IDE dans le choix des données qu'ils souhaitent télécharger. Les informations contenues dans ce message sont les suivantes:

— Certificats de sécurité,

— Identification du véhicule,

— Date et heure actuelles sur la VU,

— Date la plus précoce et la plus tardive pour le téléchargement (données de la VU),

— Indications concernant la présence de cartes dans la VU,

— Téléchargements antérieurs vers une entreprise,

— Verrouillages d'entreprise,

— Contrôles précédents.»;

e) au point 2.2.2.16, le paragraphe DDP_018, dernier tiret, est remplacé par le texte suivant:

«— FA données indisponibles

L'objet d'une demande de transfert de données n'est pas accessible au sein de la VU (p. ex. absence d'insertion de carte, téléchargement de données de la VU de génération 1 demandé en dehors du cadre du contrôle d'un conducteur par une autorité de contrôle autre qu'une autorité de contrôle de l'UE, etc.).»;

f) le point 2.2.6.1 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_029 est remplacé par le texte suivant:

«Le champ de données du message "Réponse positive à un récapitulatif de transfert de données" doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 01 ou 21 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 01 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 21 Hex)»;

g) le point 2.2.6.2 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_030 est remplacé par le texte suivant:

«Le champ de données du message "Réponse positive à une demande de transfert de données relatives aux activités" doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 02 ou 22 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 02 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 22 Hex)»;

iv) l'élément VuGNSSCDRecordArray sous l'intitulé «Structure de données de génération 2 (TREP 22 Hex)» est remplacé comme suit:

«VuGNSSADRecordArray	Positions GNSS du véhicule lorsque le temps de conduite accumulé du véhicule atteint un multiple de trois heures. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.»

h) le point 2.2.6.3 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_031 est remplacé par le texte suivant:

«Le champ de données du message "Réponse positive à une demande de transfert de données relatives aux événements et anomalies" doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 03 ou 23 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 03 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 23 Hex)»;

iv) l'élément VuTimeAdjustmentGNSSRecordArray sous le titre «Structure de données de génération 2 (TREP 23 Hex)» est supprimé;

i) le point 2.2.6.4 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_032 est remplacé par le texte suivant:

«Le champ de données du message "Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule" doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 04 ou 24 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 04)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 24)»;

j) le point 2.2.6.5 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_033 est remplacé par le texte suivant:

«Le champ de données du message "Réponse positive à une demande de transfert de données techniques" doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 05 ou 25 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 05)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 25)»;

k) au point 3.3, le paragraphe DDP_035 est remplacé par le texte suivant:

«DDP_035 Le téléchargement d'une carte tachygraphique comporte les opérations suivantes:

— Téléchargement des informations communes que contient la carte dans les EF (fichiers élémentaires) ICC et IC. Ces informations à caractère facultatif ne sont protégées par aucune signature numérique.

— (pour les cartes tachygraphiques de première et deuxième générations) Téléchargement des EF dans le fichier spécialisé Tachograph DF:

— Téléchargement des EF Card_Certificate et CA_Certificate. Ces informations ne sont protégées par aucune signature numérique.

Il faut impérativement télécharger ces fichiers lors de toute session de téléchargement.

— Téléchargement des autres EF de données d'application (dans le Tachograph DF) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique, conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A.

— Il y a lieu de télécharger au moins les Application_Identification et Identification lors de toute session de téléchargement.

— Lors du téléchargement d'une carte de conducteur, il faut également procéder obligatoirement au téléchargement des EF suivants:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— (pour les cartes tachygraphiques de deuxième génération uniquement) Excepté lorsque le téléchargement d'une carte de conducteur insérée dans une VU est effectué durant le contrôle des conducteurs par une autorité de contrôle autre qu'une autorité de contrôle de l'UE, au moyen d'une carte de contrôle de première génération, télécharger les EF dans le Tachograph_G2 DF:

— Télécharger les EF CardSignCertificate, CA_Certificate et Link_Certificate (le cas échéant). Ces informations ne sont protégées par aucune signature numérique.

Il faut impérativement télécharger ces fichiers lors de toute session de téléchargement.

— Téléchargement des autres EF de données d'application (dans le Tachograph_G2 DF) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique, conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B.

— Il y a lieu de télécharger au moins les Application_Identification et Identification lors de toute session de téléchargement.

— Lors du téléchargement d'une carte de conducteur, il faut également procéder obligatoirement au téléchargement des EF suivants:

— Events_Data,

— Faults_Data,

— Driver_Activity_Data,

— Vehicles_Used,

— Places,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Lors du téléchargement d'une carte de conducteur, il convient de mettre à jour la date LastCardDownload dans l'EF Card_Download, dans les DF Tachograph et, le cas échéant, Tachograph_G2 .

— Lors du téléchargement d'une carte d'atelier, il convient de réinitialiser le compteur d'étalonnage enregistré dans l'EF Card_Download dans les DF Tachograph et, le cas échéant, Tachograph_G2 .

— Lors du téléchargement d'une carte d'atelier, l'EF `Sensor_Installation_Data` dans les DF `Tachograph` et, le cas échéant, `Tachograph_G2` n'est pas téléchargé.»;

l) au point 3.3.2, le premier alinéa du paragraphe DDP_037 est remplacé par le texte suivant:

«La séquence du téléchargement des EF ICC, IC, Card_Certificate (ou CardSignCertificate pour le DF Tachograph_G2), CA_Certificate et Link_Certificate (pour le DF Tachograph_G2 uniquement) est la suivante:»;

m) au point 3.3.3, le tableau est remplacé comme suit:

«Carte	Dir	IDE/IFD	Signification/Remarques
	⇦	**Select File**	
OK	⇨		
	⇦	**Procéder au hachage du fichier (Hash of File)**	— Permet de calculer la valeur de hachage par rapport au contenu du fichier sélectionné en appliquant l'algorithme de hachage prescrit en conformité avec l'appendice 11, partie A ou B. Cette commande n'est pas une commande ISO.
Calculer le hachage du fichier et enregistrer temporairement la valeur de hachage retenue			
OK	⇨		
	⇦	**Read Binary**	Si le fichier contient plus de données que le tampon ou la carte ne peut en contenir, la commande doit être réitérée jusqu'à ce que les données que contient ce fichier aient été extraites dans leur intégralité.
Données OK	⇨	Sauvegarder les données sur l'ESM	conformément à **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature**	
Exécution opération de sécurité "Calcul de la signature numérique" à l'aide de la valeur de hachage temporairement enregistrée			
Signature OK	⇨	Adjonction de données à celles préalablement sauvegardées sur l'ESM	conformément à **3.4** Data storage format»

n) au point 3.4.2, le paragraphe DDP_046 est remplacé par le texte suivant:

«DDP_046 Toute signature doit être sauvegardée sous forme d'objet TLV immédiatement après l'objet TLV qui contient les données que recèle le fichier concerné.

Définition	Signification	Longueur
FDI (2 octets) || "00"	Balise pour EF (FDI) dans le Tachograph ou pour les informations communes que contient la carte	3 octets
FDI (2 octets) || "01"	Balise pour signature d'EF (FDI) dans le DF Tachograph	3 octets
FDI (2 octets) || "02"	Balise pour EF (FDI) dans le DF Tachograph_G2	3 octets
FDI (2 octets) || "03"	Balise pour signature d'EF (FDI) dans le DF Tachograph_G2	3 octets
xx xx	Longueur du champ valeur	2 octets

Exemple de données enregistrées dans un fichier de téléchargement sur un ESM:

Balise	Longueur	Valeur
00 02 00	00 11	— Données de l'EF ICC
C1 00 00	00 C2	— Données de l'EF Card_Certificate
		— ...
05 05 00	0A 2E	Données de l'EF Vehicles_Used (dans le DF Tachograph)
05 05 01	00 80	Signature de l'EF Vehicles_Used (dans le DF Tachograph)
05 05 02	0A 2E	Données de l'EF Vehicles_Used (dans le DF Tachograph_G2)
05 05 03	xx xx	Signature de l'EF Vehicles_Used (dans le DF Tachograph_G2)»

o) au point 4, le paragraphe DDP_049 est remplacé par le texte suivant:

«DDP_049 Cartes de conducteur de première génération: Les données doivent être téléchargées selon le protocole de téléchargement de données de première génération. Les données téléchargées auront le même format que les données téléchargées depuis une unité embarquée sur un véhicule de première génération.

Cartes de conducteur de deuxième génération: À ce stade, la VU doit procéder au téléchargement de la carte dans son intégralité, fichier par fichier, en conformité avec le protocole de téléchargement de carte défini au paragraphe 3 ainsi qu'à l'envoi à l'IDE de toutes les données extraites de la carte dans le format de fichier TLV approprié (cf. 3.4.2) et encapsulées dans un message "Réponse positive à une demande de transfert de données".»;

34) au point 2 de l'appendice 8, le paragraphe suivant l'intitulé «Références» est remplacé par le texte suivant:

«ISO 14230-2: Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 2: Couche de liaison de données.

Première édition: 1999.»;

35) l'appendice 9 est modifié comme suit:

a) dans la table des matières, le point 6 est remplacé par le texte suivant:

«6. ESSAIS DES ÉQUIPEMENTS EXTERNES DE COMMUNICATION À DISTANCE»;

b) au point 1.1, le premier tiret est remplacé par le texte suivant:

«— une **certification de sécurité** basée sur des spécifications de critères communs contre une cible de sécurité parfaitement conforme à l'appendice 10 de la présente annexe,»;

c) au point 2, le tableau des essais fonctionnels de l'unité embarquée sur le véhicule est remplacé par ce qui suit:

«N°	Essai	Description	Exigences connexes
1	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
1.2	Résultats des essais menés par le fabricant	Résultats des essais menés par le fabricant pendant la phase d'intégration. Démonstrations sur papier.	88, 89,91
2	**Inspection visuelle**		
2.1	Conformité avec la documentation		
2.2	Identification/marquage		224 à 226
2.3	Matériaux		219 à 223
2.4	Scellements		398, 401 à 405
2.5	Interfaces externes		
3	**Essais de fonctionnement**		
3.1	Fonctions prévues		02, 03, 04, 05, 07, 382
3.2	Modes d'exploitation		09 à 11*, 134, 135
3.3	Droits d'accès aux fonctions et données		12* 13*, 382, 383, 386 à 389
3.4	Surveillance de l'insertion et du retrait des cartes		15, 16, 17, 18, 19*, 20*, 134
3.5	Mesure de la vitesse et de la distance		21 à 31
3.6	Chronométrage (essai exécuté à 20 °C)		38 à 43
3.7	Surveillance des activités du conducteur		44 à 53, 134
3.8	Surveillance de l'état de conduite		54, 55, 134
3.9	Entrées manuelles		56 à 62
3.10	Gestion des dispositifs de verrouillage de l'entreprise		63 à 68
3.11	Suivi des activités de contrôle		69, 70
3.12	Détection d'événements et/ou d'anomalies		71 à 88, 134

N°	Essai	Description	Exigences connexes
3.13	Données d'identification des équipements		93*, 94*, 97, 100
3.14	Données d'insertion et de retrait de la carte du conducteur		102* à 104*
3.15	Données relatives aux activités du conducteur		105* à 107*
3.16	Données relatives aux lieux et aux emplacements		108* à 112*
3.17	Données relatives aux kilométrages		113* à 115*
3.18	Données détaillées relatives à la vitesse		116*
3.19	Données relatives aux événements		117*
3.20	Données relatives aux anomalies		118*
3.21	Données d'étalonnage		119* à 121*
3.22	Données de réglage de l'heure		124*, 125*
3.23	Données relatives aux activités de contrôle		126*, 127*
3.24	Données relatives aux dispositifs de verrouillage de l'entreprise		128*
3.25	Téléchargement de données relatives aux activités		129*
3.26	Données relatives aux conditions particulières		130*, 131*
3.27	Enregistrement et mémorisation sur les cartes tachygraphiques		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Affichage		90, 134, 151 à 168, PIC_001, DIS_001
3.29	Impression		90, 134, 169 à 181, PIC_001, PRT_001 à PRT_014
3.30	Avertissement		134, 182 à 191, PIC_001
3.31	Téléchargement de données à destination de supports externes		90, 134, 192 à 196
3.32	Communication à distance pour les contrôles routiers ciblés		197 à 199
3.33	Données de sortie à destination de dispositifs externes supplémentaires		200, 201
3.34	Étalonnage		202 à 206*, 383, 384, 386 à 391
3.35	Contrôles routiers d'étalonnage		207 à 209
3.36	Réglage de l'heure		210 à 212*
3.37	Absence d'interférence des fonctions supplémentaires		06, 425

N°	Essai	Description	Exigences connexes
3.38	Interface des capteurs de mouvement		02, 122
3.39	Dispositif GNSS externe		03, 123
3.40	Vérifier que la VU détecte, enregistre et stocke les événements et/ou anomalies défini(e)s par le fabricant de la VU lorsqu'un capteur de mouvement couplé réagit à des champs magnétiques qui perturbent la détection des mouvements du véhicule.		217
3.41	Suite de chiffrement et paramètres de domaines normalisés		CSM_48, CSM_50
4	**Essais environnementaux**		
4.1	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: Essai conforme à la norme ISO 16750-4, Chapitre 5.1.1.2: Essai d'exploitation à basse température (72 h à – 20 °C) Cet essai satisfait à la norme CEI 60068-2-1: Essais d'environnement — Partie 2-1: essais - essai A: froid Essai conforme à la norme ISO 16750-4: Chapitre 5.1.2.2: Essai d'exploitation à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai environnemental de base; partie 2: essais; essais B: chaleur sèche Essai conforme à la norme ISO 16750-4: Chapitre 5.3.2: Variation rapide de température avec durée de transition spécifiée (– 20 °C/70 °C, 20 cycles, temps de maintien de 2 h à chaque température). Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Humidité	S'assurer que l'unité embarquée sur le véhicule est capable de résister à un cycle de chaleur humide (essai de résistance à la chaleur) en exécutant l'essai CEI 60068-2-30, essai Db, comportant six cycles de 24 heures, la température variant de + 25 °C à + 55 °C et le taux d'humidité relative atteignant 97 % à + 25 °C et 93 % à + 55 °C.	214
4.3	Mécanique	1. Vibrations sinusoïdales. S'assurer que l'unité embarquée sur le véhicule est capable de résister à des vibrations sinusoïdales possédant les caractéristiques suivantes: déplacement constant compris entre 5 et 11 Hz: 10 mm max; accélération constante comprise entre 11 et 300 Hz: 5 g L'essai CEI 60068-2-6, essai Fc, permet de vérifier la satisfaction de cette exigence. La durée minimale de cet essai s'élève à 3 × 12 heures (12 heures par essieu). La norme ISO 16750-3 n'impose pas d'essai de vibrations sinusoïdales aux dispositifs situés dans la cabine découplée du véhicule.	219

N°	Essai	Description	Exigences connexes
		2. Vibrations aléatoires: Essai conforme à la norme ISO 16750-3: Chapitre 4.1.2.8: Essai VIII: Véhicule commercial, cabine de véhicule découplée. Essai de vibrations aléatoires, 10...2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS latéral 13,1 m/s^2, 3 essieux, 32 h par essieu, y compris un cycle de température – 20...70 °C. Cet essai satisfait à la norme CEI 60068-2-64: Essais d'environnement — Partie 2-64: Essais — Essai Fh: Vibrations aléatoires à large bande et guide 3. Chocs: choc mécanique d'un demi-sinus de 3 g conformément à la norme ISO 16750. Il convient d'exécuter les essais décrits ci-avant sur des échantillons distincts du type d'équipement testé.	
4.4	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653: Véhicules routiers - Degrés de protection (codes IP) - Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (paramètres inchangés); valeur minimale IP 40	220, 221
4.5	Protection contre les surtensions	S'assurer que l'unité embarquée sur le véhicule est capable de supporter une tension d'alimentation de: versions 24 V: 34 V à +40 °C 1 heure versions 12 V: 17 V à + 40 °C 1 heure(ISO 16750-2)	216
4.6	Protection contre les inversions de polarité	S'assurer que l'unité embarquée sur le véhicule est capable de supporter une inversion de polarité au niveau de son alimentation électrique (ISO 16750-2)	216
4.7	Protection contre les courts-circuits	S'assurer que les signaux d'entrée et de sortie sont protégés contre les courts-circuits à l'alimentation électrique et à la terre (ISO 16750-2)	216
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique: 2010 + AMD1:2014: +/- 4 kV pour le contact et +/- 8 kV pour la décharge d'air	218

N°	Essai	Description	Exigences connexes
5.3	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 3: impulsion 1a: Vs = – 450 V Ri = 50 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +20V Ri = 0,05 ohms impulsion 3a: Vs = – 150V Ri = 50 ohms impulsion 3b: Vs = +150V Ri = 50 ohms impulsion 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulsion 5: Vs = + 120 V, Ri = 2,2 ohms, td = 250 ms Pour les versions 12V: conformité avec la norme ISO 7637-1 + Règlement CEE n° 10 Rév. 3: impulsion 1: Vs = –+75V Ri = 10 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +10V Ri = 0,05 ohms impulsion 3a: Vs = – 112V Ri = 50 ohms impulsion 3b: Vs = +75V Ri = 50 ohms impulsion 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulsion 5: Vs = + 65 V, Ri = 3 ohms, td = 100 ms L'impulsion 5 ne sera testée que pour les unités à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218»

d) le point 6 est remplacé par le texte suivant:

«6. ESSAI DES ÉQUIPEMENTS EXTERNES DE COMMUNICATION À DISTANCE

N°	Essai	Description	Exigences connexes
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle**		
2.1.	Conformité avec la documentation		
2.2.	Identification/marquage		225, 226
2.3	Matériaux		219 à 223
3.	**Essais de fonctionnement**		
3.1	Communication à distance pour les contrôles routiers ciblés		4, 197 à 199

N°	Essai	Description	Exigences connexes
3.2	Enregistrement et stockage de données sur la mémoire		91
3.3	Communication avec l'unité embarquée sur le véhicule		Appendice 14, paragraphes DSC_66 à DSC_70, DSC_71 à DSC_76
4.	**Essais environnementaux**		
4.1	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: Essai conforme à la norme ISO 16750-4, Chapitre 5.1.1.2: Essai d'exploitation à basse température (72 h à -20 °C) Cet essai satisfait à la norme CEI 60068-2-1: Essais d'environnement — Partie 2-1: essais - essai A: froid Essai conforme à la norme ISO 16750-4: Chapitre 5.1.2.2: Essai d'exploitation à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai environnemental de base; partie 2: essais; essais B: chaleur sèche Essai conforme à la norme ISO 16750-4: Chapitre 5.3.2: Variation rapide de température avec durée de transition spécifiée (-20 °C/70 °C, 20 cycles, temps de maintien de 1 h à chaque température) Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653: Véhicules routiers - Degrés de protection (code IP) - Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (valeur ciblée IP 40)	220, 221
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique: 2010 + AMD1:2014: +/- 4 kV pour le contact et +/- 8 kV pour la décharge d'air	218

N°	Essai	Description	Exigences connexes
5.3	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 3: impulsion 1a: Vs = -450 V Ri = 50 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +20V Ri = 0,05 ohms impulsion 3a: Vs = -150V Ri = 50 ohms impulsion 3b: Vs = +150V Ri = 50 ohms impulsion 4: Vs = -16 V Va = -12 V t6 = 100 ms impulsion 5: Vs = + 120 V, Ri = 2,2 ohms, td = 250 ms Pour les versions 12V: conformité avec la norme ISO 7637-1 + Règlement CEE n° 10 Rév. 3: impulsion 1: Vs = -75V Ri = 10 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +10V Ri = 0,05 ohms impulsion 3a: Vs = -112V Ri = 50 ohms impulsion 3b: Vs = +75V Ri = 50 ohms impulsion 4: Vs = -6 V Va = -5 V t6 = 15 ms impulsion 5: Vs = + 65 V, Ri = 3 ohms, td = 100 ms L'impulsion 5 ne sera testée que pour les unités à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218»

e) le tableau du point 8 relatif aux essais d'interopérabilité est remplacé par ce qui suit:

«N°	Essai	Description
	8.1 Essais d'interopérabilité entre unités embarquées sur véhicule et cartes tachygraphiques	
1	Authentification mutuelle	S'assurer de la bonne exécution de la procédure d'authentification mutuelle entre l'unité embarquée sur le véhicule et la carte tachygraphique
2	Essais de lecture/écriture	Mettre à exécution un scénario d'activité classique sur l'unité embarquée sur le véhicule. Le scénario doit être adapté au type de carte testé et comporter l'exécution d'opérations d'écriture dans le plus grand nombre possible d'EF que présente la carte. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants Procéder à des impressions quotidiennes pour s'assurer de la bonne lisibilité des enregistrements correspondants.

N°	Essai	Description
	8.2 Essais d'interopérabilité entre unités embarquées sur véhicule et capteurs de mouvement	
1	Appariement	S'assurer de la bonne exécution de l'appariement entre l'unité embarquée sur le véhicule et le capteur de mouvement
2	Essais d'activité	Exécuter un scénario d'activité classique sur le capteur de mouvement. Le scénario implique une activité normale et la création d'un nombre d'événement et d'anomalies aussi élevé que possible. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants Procéder à une impression quotidienne pour s'assurer de la bonne lisibilité des enregistrements correspondants.
	8.3 Essais d'interopérabilité entre les VU et les dispositifs GNSS externes (le cas échéant)	
1	Authentification mutuelle	S'assurer de la bonne exécution de la procédure d'authentification mutuelle (couplage) entre l'unité embarquée sur le véhicule et le module GNSS externe.
2	Essais d'activité	Exécuter un scénario d'activité classique sur le dispositif GNSS externe. Le scénario implique une activité normale et la création d'un nombre d'événement et d'anomalies aussi élevé que possible. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants Procéder à une impression quotidienne pour s'assurer de la bonne lisibilité des enregistrements correspondants.»

36) l'appendice 11 est modifié comme suit:

a) au point 8.2.3, le paragraphe CSM_49 est remplacé par le texte suivant:

«CSM_49 Les unités embarquées sur véhicule, les cartes tachygraphiques et les dispositifs GNSS externes devront être compatibles avec les algorithmes SHA-256, SHA-384 et SHA-512 définis dans [SHS].»;

b) au point 9.1.2, le premier alinéa du paragraphe CSM_58 est remplacé par le texte suivant:

«CSM_58 Dès lors que l'ERCA génère une nouvelle paire de clés racine européenne, l'organisme crée un nouveau certificat de lien destiné à la nouvelle clé publique européenne et le signe avec la clé privée européenne précédente. La durée de validité d'un certificat de lien est de 17 ans plus trois mois. La figure 1 de la section 9.1.7 l'illustre également.»;

c) au point 9.1.4, le paragraphe CSM_72 est remplacé par le texte suivant:

«CSM_72 Deux paires de clés ECC uniques sont générées pour chaque unité embarquée sur véhicule, appelées VU_MA et VU_Sign. Cette tâche incombe aux fabricants de VU. Dès lors qu'une paire de clés VU est générée, la partie qui la génère doit adresser la clé publique à sa MSCA afin d'obtenir un certificat VU correspondant, signé par la MSCA. La clé privée sert uniquement à une unité embarquée sur véhicule.»

d) le point 9.1.5 est modifié comme suit:

i) le paragraphe CSM_83 est remplacé par le texte suivant:

«CSM_83 Une paire de clés ECC unique appelée Card_MA est générée pour chaque carte tachygraphique. Une deuxième paire de clés ECC unique, appelé Card_Sign, est générée en plus pour chaque carte de conducteur et chaque carte d'atelier. Cette tâche incombe aux fabricants et aux personnalisateurs de cartes. Dès lors qu'une paire de clés pour carte est générée, la partie qui la génère doit adresser la clé publique à sa MSCA afin d'obtenir un certificat pour carte correspondant, signé par la MSCA. La clé privée sert uniquement à la carte tachygraphique.»;

ii) le paragraphe CSM_88 est remplacé par le texte suivant:

«CSM_88 La durée de validité d'un certificat Card_MA est la suivante:

— Pour les cartes de conducteur: 5 ans

— Pour les cartes d'entreprise: 5 ans

— Pour les cartes de contrôle: 2 ans

— Pour les cartes d'atelier: 1 an»;

iii) au paragraphe CSM_91, le texte suivant est ajouté:

«— En outre, uniquement pour les cartes de contrôle, les cartes d'entreprise et les cartes d'atelier et seulement si ces cartes sont émises dans les trois premiers mois de la période de validité d'un nouveau certificat EUR: le certificat EUR plus ancien de deux générations, le cas échéant.

Remarque pour le dernier point: par exemple, au cours des trois premiers mois du certificat ERCA(3) (voir la figure 1), les cartes mentionnées incluent le certificat ERCA(1). L'inclusion du certificat ERCA est nécessaire pour permettre à ces cartes d'effectuer des téléchargements de données à partir des VU d'ERCA(1), dont la durée de vie normale de 15 ans, à laquelle s'ajoute la période de téléchargement des données de trois mois, expire au cours de ces mois; voir le dernier point de l'exigence 13 de l'annexe IC.»;

e) le point 9.1.6 est modifié comme suit:

i) le paragraphe CSM_93 est remplacé par le texte suivant:

«CSM_93 Une paire de clés ECC unique appelée EGF_MA est générée pour chaque dispositif GNSS externe. Cette tâche incombe aux fabricants des dispositifs GNSS externes. Dès lors qu'une paire de clés EGF_MA est générée, la partie qui la génère doit adresser la clé publique à sa MSCA afin d'obtenir un certificat EGF_MA correspondant, signé par la MSCA. La clé privée sert uniquement au dispositif GNSS externe.»;

ii) le paragraphe CSM_95 est remplacé par le texte suivant:

«CSM_95 Un dispositif GNSS externe utilise sa paire de clés EGF_MA, composée d'une clé privée EGF_MA.SK et d'une clé publique EGF_MA.PK, exclusivement pour effectuer des opérations d'authentification mutuelle et de concordance des clés de session avec les VU, comme le prévoit la section 11.4 du présent appendice.»;

f) le point 9.1.7 est modifié comme suit:

i) la figure 1 est remplacée par ce qui suit:

«*Figure 1*

Émission et utilisation de différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et d'équipement

»;

ii) dans les notes relatives à la figure 1, le paragraphe 6 est remplacé par le texte suivant:

«6. Pour gagner de l'espace, la différence entre les durées de validité des certificats Card_MA et des certificats Card_Sign n'est précisée que pour la première génération.»;

g) le point 9.2.1.1 est modifié comme suit:

i) au paragraphe CSM_106, le premier tiret est remplacé par le texte suivant:

«— Pour les clés maîtresses du capteur de mouvement sur 128 bits: CV = "B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83" »;

ii) au paragraphe CSM_107, le premier alinéa est remplacé par le texte suivant:

«Chaque fabricant de capteurs de mouvement génère une clé de couplage aléatoire unique K_P pour chaque capteur de mouvement et communique chaque clé de couplage à l'organisme de certification de son État membre. La MSCA chiffre chaque clé de couplage séparément à l'aide de la clé maîtresse du capteur de mouvement K_M et retourne la clé cryptée au fabricant de capteurs de mouvement. Pour chaque clé cryptée, la MSCA avertit le fabricant de capteurs de mouvement du numéro de version de la K_M associée.»;

iii) le paragraphe CSM_108 est remplacé par le texte suivant:

«CSM_108 Chaque fabricant de capteurs de mouvement génère un numéro de série unique pour chaque capteur de mouvement et communique tous les numéros de série à l'organisme de certification de son État membre. La MSCA chiffre chaque numéro de série séparément à l'aide de la clé d'identification K_{ID} et retourne le numéro de série crypté au fabricant de capteurs de mouvement. Pour chaque numéro de série crypté, la MSCA avertit le fabricant de capteurs de mouvement du numéro de version du K_{ID} associé.»;

h) le point 9.2.2.1 est modifié comme suit:

i) le paragraphe CSM_123 est remplacé par le texte suivant:

«CSM_123 Pour chaque VU, le fabricant de VU crée un numéro de série VU unique qu'il adresse aux organismes de certification de l'État membre en vue d'obtenir un jeu de deux clés DSRC propre aux VU. Le numéro de série VU relève du type de données `VuSerialNumber`.

Remarque:

— Ce numéro de série VU est identique à l'élément vuSerialNumber de VuIdentification (voir l'appendice 1) et à la référence du titulaire de certificat figurant dans les certificats de la VU.

— Le numéro de série de la VU peut ne pas être connu au moment où un fabricant d'unité embarquée sur véhicule demande les clés de DSRC propres à la VU. Dans ce cas, le fabricant de VU envoie l'ID unique de demande de certificat qu'il a utilisé au moment de sa demande de certificats de la VU; cf. CSM_153. Cet ID de demande de certificat est donc identique à la référence des organismes de certification indiquée dans les certificats de la VU.»;

ii) au paragraphe CSM_124, l'exigence en matière d'information à l'étape 2 est remplacée comme suit:

«info = numéro de série VU ou ID de la demande de certificat, comme indiqué au CSM_123»;

iii) le paragraphe CSM_128 est remplacé par le texte suivant:

«CSM_128 La MSCA archive toutes les clés DSRC propres aux VU qu'elle a générées, ainsi que leur numéro de version et le numéro de série VU ou l'ID de la demande de certificat utilisé pour les obtenir.»;

i) au point 9.3.1, le premier alinéa du paragraphe CSM_135 est remplacé par le texte suivant:

«Les règles de codage distinctes (DER) conformes à la norme [ISO 8825-1] servent à encoder les objets de données au sein des certificats. Le tableau 4 présente le codage intégral du certificat, y compris toutes les balises et les longueurs en octets.»;

j) au point 9.3.2.3, le paragraphe CSM_141 est remplacé par le texte suivant:

«CSM_141 L'autorisation du titulaire de certificat permet d'identifier le type de certificat. Elle se compose des six octets principaux de l'ID de l'application tachygraphique concaténée avec le type d'équipement, qui indique le type d'équipement auquel est destiné le certificat. Concernant les certificats VU, les certificats de carte de conducteur et les certificats de carte d'atelier, le type d'équipement est également utilisé pour distinguer les certificats pour l'authentification mutuelle des certificats à utiliser pour la création d'une signature numérique (voir la section 9.1 et l'appendice 1, type de données EquipmentType).»;

k) au point 9.3.2.5, l'alinéa suivant est ajouté au paragraphe CSM_146:

«*Remarque:* pour un certificat de carte, la valeur du CHR est égale à la valeur de l'élément cardExtendedSerialNumber du fichier EF_ICC; voir appendice 2. Pour un certificat EGF, la valeur du CHR est égale à la valeur de l'élément sensorGNSSSerialNumber du fichier EF_ICC; voir appendice 14. Pour un certificat VU, la valeur du CHR est égale à l'élément vuSerialNumber de VuIdentification (voir l'appendice 1), à moins que le fabricant ne connaisse pas le numéro de série propre au fabricant au moment où le certificat est demandé.»;

l) au point 9.3.2.6, le paragraphe CSM_148 est remplacé par le texte suivant:

«CSM_148 La date d'entrée en vigueur du certificat indique la date et l'heure de début de la durée de validité du certificat.»;

m) le point 9.3.3 est modifié comme suit:

i) au paragraphe CSM_151, le premier alinéa est remplacé par le texte suivant:

«Lors de la demande d'un certificat, la MSCA adresse les données suivantes à l'ERCA:»;

ii) le paragraphe CSM_153 est remplacé par le texte suivant:

«CSM_153 Un fabricant d'équipement envoie les données suivantes dans une demande de certificat à une MSCA, ce qui lui permet de créer la référence du titulaire de certificat du nouvel équipement:

— S'il est connu (cf. CSM_154), un numéro de série de l'équipement, propre au fabricant, ainsi que le type d'équipement et le mois de sa fabrication. Sinon, un identificateur unique de demande de certificat.

— Le mois et l'année de fabrication de l'équipement ou de la demande de certificat.

Le fabricant s'assure de l'exactitude de ces données et du fait que le certificat renvoyé par la MSCA est inséré dans l'équipement auquel il est destiné.»;

n) le point 10.2.1 est modifié comme suit:

i) au paragraphe CSM_157, le texte précédant les notes relatives à la figure 4 est remplacé par le texte suivant:

«Les VU adoptent le protocole prévu à la figure 4 pour vérifier la chaîne de certificat d'une carte tachygraphique. Pour chaque certificat lu à partir de la carte, la VU vérifie que le champ "Autorisation du titulaire de certificat" (CHA) est correct:

— Le champ CHA du certificat Card indique un certificat Card pour l'authentification mutuelle (voir l'appendice 1, type de données EquipmentType).

— Le champ CHA du certificat Card.CA indique une MSCA.

— Le champ CHA du certificat Card.Link indique une ERCA.»;

ii) au paragraphe CSM_159, la phrase suivante est ajoutée:

«Si l'enregistrement de tous les autres types de certificats est facultatif, la VU a l'obligation d'enregistrer les nouveaux certificats de lien présentés par une carte.»;

o) le point 10.2.2 est modifié comme suit:

i) au paragraphe CSM_161, le texte précédant la figure 5 est remplacé par le texte suivant:

«Les cartes tachygraphiques adoptent le protocole prévu à la figure 5 pour vérifier la chaîne de certificat d'une VU. Pour chaque certificat présenté par la VU, la carte vérifie que le champ de l'autorisation du titulaire de certificat (CHA) est correct:

— Le champ CHA du certificat VU.Link indique l'ERCA.

— Le champ CHA du certificat VU.CA indique une MSCA.

— Le champ CHA du certificat VU indique un certificat VU pour l'authentification mutuelle (voir l'appendice 1, type de données EquipmentType).»;

ii) le paragraphe CSM_165 est remplacé par le texte suivant:

«CSM_165 Si la commande MSE: Set AT aboutit, la carte définit le VU.PK indiqué pour une utilisation ultérieure pendant l'authentification de la VU et mémorise temporairement Comp(VU.PKeph). Si plusieurs commandes MSE: Set AT aboutissent, elles sont adressées avant de procéder à la concordance des clés de session. La carte mémorise uniquement le dernier Comp(VU.PKeph) reçu. La carte réinitialise Comp(VU.PKeph) après une commande GENERAL AUTHENTICATE réussie.»;

p) le point 10.3 est modifié comme suit:

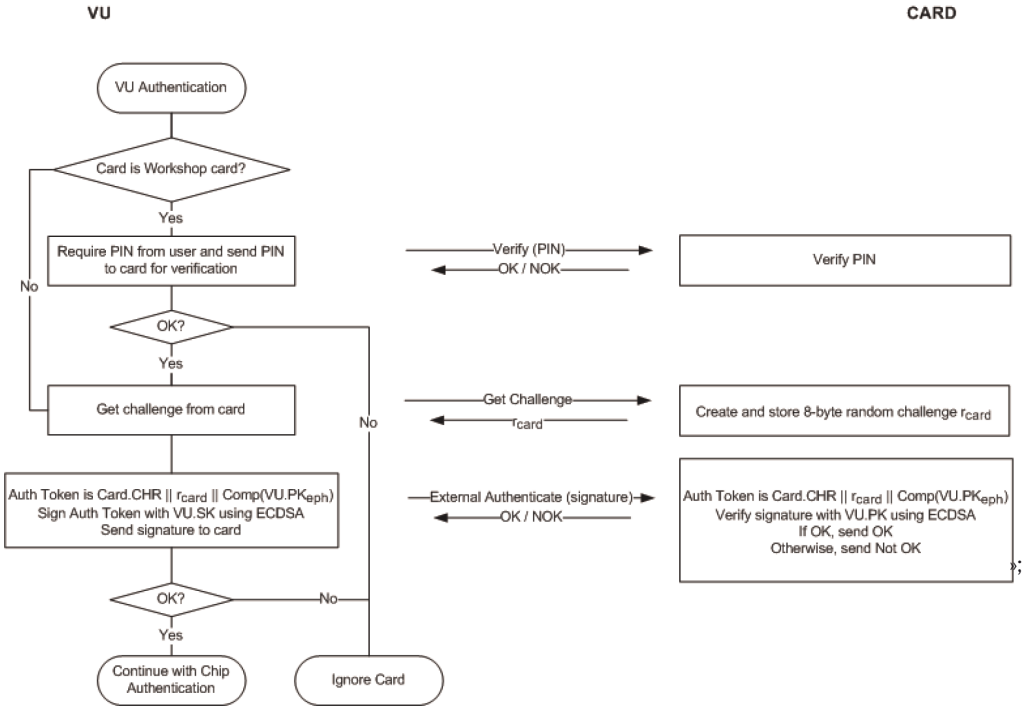
i) le premier alinéa du paragraphe CSM_170 est remplacé par le texte suivant:

«La VU inclut à proximité du défi de la carte, la signature de la référence du titulaire du certificat extraite du certificat de la carte.»;

ii) au paragraphe CSM_171, la figure 6 est remplacée comme suit:

«*Figure 6*

Protocole d'authentification de la VU



»;

iii) le paragraphe CSM_174 est remplacé par le texte suivant:

«CSM_174 À réception de la signature de la VU dans une commande EXTERNAL AUTHENTICATE, la carte:

— calcule le jeton d'authentification en concaténant Card.CHR, le lanceur de défis de la carte rcard et l'identificateur de la clé publique éphémère de la VU Comp(VU.PKeph);

— vérifie la signature de la VU à l'aide de l'algorithme ECDSA, en utilisant l'algorithme de hachage associé à la taille de clé de la paire de clés VU_MA de la VU, conformément au CSM_50, combiné à la VU.PK et au jeton d'authentification calculé.»;

q) au point 10.4, le paragraphe CSM_176 est modifié comme suit:

i) le deuxième alinéa est remplacé par le texte suivant:

«2. La VU adresse le point public $VU.PK_{eph}$ de sa paire de clés éphémères à la carte. Le point public est converti en chaîne d'octets comme le précise le [TR-03111]. On utilise la structure cryptée non compressée. Conformément au CSM_164, la VU génère cette paire de clés éphémères avant de vérifier la chaîne de certificat de la VU. La VU a envoyé l'identificateur de la clé publique éphémère $Comp(VU.PK_{eph})$ à la carte qui l'a mémorisé.»;

ii) le sixième alinéa est remplacé par le texte suivant:

«6. En utilisant K_{MAC}, la carte calcule un jeton d'authentification en fonction du point public éphémère de la VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Le point public prend le format utilisé par la VU (voir le point 2 ci-dessus). La carte envoie N_{PICC} et T_{PICC} à l'unité embarquée sur véhicule.»;

r) au point 10.5.2, le paragraphe CSM_191 est remplacé par le texte suivant:

«CSM_191 Tout objet de données à chiffrer doit être complété conformément à la norme [ISO 7816-4] en utilisant l'indicateur "01" de contenu de remplissage. Concernant le calcul du MAC, les objets de données de l'APDU sont complétés conformément à la norme [ISO 7816-4].

Remarque: le remplissage destiné à la messagerie sécurisée est toujours affecté à la couche de messagerie sécurisée, jamais aux algorithmes CMAC ou CBC.

Résumé et exemples

Une commande APDU de la messagerie sécurisée appliquée respecte la structure suivante, selon le cas de chaque commande non sécurisée (DO correspond à l'objet de données):

Cas 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Cas 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Cas 3 (octet INS pair): CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le

Cas 3 (octet INS impair): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le

Cas 4 (octet INS pair): CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le

Cas 4 (octet INS impair): CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

où Le = '00' ou '00 00' selon que l'on utilise des zones de longueur courte ou étendue; cf. [ISO 7816-4].

Une réponse APDU de la messagerie sécurisée appliquée respecte la structure suivante, selon le cas de chaque réponse non sécurisée:

Cas 1 ou 3: DO '99' || DO '8E' || SW1SW2

Cas 2 ou 4 (octet INS pair) sans cryptage: DO '81' || DO '99' || DO '8E' || SW1SW2

Cas 2 ou no 4 (octet INS pair) avec cryptage: DO '87' || DO '99' || DO '8E' || SW1SW2

Cas 2 ou 4 (octet INS impair) sans cryptage: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Remarque: Les cas 2 ou 4 (octet INS impair) avec cryptage ne servent jamais pour la communication entre une VU et une carte.

Ci-après suivent trois exemples de transformations APDU pour des commandes avec un code INS pair. La figure 8 illustre une commande APDU authentifiée relevant du cas 4, la figure 9 illustre une réponse APDU authentifiée relevant des cas 1 ou 3 et la figure 10 indique une réponse APDU cryptée et authentifiée relevant des cas 2 ou 4.

Figure 8

Transformation d'une commande APDU authentifiée relevant du cas 4

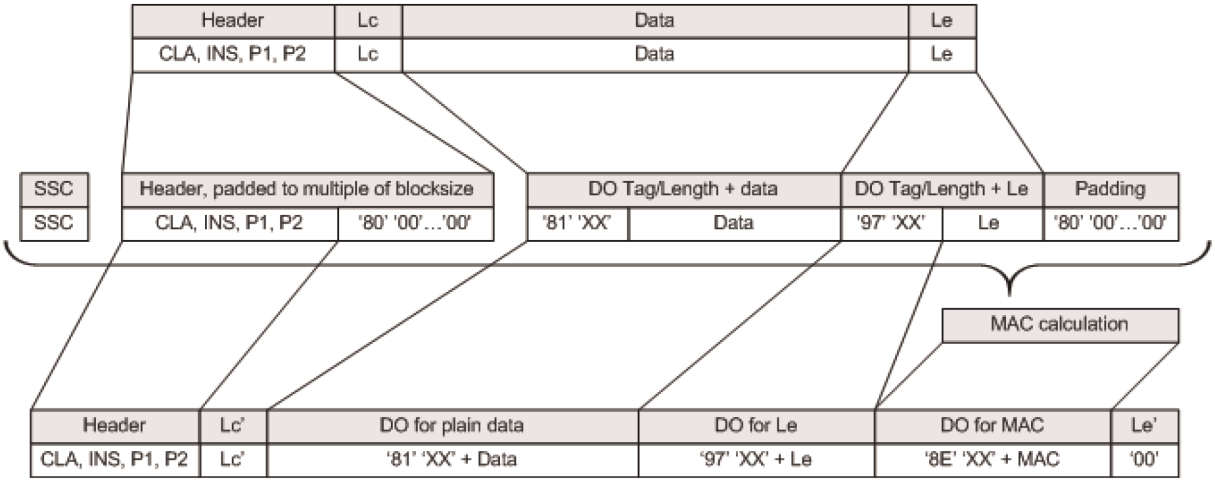


Figure 9

Transformation d'une réponse APDU authentifiée relevant des cas 1 ou 3

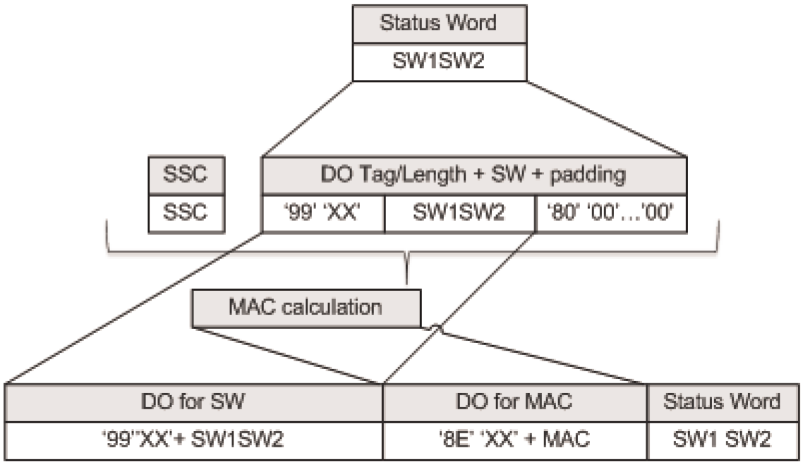
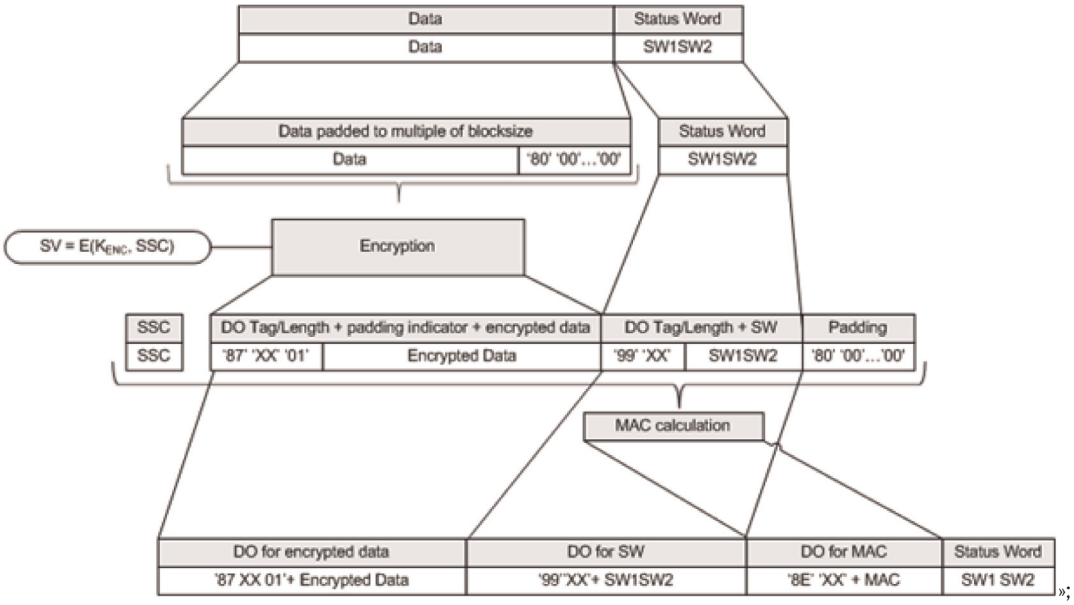


Figure 10

Transformation d'une réponse APDU cryptée et authentifiée relevant des cas 2 ou 4



»;

s) au point 10.5.3, le paragraphe CSM_193 est remplacé par le texte suivant:

«CSM_193 Une carte tachygraphique abandonne une session de messagerie sécurisée en cours si et seulement si l'une des conditions suivantes survient:

— elle reçoit une réponse APDU en clair,

— elle détecte une erreur de messagerie sécurisée dans une commande APDU:

— un objet de données de messagerie sécurisée manque, l'ordre des objets de données est erroné ou un objet de données inconnu est présent.

— un objet de données de la messagerie sécurisée est erroné, p. ex. la valeur MAC est erronée ou la structure TLV est erronée.

— l'alimentation est coupée ou la carte est réinitialisée,

— la VU entame la procédure d'authentification de la VU,

— la limite pour le nombre de commandes et de réponses associées de la session actuelle est atteinte. Pour une carte donnée, cette limite est définie par son fabricant et tient compte des exigences de sécurité du matériel utilisé, avec une valeur maximale de 240 commandes et réponses associées de SM par session.»;

t) le point 11.3.2 est modifié comme suit:

i) le premier alinéa du paragraphe CSM_208 est remplacé par le texte suivant:

"Pendant le couplage à une VU, un dispositif GNSS externe utilise le protocole décrit à la figure 5 (section 10.2.2) pour vérifier la chaîne de certification de la VU.";

ii) le paragraphe CSM_210 est remplacé par le texte suivant:

«CSM_210 Une fois le certificat VU_MA vérifié, le dispositif GNSS externe mémorise ce certificat pour l'utiliser en fonctionnement normal; cf. section 11.3.3.»;

u) au point 11.3.3, le premier alinéa du paragraphe CSM_211 est remplacé par le texte suivant:

«En fonctionnement normal, une unité embarquée sur véhicule et un EGF respectent le protocole décrit sur la figure 11 pour vérifier la validité dans le temps du certificat EGF_MA mémorisé et pour définir la clé publique VU_MA en vue de l'authentification ultérieure de la VU. Aucune autre vérification mutuelle des chaînes de certificats n'a lieu en fonctionnement normal.»;

v) au point 12.3, le tableau 6 est remplacé par le tableau suivant:

«*Tableau 6*

Nombre d'octets de données cryptées et en clair par instruction comme le prévoit la norme [ISO 16844-3]

Instruction	Demande/ Réponse	Description des données	Nbre d'octets de données en clair selon [ISO 16844-3]	Nbre d'octets de données en clair utilisant des clés AES	Nbre d'octets de données cryptées utilisant des clés AES d'une longueur (en bits) de		
					128	192	256
10	demande	Données d'authentification + numéro de fichier	8	8	16	16	16
11	réponse	Données d'authentification + contenu de fichier	16 bits ou 32 bits selon le fichier	16 bits ou 32 bits selon le fichier	32 / 48	32 / 48	32 / 48
41	demande	numéro de série MoS	8	8	16	16	16
41	réponse	Clé de couplage	16	16 / 24 / 32	16	32	32
42	demande	Clé de session	16	16 / 24 / 32	16	32	32
43	demande	Informations de couplage	24	24	32	32	32
50	réponse	Informations de couplage	24	24	32	32	32
70	demande	Données d'authentification	8	8	16	16	16
80	réponse	Valeur du compteur MoS + données d'authen.	8	8	16	16	16»

w) au point 13.1, l'exigence relative au numéro de série de la VU au paragraphe CSM_224 est remplacée par le texte suivant:

«**Numéro de série de la VU** le numéro de série de la VU ou l'ID de la demande de certificat (type de données VuSerialNumber ou CertificateRequestID) - voir le paragraphe CSM_123»;

x) au point 13.3, le paragraphe CSM_228, deuxième tiret, est remplacé par le texte suivant:

«2. La carte de contrôle utilise la clé maîtresse DSRC indiquée en combinaison avec le numéro de série de la VU ou l'ID de la demande de certificat dans les données relatives à la sécurité DSRC pour calculer les clés DSRC propres à la VU K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC, comme le précise le CSM_124.»;

y) le point 14.3 est modifié comme suit:

i) au paragraphe CSM_234, le texte précédant les notes relatives à la figure 13 est remplacé par le texte suivant:

«Un IDE peut procéder à la vérification d'une signature par rapport aux données téléchargées lui-même ou utiliser une carte de contrôle à cette fin. S'il utilise une carte de contrôle, la vérification de la signature respecte l'illustration de la Figure 13. Pour vérifier la validité temporelle d'un certificat présenté par l'IDE, la carte de contrôle utilise son heure interne actuelle, comme indiqué au CSM_167. La carte de contrôle actualise son heure actuelle si la Date effective d'un certificat authentique représentant une "source d'heure valide" est plus récente que l'heure actuelle de la carte. La carte accepte uniquement les certificats suivants comme source d'heure valide:

— certificats de lien ERCA de deuxième génération;

— certificats MSCA de deuxième génération;

— certificats VU_Sign ou Card_Sign de deuxième génération émis par le même pays que le certificat de carte de ladite carte de contrôle.

S'il procède lui-même à la vérification de la signature, l'IDE vérifie l'authenticité et la validité de tous les certificats dans la chaîne de certificats contenue dans le fichier de données ainsi que la signature par rapport aux données conformément à la procédure relative aux signatures définie par les [DSS]. Dans les deux cas, pour chaque certificat lu depuis le fichier de données, il est nécessaire de vérifier que le champ "Autorisation du titulaire de certificat" (CHA) est correct:

— Le champ CHA du certificat EQT indique un certificat de la VU ou de la carte (le cas échéant) à signer (voir l'appendice 1, type de données EquipmentType).

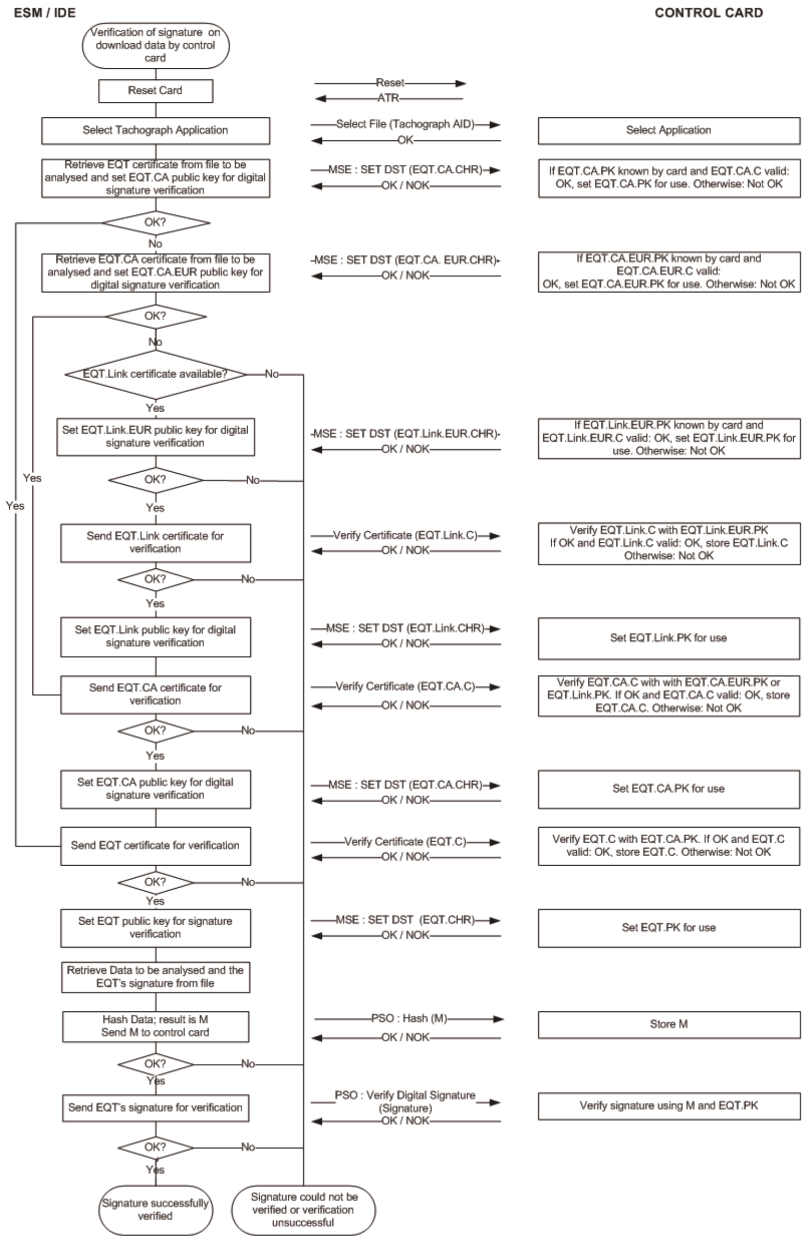
— Le champ CHA du certificat EQT.CA indique une MSCA.

— Le champ CHA du certificat EQT.Link indique une ERCA.»;

ii) la figure 13 est remplacée par ce qui suit:

«*Figure 13*

Protocole de vérification de la signature associée à un fichier de données téléchargé



»;

37) l'appendice 12 est modifié comme suit:

a) le point 3 est modifié comme suit:

i) au paragraphe GNS_4, le deuxième alinéa suivant la figure 2 est remplacé par le texte suivant:

«La résolution de la position repose sur la structure de la phrase RMC décrite ci-dessus. La première partie des champs 3) et 5) correspondent aux degrés. Le reste correspond aux minutes avec trois décimales. La résolution est donc de 1/1 000 minute ou 1/60 000 degré (parce qu'une minute correspond à 1/60 degré).»;

ii) le paragraphe GNS_5 est remplacé par le texte suivant:

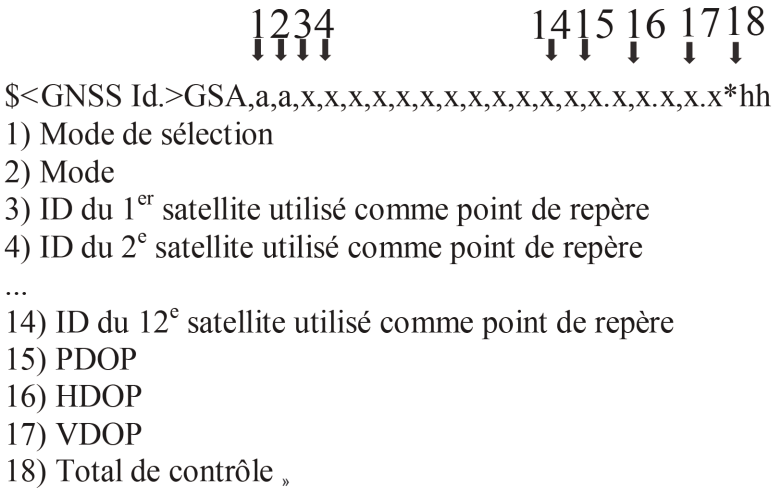
«GNS_5 L'unité embarquée sur le véhicule mémorise dans la base de données de la VU les informations relatives au positionnement en termes de latitude et de longitude selon une résolution d'1/10 minute ou 1/600 degré, comme le décrit l'appendice 1 pour les coordonnées géographiques type.

La VU peut utiliser la commande GPS DOP et satellites actifs (GSA) pour déterminer et enregistrer la disponibilité et l'exactitude du signal. En particulier, HDOP sert à fournir une indication sur le degré d'exactitude des données de localisation enregistrées (cf. 4.2.2). La VU enregistre la valeur du coefficient d'affaiblissement de la précision de positionnement horizontal (HDOP) calculée comme étant la minimale des valeurs HDOP recueillies sur les systèmes GNSS disponibles.

L'identificateur du système GNSS indique l'identifiant NMEA correspondant pour chaque constellation GNSS et pour le SBAS (Satellite-Based Augmentation System).

Figure 3

Structure de la phrase GSA



iii) le paragraphe GNS_6 est remplacé par le texte suivant:

«GNS_6 La phrase GSA est mémorisée avec le numéro d'enregistrement "02" à "06"»;

b) le point 4.2.1 est modifié comme suit:

i) le paragraphe GNS_16 est remplacé par le texte suivant:

«GNS_16 Le protocole de communication ne doit pas prendre en charge les zones de longueur étendue.»;

ii) le paragraphe GNS_18 est remplacé par le texte suivant:

«GNS_18 Concernant les fonctions 1) de collecte et de diffusion des données GNSS, 2) de collecte des données de configuration du dispositif GNSS externe et 3) du protocole de gestion, l'émetteur-récepteur sécurisé GNSS simule une carte intelligente dont l'architecture du système de fichiers comprend un fichier maître (MF), un fichier spécialisé (DF) doté de l'identificateur d'application spécifié en appendice 1, chapitre 6.2 ("FF 44 54 45 47 4D"), trois fichiers élémentaires contenant des certificats et un fichier élémentaire unique (EF.EGF) dont l'identificateur de fichier correspond à "2F2F" comme le prévoit le tableau 1.»;

iii) le paragraphe GNS_20 est remplacé par le texte suivant:

«GNS_20 L'émetteur-récepteur sécurisé GNSS doit utiliser une mémoire pour enregistrer les données et pouvoir effectuer au moins 20 millions de cycles d'écriture et de lecture. Hormis cet aspect, la conception interne et la mise en œuvre de l'émetteur-récepteur sécurisé GNSS incombent aux fabricants.

Le tableau 1 fournit la modélisation des numéros d'enregistrement et des données. Remarque: il existe cinq phrases GSA correspondant aux constellations GNSS et au SBAS (Satellite-Based Augmentation System).»;

c) au point 4.2.2, le cinquième alinéa du paragraphe GNS_23 est remplacé par le texte suivant:

«5. Le processeur de la VU vérifie les données reçues en extrayant les informations (p. ex. la latitude, la longitude ou l'heure) de la phrase RMC NMEA. Cette dernière inclut les informations si le positionnement est valide. Si tel n'est pas le cas, les données de localisation ne sont pas encore mises à disposition et ne peuvent pas servir à enregistrer la position du véhicule. Si le positionnement est valide, le processeur de la VU extrait également les valeurs HDOP des phrases GSA NMEA et calcule la valeur minimale d'après les systèmes de satellites disponibles (p. ex., lorsque les points de repère sont disponibles).»;

d) au point 4.4.1, le paragraphe GNS_28 est remplacé par le texte suivant:

«GNS_28 Si la VU ne parvient pas à gérer la communication avec le dispositif GNSS externe apparié pendant plus de 20 minutes consécutives, la VU génère et enregistre dans la VU un évènement de type EventFaultType avec la valeur enum "0E"H Communication error with the external GNSS facility assorti d'un horodatage indiquant l'heure actuelle. L'événement n'est généré que si les deux conditions suivantes sont satisfaites: a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule circule. Dans ce contexte, une erreur de communication survient lorsque l'émetteur-récepteur sécurisé de la VU ne reçoit pas de message de réponse après un message de demande, au sens de la section 4.2.»;

e) au point 4.4.2, le paragraphe GNS_29 est remplacé par le texte suivant:

«GNS_29 En cas d'atteinte au dispositif GNSS externe, l'émetteur-récepteur sécurisé GNSS efface toute sa mémoire, y compris le matériel cryptographique. Comme le prévoient GNS_25 et GNS_26, la VU détecte les infractions si la réponse possède l'état "6690". La VU génère ensuite un événement de type EventFaultType enum "19"H Tamper detection of GNSS. Le dispositif GNSS externe peut également arrêter de répondre aux demandes externes.»;

f) au point 4.4.3, le paragraphe GNS_30 est remplacé par le texte suivant:

«GNS_30 Si l'émetteur-récepteur sécurisé GNSS ne reçoit aucune donnée du récepteur GNSS pendant plus de trois heures successives, il génère un message de réponse à la commande READ RECORD où le nombre RECORD est égal à "01" et contenant une zone de données de 12 octets tous définis sur 0xFF. Dès réception du message de réponse avec cette valeur de zone de données, la VU génère et mémorise un évènement de type EventFaultType enum "0D"H Absence of position information from GNSS receiver assorti d'un horodatage indiquant l'heure actuelle uniquement si les deux conditions suivantes sont satisfaites: a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule circule.»;

g) au point 4.4.4, le texte du paragraphe GNS_31, jusqu'à la figure 4, est remplacé par le texte suivant:

«Si la VU détecte que le certificat EGF utilisé pour l'authentification mutuelle n'est plus valide, la VU génère et enregistre un événement de l'équipement d'enregistrement de type EventFaultType enum *"1B"H External GNSS facility certificate expired* assorti d'un horodatage indiquant l'heure actuelle. La VU utilise encore les données de positionnement GNSS reçues.»;

h) au point 5.2.1, le paragraphe GNS_34 est remplacé par le texte suivant:

«GNS_34 Si la VU ne reçoit aucune donnée du récepteur GNSS pendant plus de trois heures successives, la VU génère et mémorise un évènement de type EventFaultType enum "0D"H Absence of position information from GNSS receiver assorti d'un horodatage indiquant l'heure actuelle uniquement si les deux conditions suivantes sont satisfaites: a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule circule.»;

i) le point 6 est remplacé par le texte suivant:

«6. CONFLIT TEMPOREL GNSS

Si la VU détecte un écart de plus d'une minute entre le temps indiqué par sa fonction de mesure du temps et le temps indiqué par le récepteur GNSS, la VU mémorise un évènement de type EventFaultType enum *"0B"H Time conflict (GNSS versus VU internal clock)*. Après le déclenchement d'un événement "Conflit temporel", la VU ne vérifie plus les écarts temporels pendant les 12 heures suivantes. Cet événement n'est pas déclenché lorsqu'aucun signal GNSS valable n'a pu être détecté par le récepteur GNSS au cours des 30 derniers jours.»;

38) l'appendice 13 est modifié comme suit:

a) au point 2, le quatrième paragraphe est remplacé par le texte suivant:

«Pour plus de précision, le présent appendice ne spécifie pas:

— la collecte de l'opération et de la gestion des *données* au sein de la VU (qui sera spécifiée ailleurs dans le *règlement* ou constituera autrement une fonction de la conception du produit).

— La forme de la présentation des données collectées pour l'application hébergée sur le dispositif externe.

— Les dispositions de protection des données au-delà de ce que prévoit Bluetooth® (comme le codage) concernant le contenu des *données* (qui sera précisé ailleurs dans le *règlement* [appendice 11 — Mécanismes de sécurité communs]).

— Les protocoles Bluetooth® qu'utilise l'interface ITS.»;

b) au point 4.2, le troisième alinéa est remplacé par le texte suivant:

"Lorsqu'un dispositif externe entre dans le champ de portée de la VU pour la première fois, la procédure de couplage Bluetooth® peut être démarrée (cf. également annexe 2). Les dispositifs partagent leur adresse, nom, profil et clé secrète commune. Cela leur permet de se connecter dès qu'ils se retrouvent à proximité l'un de l'autre à nouveau. Après cette étape, le dispositif externe est sécurisé et en mesure d'effectuer des demandes de téléchargement de données émanant du tachygraphe. Il n'est pas prévu d'ajouter des mécanismes de codage supplémentaires au-delà de ceux assurés par Bluetooth®. Cependant, si des mécanismes de sécurité additionnels se révélaient nécessaires, ils seraient ajoutés conformément à l'appendice 11 Mécanismes de sécurité communs.";

c) le point 4.3 est modifié comme suit:

i) le premier alinéa est remplacé par le texte suivant:

«Pour des raisons de sécurité, la VU nécessite un système d'autorisation de code PIN distinct du couplage Bluetooth®. Chaque VU est en mesure de générer des codes PIN à des fins d'authentification, composés d'au moins quatre chiffres. Chaque fois qu'un dispositif externe se couple avec la VU, il doit fournir le code PIN correct avant de recevoir des données, quelles qu'elles soient.»;

ii) le troisième paragraphe suivant le tableau 1 est remplacé par le texte suivant:

«Il arrive que le fabricant permette à titre facultatif de modifier le code PIN directement sur la VU; toutefois, le code PUC n'est pas modifiable. La modification du code PIN, le cas échéant, requiert d'indiquer le code PIN directement sur la VU.»;

d) au point 4.4, le deuxième paragraphe suivant l'intitulé «zone de données» est remplacé par le texte suivant:

«Si les données à manipuler dépassent l'espace disponible dans un message, elles seront partagées en plusieurs sous-messages. Chaque sous-message présente le même en-tête et le même SID, mais contient un compteur sur deux octets, un compteur courant (CC) et un compteur max (CM) pour indiquer le numéro du sous-message. Afin de permettre le contrôle d'erreur et l'abandon éventuel d'un échange de données, le dispositif récepteur accuse réception de chaque sous-message. Le dispositif récepteur est à même d'accepter le sous-message, d'en demander la réémission et de demander au dispositif émetteur d'en reprendre ou d'en abandonner la transmission.»;

e) l'annexe 1 est modifiée comme suit:

i) le titre est remplacé par le texte suivant:

«1) LISTE DES DONNÉES DISPONIBLES GRÂCE À L'INTERFACE ITS»;

ii) l'élément suivant est inséré dans le tableau au point 3, après l'élément «Absence d'informations de position en provenance du récepteur GNSS»:

«Erreur de communication avec le dispositif GNSS externe	— l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, — les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	— la date et l'heure du début de l'événement, — la date et l'heure de la fin de l'événement, — le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, — le nombre d'événements semblables survenus le même jour.»

iii) au point 5, le tiret suivant est ajouté:

«— anomalie sur l'interface ITS (le cas échéant)»;

f) les spécifications ASN.1 à l'annexe 3 sont modifiées comme suit:

i) les lignes 206a à 206e ci-après sont insérées après la ligne 206:

```
»206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }»;
```

ii) les lignes 262 à 264 sont remplacés comme suit:

```
«262    driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), »;
```

iii) la ligne 275 est remplacée comme suit:

```
«275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),«;
```

iv) les lignes 288 à 310 sont remplacés comme suit:

```
«288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310»
```

v) les lignes 362 et 363 sont remplacées comme suit:

```
«362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),»;
```

vi) les lignes 410a et 410b suivantes sont insérées après la ligne 410:

```
«410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,»;
```

vii) les lignes 539a à 539j ci-après sont insérées après la ligne 539:

```
«539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j»;
```

39) l'appendice 14 est modifié comme suit:

a) l'élément 5.5 de la table des matières est remplacé comme suit:

«5.5 Conformité à la directive (UE) 2015/719 ..... 490»;

b) au point 2, le troisième alinéa est remplacé par le texte suivant:

«Ce cas de figure prévoit une durée de communication limitée parce que *la communication* est ciblée et qu'elle se fait à courte portée. Par ailleurs, les autorités de contrôle compétentes peuvent utiliser les moyens de communication assurant le contrôle à distance des tachygraphes (RTM) pour d'autres applications, comme le poids maximal et les dimensions maximales des poids lourds définis dans la directive (UE) 2015/719. Ces opérations peuvent être distinctes du contrôle à distance des tachygraphes ou consécutives à celui-ci, à la discrétion des autorités de contrôle compétentes.»;

c) le point 5.1 est modifié comme suit:

i) au paragraphe DSC_19, le douzième tiret est remplacé par le texte suivant:

«— L'antenne DSRC-VU est placée de manière à optimiser la communication DSRC entre le véhicule et l'antenne de lecture en bord de route, lorsque le lecteur se trouve à une distance de 15 mètres devant le véhicule et à 2 mètres de hauteur, en ciblant le centre horizontal et vertical du pare-brise. Pour les véhicules légers, une installation sur la partie supérieure du pare-brise convient. Pour tous les autres véhicules, l'antenne DSRC est placée près de la partie inférieure ou de la partie supérieure du pare-brise.»;

ii) au paragraphe DSC_22, le premier alinéa est remplacé par le texte suivant:

«Le format de l'antenne n'est pas défini et demeure une décision commerciale, à condition que la DSRC-VU installée satisfasse aux exigences de conformité définies à la section 5 ci-dessous. L'antenne est positionnée comme défini au point DSC_19 et elle prend efficacement en charge les cas d'usage décrits en 4.1.2 et en 4.1.3.»;

d) au point 5.4.3, la séquence 7 est remplacée par ce qui suit:

«7	REDCR	>	DSRC-VU	Envoie GET.request concernant les données d'un autre attribut (si nécessaire)»

e) au point 5.4.4, le module ASN.1 au paragraphe DCS_40 est modifié comme suit:

i) la première ligne de la séquence relative au `TachographPayload` est remplacée par ce qui suit:

```
«tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509[1]»
```

ii) la note de bas de page 1 suivante est ajoutée:

«1. Si un LPN contient un AlphabetIndicator LatinAlphabetNo2 ou latinCyrillicAlphabet, les caractères spéciaux sont retranscrits par l'unité d'interrogation routière en utilisant les règles spéciales prévues par l'annexe E de la norme ISO/DIS 14 906,2»;

iii) l'exposant 2 est supprimé de la ligne où l'horodatage de l'enregistrement actuel est défini;

iv) le module ASN.1 pour `RtmTransferAck` est remplacé par ce qui suit:

```
«RtmTransferAck ::= INTEGER {
                    Ok (1),
                    NoK (2)
                    } (1..255)»;
```

f) au point 5.4.5, l'élément RTM12 du tableau 14.3 est remplacé par le texte suivant:

«**RTM12** **Anomalie du capteur**	La VU génère une valeur exprimée par un nombre entier pour l'élément de données RTM12. La VU attribue à la variable sensorFault une valeur de: — 1 si un événement de type anomalie de capteur "35"H a été enregistré au cours des 10 derniers jours, — 2 si un événement de type anomalie du récepteur GNSS (interne ou externe, avec les valeurs enum "36"H ou "37"H) a été enregistré au cours des 10 derniers jours. — 3 si un événement de type erreur de communication avec le dispositif GNSS externe "0E"H a été enregistré au cours des 10 derniers jours — 4 si à la fois des anomalies de capteur et des anomalies de récepteur GNSS ont été enregistrées au cours des 10 derniers jours — 5 si à la fois des anomalies de capteur et des erreurs de communication avec le dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours — 6 si à la fois des anomalies de récepteur GNSS et des erreurs de communication avec le dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours — 7 si des anomalies des trois types ont été enregistrées au cours des 10 derniers jours AUTREMENT, une valeur de 0 est attribuée si aucun événement n'a été enregistré au cours des 10 derniers jours.	– erreur de capteur un octet conformément au dictionnaire des données	`sensorFault INTEGER (0..255),;` »

g) au point 5.4.6, le paragraphe DSC_43 est remplacé par le texte suivant:

«DSC_43
Pour tous les échanges DSRC, les données sont codées à l'aide des règles PER (Packed Encoding Rules) NON ALIGNÉES, à l'exception de `TachographPayload` et `OwsPayload`;, qui sont encodées à l'aide des règles OER (Octet Encoding Rules) définies par la norme ISO/IEC 8825-7, Rec. ITU-T X.696.»;

h) au point 5.4.7, dans la quatrième colonne du tableau 14.9, le texte de la cellule décrivant `Rtm-ContextMark`; est remplacé par ce qui suit:

«Identificateur d'objet de la norme, partie et version prise en charge. Exemple: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1).

Le premier octet est 06H, qui est l'identificateur d'objet. Le deuxième octet est 06H, qui est sa longueur. Les 6 octets suivants codent l'identificateur d'objet de l'exemple.»;

i) les points 5.5 et 5.5.1 sont remplacés par le texte suivant:

«5.5. **Conformité à la directive (UE) 2015/719**

5.5.1. *Récapitulatif*

DSC_59 Pour respecter la directive (UE) 2015/719 sur les poids et les dimensions maximaux des poids lourds, le protocole de transaction de téléchargement des données OWS utilisant la liaison d'interface DSRC 5,8 GHz est le même que celui servant aux données RTM (cf. 5.4.1). La seule différence réside dans le fait que l'identificateur d'objet associé à la norme TARV respecte la norme ISO 15638 (TARV) partie 20 concernant les WOB/OWS.»;

j) au point 5.6.1, l'alinéa a) du paragraphe DSC_68 est remplacé par le texte suivant:

«a) Pour que la fourniture de la VU et de la DSRC-VU, voire de différents lots de la DSRC-VU, puisse être sous-traitée à plusieurs fournisseurs, la connexion reliant la VU et la DSRC-VU non interne à la VU doit être une connexion ouverte normalisée. La VU doit être connectée à la DSRC-VU»;

k) au point 5.7.1, le paragraphe DSC_77 est remplacé par le texte suivant:

«DSC_77 *Les données* sont fournies déjà sécurisées par la fonction *VUSM* à la *DSRC-VU*. La *VUSM* vérifie que les données enregistrées dans la *DSRC-VU* le sont de manière satisfaisante. L'enregistrement et le signalement de toutes les erreurs survenues pendant le transfert de données depuis la *VU* vers la mémoire de la *DSRC-VU* doivent être consignés avec le type EventFaultType et la valeur enum d'erreur de communication '0C'H Communication error with the remote communication facility, ainsi que l'horodatage.»;

40) l'appendice 15 est modifié comme suit:

a) au point 2.2, le premier alinéa est remplacé par le texte suivant:

«Il est entendu que la première génération de cartes tachygraphiques est interopérable avec la première génération d'unités embarquées sur les véhicules (conformément à l'annexe 1B du règlement (CEE) n° 3821/85), alors que la deuxième génération de cartes tachygraphiques est interopérable avec la deuxième génération d'unités embarquées sur les véhicules (conformément à l'annexe IC de la présente directive). De plus, les exigences ci-dessous s'appliquent.»;

b) le point 2.4.1, paragraphe MIG_11, est modifié comme suit:

i) le premier tiret est remplacé par le texte suivant:

«— EF ICC, IC non signés (facultatif), »;

ii) le troisième tiret est remplacé par le texte suivant:

«— d'autres EF de données d'application (au sein du DF Tachograph) nécessaires au protocole de téléchargement des cartes de première génération. Ces informations seront protégées par une signature numérique conformément aux mécanismes de sécurité de première génération.

Ce type de téléchargement n'inclura pas d'EF de données d'application uniquement présents sur les cartes de conducteur (et d'atelier) de deuxième génération (EF de données d'application au sein du DF Tachograph_G2).»;

c) au point 2.4.3, les points MIG_014 et MIG_015 sont remplacés par le texte suivant:

«MIG_014 En dehors du cadre du contrôle d'un conducteur par des autorités de contrôle autre que celles de l'UE, les données sont téléchargées depuis une unité embarquée sur véhicule de deuxième génération selon les mécanismes de sécurité de deuxième génération et le protocole de téléchargement de données défini à l'appendice 7 de la présente annexe.

MIG_015 Pour permettre le contrôle des conducteurs par des autorités de contrôle autres que celles de l'UE, il peut également être rendu possible de télécharger des données depuis des unités embarquées sur véhicule de deuxième génération selon les mécanismes de sécurité de première génération. Les données téléchargées auront alors le même format que les données téléchargées depuis une unité embarquée sur un véhicule de première génération. Cette fonctionnalité peut être sélectionnée grâce aux commandes du menu.»

ANNEXE II

L'annexe II du règlement (UE) 2016/799 est modifiée comme suit:

1) au chapitre I, le point 1, paragraphe b), est remplacé par le texte suivant:

«b) d'un numéro d'homologation correspondant au numéro du certificat d'homologation établi pour le prototype de l'appareil de contrôle, de la feuille d'enregistrement ou de la carte tachygraphique, placé dans une position quelconque à proximité immédiate du rectangle.»;

2) au chapitre III, le point 5 est remplacé par le texte suivant:

«5. Présenté à l'homologation le .....»;

3) au chapitre IV, le point 5 est remplacé par le texte suivant:

«5. Présenté à l'homologation le .....»;