

Distr.: General 5  
December 2018

Original: English only

---

## **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)**

**Twentieth session**

Geneva, 18 February 2019

Item 2 (b) of the provisional agenda

**Programme of Work**

**Appendix 1C**

### **Appendix 1C**

#### **Submitted by European Commission**

The European Commission has submitted Informal document No. 1 (February 2019) “Smart Digital Tachograph Technical Analysis for the Amendment of Regulation 799/2016” as an aid to understand the changes in Regulation European Union 2016/799. SC.1 is invited to continue its review of ECE/TRANS/SC.1/GE.21/2018/1 taking into account any relevant information in this document.



## JRC TECHNICAL REPORTS

# Smart Digital Tachograph

*Technical Analysis for  
the Amendment of  
Regulation 799/2016.*

Mahieu, V.

Chiaranello, M.

Baldini, G.M.

Sportiello, L.

Kunegel, J.

Herrera Alcantara, A.

Nordvik, J.P.

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

**Contact information**

Name: Antonio Herrera Alcantara

Address: Joint Research Centre, Via Enrico Fermi 2749, TP 360, 21027 Ispra (VA), Italy

Email: Antonio.HERRERA-ALCANTARA@ec.europa.eu

Tel.: + 39 0332 78 5029

**JRC Science Hub**

<https://ec.europa.eu/jrc>

JRC110452

Ispra, Italy: European Commission, 2017

The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted. The European Commission shall not be held liable for any consequences stemming from the reuse.

**Contents**

Abstract .....2  
Executive Summary .....3  
Checklist of Changes.....4

## Abstract

# Smart Digital Tachograph

## Technical Analysis for the Amendment to Regulation 799/2016

Date: 07/12/2017  
Version: 1.0  
Status: Amendment approved by the Road Transport Committee on 06/12/2017  
Author(s): V. Mahieu, M. Chiaramello, G.M. Baldini, L Sportiello, A. Herrera Alcantara  
Approved by: J.P. Nordvik  
Public: MOVE/C1, JRC/Dir E  
EU Classification **UNCLASSIFIED**

## Executive Summary

The technical specifications for the Smart Digital Tachograph, usually referred to as "Annex 1C", were published on 18/03/2016 as Commission Implementing Regulation (EU) No 799/2016, 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.

Following the publication, the JRC and industry identified a number technical issues and functional shortcomings leading to the need for an amendment of Regulation 799/2016.

The JRC has coordinated a platform of experts from Digital Tachograph equipment manufacturers to analyse the issues and propose the changes needed in the Regulation in order to tackle the known problems, this is a high level summary of the numerous changes:

- Accumulated driving time
- Events & faults
- Automatic time adjustments
- Data download
- ITS interface
- Daily work period begin/end
- Other minor fixes and light changes

This document gathers in a structured table, the checklist of changes, the analysis and rationale for all the individual changes proposed for the amendment of Regulation 799/2016 in a traceable manner. This table has served as the basis for the preparation of the amendment finally approved by the Road Transport Committee on 06/12/2017.

## Checklist of Changes

<p>CHECKLIST OF CHANGES FOR AMENDED ANNEX IC and APPENDIXES  <b>IMPLEMENTING REGULATION, ANNEX IC and APPENDIXES</b></p>			
Ref (section/page/req)	Published Text + Issue	New text + Rationale	L139/
Reg.(EU) n° 799/2016 article 2	<p>(8) 'tachograph component' or 'component' means any of the following elements: the vehicle unit, the motion sensor, the tachograph card, the record sheet, the external GNSS facility and the remote early detection facility;</p> <p>Issue: The cards are not a component of a tachograph</p>	<p>Replace definition 8 with:</p> <p>(8) 'tachograph component' or '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;</p> <p>Rationale: The cards are not a component of a tachograph</p>	3
Reg.(EU) n° 799/2016 article 2	<p><b>Issue:</b> unclear definition of "Vehicle Unit" and its composition in components and possible contradiction with Article 2</p>	<p>Add definition 10:</p> <p>(10) 'vehicle unit' means:</p> <p>the tachograph excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may be a single unit or several units distributed in the vehicle, provided that it complies with the security requirements of this Regulation; the vehicle unit includes, among other things, a processing unit,</p>	3

		<p>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;</p> <p>The vehicle unit also includes a GNSS receiver and a remote communication facility.</p> <p>The vehicle unit may be composed of the following type approvable components:</p> <ul style="list-style-type: none"> <li>- vehicle unit, as a single component (including GNSS receiver and remote communication facility),</li> <li>- vehicle unit main body (including remote communication facility), and external GNSS facility,</li> <li>- vehicle unit main body (including GNSS receiver), and external remote communication facility,</li> <li>- vehicle unit main body, external GNSS facility, and external remote communication facility.</li> </ul> <p>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, the time measurement function, etc.</p> <p>In this Regulation, in order to simplify the text and ease understanding, "vehicle unit (VU)" is used for "vehicle unit or vehicle unit main body".</p> <p><b>Rationale:</b> Clearer definition</p>
--	--	--



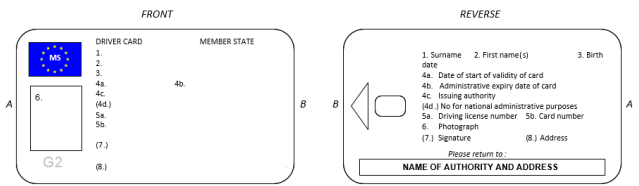
<p><i>Annex II article 1</i></p>	<p>(b) an approval number corresponding to the number of the approval certificate drawn up for the prototype of the recording equipment or the record sheet or to the number of a tachograph card, placed at any point within the immediate proximity of that rectangle.</p> <p><b>Issue:</b> typo</p>	<p><i>(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 <b>the</b> tachograph card, placed at any point within the immediate proximity of that rectangle.</i></p> <p><b>Rationale:</b> typo corrected</p>	<p>XXX</p>
<p><i>Annex II Chapter III</i></p>	<p>5. Submitted for approval for ....</p> <p><b>Issue:</b> typo</p>	<p><i>5. Submitted for approval <b>on</b> ....</i></p> <p><b>Rationale:</b> typo corrected</p>	<p>XXX</p>
<p><i>Annex II Chapter IV</i></p>	<p>5. Submitted for approval for ....</p> <p><b>Issue:</b> typo</p>	<p><i>5. Submitted for approval <b>on</b> ....</i></p> <p><b>Rationale:</b> typo corrected</p>	<p>XXX</p>
<p><i>Annex IC, definition 'yy'</i></p>	<p>(yy) 'adaptor' means:</p> <p>a device, providing a signal permanently representative of vehicle speed and/or distance travelled,</p> <p>other than the one used for the independent movement detection, and which is:</p> <p>— 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 (1), as last amended) put into service</p> <p>since 1 May 2006,</p>	<p><i>(yy) 'adaptor' means:</i></p> <p><i>a device, providing a signal permanently representative of vehicle speed and/or distance travelled,</i></p> <p><i>other than the one used for the independent movement detection, and which is:</i></p> <p><i>— 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 (1), as last amended) <del>put into service</del></i></p> <p><i><b>since 1 May 2006,</b></i></p>	<p>018</p>

	<p><b>Issue:</b> the sentence “put into service since 1 May 2006” is too restrictive and forbid any retrofit on older vehicles</p>	<p><b>Rationale:</b> It is better to delete “put into service since 1 May 2006”. This will give the possibility to install a digital Tacho also in older vehicle. This supports a better security and can help mitigating fraud.</p>	
Annex 1 C req. 49	<p>The first change of activity to 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).</p> <p><b>Issue:</b> In all the text it is BREAK/REST</p>	<p>The first change of activity to <b>BREAK/REST</b> 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).</p> <p><b>Rationale:</b> No reasons to process the BREAK differently than the REST.</p>	025
Annex 1 C req. 59	<p>(59) The driver shall then enter the current place of the vehicle, which shall be considered as a temporary entry.</p> <p><b>Issue:</b> It is not clear what happens if the user did no end place entry during manual entry at card insertion but did give a begin place entry.</p>	<p>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):</p> <ul style="list-style-type: none"> <li>- Entry of a place where the current daily work period begins during manual entry according to requirement (61)</li> <li>- 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)</li> </ul> <p>Under the following conditions temporary entry made at last card withdrawal is overwritten and validated:</p> <ul style="list-style-type: none"> <li>- 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 entry according to requirement (61)</li> </ul> <p><b>Rationale:</b> with the changes no more overwriting is possible</p>	025

<p>Annex 1 C req. 61</p>	<p>(61) Upon driver (or workshop) card insertion, and only at this time, the recording equipment shall allow manual entries of activities. Manual entries of activities shall be performed using local time and date values of the time zone (UTC offset) currently set for the vehicle unit.</p> <p>.....</p> <p>During the manual entries associated with card insertion and if applicable, the card holder shall have the opportunity to input:</p> <ul style="list-style-type: none"> <li>- a place where a previous daily work period ended, associated to the relevant time (thus overwriting the entry made at the last card withdrawal),</li> <li>- a place where the current daily work period begins, associated to the relevant time.</li> </ul> <p><b>issue:</b> ambiguity in management of end of daily work period</p>	<p>(61) Upon driver (or workshop) card insertion, and only at this time, the recording equipment shall allow manual entries of activities. Manual entries of activities shall be performed using local time and date values of the time zone (UTC offset) currently set for the vehicle unit.</p> <p>.....</p> <p>During the manual entries associated with card insertion and if applicable, the card holder shall have the opportunity to input:</p> <ul style="list-style-type: none"> <li>- 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),</li> <li>- a place where the current daily work period begins, associated to the relevant time (thus validating a temporary entry made at last card withdrawal).</li> </ul> <p><b>Rationale:</b> Ambiguity solved.</p>	<p>025</p>
<p>Annex 1C req. 89</p>	<p>Req 89: The recording equipment shall self detect faults through self-tests and built-in-tests, according to the following table</p> <p><b>Issue:</b> wording unclear</p>	<p>Req 89: The recording equipment shall detect faults through self-tests and built-in-tests, according to the following table</p> <p><b>Rationale:</b> no more ambiguity</p>	<p>031</p>
<p>Annex 1C Req 116</p>	<p>(21) The motion sensor (possibly embedded in the adaptor) is the main source for speed and distance measurement.</p>		<p>035</p>

	<p>...</p> <p>(24) The speed measurement function shall also provide the information whether the vehicle is moving or stopped. The vehicle shall be considered as moving as soon as the function detects more than 1 imp/ sec for at least 5 seconds from the motion sensor, otherwise the vehicle shall be considered as stopped.</p> <p>...</p> <p>3.12.7 Detailed speed data</p> <p>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 driven.</p> <p><b>Issue:</b> req 116 by using the wording driven is creating problems and ambiguity regarding the calculation of the minute, and is introducing a change compared with Annex IB wording</p>	<p>(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 <b>vehicle has been moving.</b></p> <p><b>Rationale:</b> Better wording, analyzed and crosschecked with VU manufacturers</p>	
Annex 1C req. 200	<p><b>Issue:</b> For back compatibility and safety of vehicle operations, personal data (like speed) recorded or produced by tachographs must continue to be communicated to sensitive platforms in the vehicle network. These data in general stay in the vehicle network. However, for any further process outside the vehicle, access to the driver consent status supports for a processing compliant with EU data protection regulation.</p>	<p>Replace the current requirement by:</p> <p>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.</p> <p>In Appendix 13, an optional ITS interface is specified and standardized. Other similar interfaces <b>or vehicle unit output channels</b> may co-exist, provided they fully comply with the</p>	46

		<p>requirements of Appendix 13 in term of minimum list of data, security and driver consent.</p> <p>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").</p> <p>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.</p> <p>The following requirements apply to ITS data made available through that interface:</p> <ul style="list-style-type: none"> <li>- these data are a set of selected existing data from the tachograph data dictionary (Appendix 1),</li> <li>- a subset of these selected data are marked 'personal data',</li> <li>- 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,</li> <li>- At any moment, the driver consent can be enabled or disabled through commands in the menu, provided the driver card is inserted,</li> <li>- 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,</li> <li>- the pairing of the external device with the ITS</li> </ul>	
--	--	--	--

		<p>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,</p> <ul style="list-style-type: none"> <li>- in any circumstances, the presence of the ITS interface cannot disturb or affect the correct functioning and the security of the vehicle unit.</li> </ul> <p>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.</p> <p>The recording equipment shall have the capacity to communicate the driver consent status to other platforms in the vehicle network.</p> <p>When the ignition of the vehicle is ON, these data shall be permanently broadcasted.</p> <p><b>Rationale:</b> Use of personal data on the vehicle network is possible for back compatibility, but is under the umbrella of the GDPR.</p>	
<p>Annex 1C req. 235</p>	<p>Issue: typo on the driver card model, not reflecting the optional driver signature.</p>	 <p><b>Rationale:</b> typo corrected, signature item 7 is in bracket (7.)</p>	<p>052</p>

<p><i>Annex 1 C req. 263 and 288</i></p>	<p>The driver card shall be able to store data related to the following faults detected by the recording equipment while the card was inserted:</p> <ul style="list-style-type: none"> <li>- Card fault (where this card is the subject of the event),</li> <li>- Recording equipment fault.</li> </ul> <p><b>Issue:</b> typo</p>	<p><i>The driver card shall be able to store data related to the following faults detected by the recording equipment while the card was inserted:</i></p> <ul style="list-style-type: none"> <li>- <i>Card fault (where this card is the subject of the <b>fault</b>),</i></li> <li>- <i>Recording equipment fault.</i></li> </ul> <p><b>Rationale:</b> typo corrected</p>	<p>056</p>
<p><i>Annex 1C req 396</i></p>	<p>(396) The plaque shall bear at least the following details: — name, address or trade name of the approved fitter or workshop,</p> <ul style="list-style-type: none"> <li>— characteristic coefficient of the vehicle, in the form 'w = ... imp/km',</li> <li>— constant of the recording equipment, in the form 'k = ... imp/km',</li> <li>— effective circumference of the wheel tyres in the form 'l = ... mm', — tyre size,</li> <li>— the date on which the characteristic coefficient of the vehicle and the effective circumference of the wheel tyres were measured,</li> <li>— the vehicle identification number,</li> <li>— the presence (or not) of an external GNSS facility,</li> <li>— the serial number of the external GNSS facility,</li> <li>— the serial number of the remote communication device,</li> </ul>	<p><i>Replace req. 396 with the following text:</i></p> <p><i>(396) The plaque shall bear at least the following details:</i></p> <ul style="list-style-type: none"> <li>— <i>name, address or trade name of the approved fitter or workshop,</i></li> <li>— <i>characteristic coefficient of the vehicle, in the form "w = ... imp/km",</i></li> <li>— <i>constant of the recording equipment, in the form "k = ... imp/km",</i></li> <li>— <i>effective circumference of the wheel tyres in the form "l = ... mm",</i></li> <li>— <i>tyre size,</i></li> <li>— <i>the date on which the characteristic coefficient of the vehicle and the effective circumference of the wheel tyres were measured,</i></li> <li>— <i>the vehicle identification number,</i></li> <li>— <i>the presence (or not) of an external GNSS facility,</i></li> <li>— <i>the serial number of the external GNSS facility, <b>if applicable</b>,</i></li> </ul>	<p>73</p>

	<ul style="list-style-type: none"> <li>– the serial number of all the seals in place,</li> <li>– the part of the vehicle where the adaptor, if any, is installed,</li> <li>– 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,</li> <li>– a description of the colour of the cable between the adaptor and that part of the vehicle providing its incoming impulses,</li> <li>– the serial number of the embedded motion sensor of the adaptor.</li> </ul> <p><b>issue:</b> Some required information may not exist (in case of internal GNSS facility for example)</p>	<ul style="list-style-type: none"> <li>– the serial number of the remote communication device, <b>if any,</b></li> <li>– the serial number of all the seals in place,</li> <li>– the part of the vehicle where the adaptor, if any, is installed,</li> <li>– 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,</li> <li>– a description of the colour of the cable between the adaptor and that part of the vehicle providing its incoming impulses,</li> </ul> <p>the serial number of the embedded motion sensor of the adaptor.</p> <p><b>rationale:</b> GNSS or remote communication facilities may be internal to the VU</p>	
<p>Annex 1 C Req. 398</p>	<p>(398) The following parts shall be sealed:</p> <ul style="list-style-type: none"> <li>– Any connection which, if disconnected, would cause undetectable alterations to be made or undetectable data loss (this may e.g. apply for the motion sensor fitting on the gearbox, the adaptor for M1/N1 vehicles, the external GNSS connection or the vehicle unit);</li> <li>– The installation plaque, unless it is attached in such a way that it cannot be removed without the markings thereon being destroyed.</li> </ul> <p><b>issue:</b> the use of certified seals is not required</p>	<p>Add the following requirement:</p> <p><b>(398a) The seals mentioned above shall be certified according to the standard EN 16882:2016.</b></p> <p><b>Rationale:</b> As seal standard EN 16882 is now published, the use of certified seals is mandatory</p>	<p>074</p>



<p>Annex 1 C Req. 401</p>	<p>Req 401: [...] This unique identification number is defined as: MMNNNNNN by non-removable marking, with MM as unique manufacturer identification (database registration to be managed by EC) and NNNNNN seal alpha-numeric number, unique in the manufacturer domain.</p> <p>Appendix 1 (Type definition): 2.71. ExtendedSealIdentifier Generation 2: The extended seal identifier uniquely identifies a seal (Annex 1C requirement 401). ExtendedSealIdentifier ::= SEQUENCE{ manufacturerCode OCTET STRING (SIZE(2)), sealIdentifier OCTET STRING (SIZE(6)) } manufacturerCode is a code of the manufacturer of the seal. sealIdentifier is an identifier for the seal which is unique for the manufacturer.</p> <p><b>Issue:</b> divergence with ISO 16882 where the seal alpha-numeric number is of 8 ciphers.</p>	<p>Req 401: [...] 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.</p> <p>Appendix 1 (Type definition): 2.71. ExtendedSealIdentifier Generation 2: The extended seal identifier uniquely identifies a seal (Annex 1C 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.</p> <p><b>Also TCS_162 to modify accordingly!</b></p> <p><b>Rationale:</b> Annex 1C to be updated in the way that the unique seal alpha-numeric number is increased to NNNNNNNN in order to be in line with ISO 16882.</p>	<p>074</p>
-------------------------------	---	--	------------

<p>Annec 1 C Req. 403</p>	<p>(403) Seals manufacturers shall be registered in a dedicated database and shall make their identification seals numbers public through a procedure to be established by the European Commission.</p> <p><b>issue:</b> this shall be done only for certified seals</p>	<p>(403) Seals manufacturers shall be registered in a dedicated database <b>when they get a seal model certified according EN 16882:2016</b> and shall make their identification seals numbers public through a procedure to be established by the European Commission.</p> <p><b>Rationale:</b> As seal standard EN 16882 is now published, the use of certified seals is mandatory</p>	<p>074</p>
<p>Annec 1 C Req. 404</p>	<p>(404) Approved workshops and vehicle manufacturers shall, in the frame of Regulation (EU) No 165/2014, only use seals from those of the seals manufacturers listed in the data base mentioned above.</p> <p><b>issue:</b> No requirement to used certified seals for workshops</p>	<p>(404) Approved workshops and vehicle manufacturers shall, in the frame of Regulation (EU) No 165/2014, only use seals <b>certified according EN 16882:2016</b> from those of the seals manufacturers listed in the data base mentioned above.</p> <p><b>Rationale:</b> As seal standard EN 16882 is now published, the use of certified seals is mandatory</p>	<p>074</p>
<p>Annex 1C</p>	<p><b>6.2 Check of new or repaired instruments</b></p> <p><b>Issue:</b> wording unclear, instruments is not defined</p>	<p><b>6.2 Check of new or repaired <b>components</b></b></p> <p><b>Rationale:</b> same wording as definition "oo" repairs.</p>	<p>075</p>
<p>Annex 1C chapter 8.1</p>	<p>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 remote communication facility to the VU. The paper, for use by the recording equipment, shall be considered as a component of the recording equipment.</p>	<p>Replace current text (until req. 425) by:</p> <p>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</p>	<p>77</p>

	<p>Any manufacturer may ask for type approval of its component with any type of motion sensor, external GNSS facility and vice versa, provided each component complies with the requirements of this annex. Alternately, manufacturers may also ask for type approval of recording equipment.</p> <p><b>issue:</b> description not enough precise for TA authorities</p>	<p><i>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.</i></p> <p><i>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.</i></p> <p><i>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.</i></p> <p><i>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.</i></p> <p><b>Rationale:</b> more precise descriptions of limits and duties.</p>	
Annex 1C req. 427	(427) Member States type approval authorities will	Replace requirement 427 with:	77

	<p>not grant a type approval certificate as long as they do not hold:</p> <ul style="list-style-type: none"> <li>– a security certificate,</li> <li>– a functional certificate,</li> <li>– and an interoperability certificate</li> </ul> <p>for the recording equipment or the tachograph card, subject of the request for type approval.</p> <p><b>Issue:</b> not all components require interoperability or security certification for the type approval</p>	<p><i>(427) Member States type approval authorities will not grant a type approval certificate as long as they do not hold:</i></p> <ul style="list-style-type: none"> <li>– a security certificate <i>(if requested by this Annex),</i></li> <li>– a functional certificate,</li> <li>– and an interoperability certificate <i>(if requested by this Annex)</i></li> </ul> <p><i>for the recording equipment or the tachograph card, subject of the request for type approval.</i></p> <p><b>Rationale:</b> solve type approval potential issues</p>	
<p>Appendix 1 2. Data Type Definition</p>	<p>Issue: there is a need to clarify the record length according GEN1/GEN2.</p>	<p>2. Data Type Definitions</p> <p><i>For any of the following data types, the default value for an "unknown" or a "not applicable" content will consist in filling the data element with 'FF' bytes.</i></p> <p><i>All data types are used for Generation 1 and Generation 2 applications unless otherwise specified.</i></p> <p><i>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 1C requirement numbers related to such data types cover both Generation 1 and</i></p>	<p>089</p>

		<p><i>Generation 2 applications.</i></p> <p><b>Rationale:</b> clarification</p>	
<p>App.1 2.19</p>	<p><b>2.19 CardEventData</b></p> <p>Information, stored in a driver or workshop card, related to the events associated with the card holder (Annex 1C requirements 260, 285, 318 and 341).</p> <pre>CardEventData ::= SEQUENCE SIZE (6) OF { cardEventRecords          SET SIZE (NoOfEventsPerType) OF CardEventRecord } </pre> <p><b>CardEventData</b> 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).</p> <p><b>cardEventRecords</b> is a set of event records of a given event type (or category for security breach attempts events).</p> <p><b>Issue: there is no distinction between Gen1 and Gen2</b></p>	<p>2.19 CardEventData</p> <p><b>Generation 1:</b></p> <p>Information, stored in a driver or workshop card, related to the events associated with the card holder (Annex 1C requirements 260 and 318).</p> <pre>CardEventData ::= SEQUENCE SIZE (6) OF { cardEventRecords SET SIZE (NoOfEventsPerType) OF CardEventRecord } </pre> <p><b>CardEventData</b> 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).</p> <p><b>cardEventRecords</b> is a set of event records of a given event type (or category for security breach attempts events).</p> <p><b>Generation 2:</b></p> <p>Information, stored in a driver or</p>	<p>96</p>

		<p>workshop card, related to the events associated with the card holder (Annex 1C requirements 285 and 341).</p> <pre> CardEventData ::= SEQUENCE SIZE(11) OF {     cardEventRecords         SET SIZE(NoOfEventsPerType) OF             CardEventRecord     } </pre> <p><b>CardEventData</b> 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).</p> <p><b>cardEventRecords</b> is a set of event records of a given event type (or category for security breach attempts events).</p> <p><b>Rationale:</b> card events data structure is different between Gen1 and Gen2.</p>	
<p>App. 1 2.30</p>	<p>Value assignment: (see this Annex chapter VII).</p> <p><b>Issue:</b> typo following a change in the numeration</p>	<p>Value assignment: (see this Annex chapter 7).</p> <p><b>Rationale:</b> typo corrected</p>	<p>099</p>

<p>App.1, 2.61 DriverCardApplicationIdentification</p>	<p>2.61 DriverCardApplicationIdentification ... Generation 2: DriverCardApplicationIdentification ::= SEQUENCE {     typeOfTachographCardId EquipmentType,     cardStructureVersion CardStructureVersion,     noOfEventsPerType NoOfEventsPerType,     noOfFaultsPerType NoOfFaultsPerType,     activityStructureLength CardActivityLengthRange,     noOfCardVehicleRecords NoOfCardVehicleRecords,     noOfCardPlaceRecords NoOfCardPlaceRecords,     noOfGNSSADRecords NoOfGNSSADRecords,     noOfSpecificConditionRecords NoOfSpecificConditionRecords } 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.  <b>issue:</b> The record of the Vehicle Units is missing in the data structure</p>	<p>2.61 DriverCardApplicationIdentification ... Generation 2: 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.  <b>Rationale</b> missing record added.</p>	<p>111</p>
<p>App. 1 2.63</p>	<p><b>Issue:</b> Revision of DSRC data</p>	<p>Replace existing definition 2.63 with 2.63 Reserved for Future Use</p>	<p>112</p>

		<p><i>Update also the table of contents</i></p> <p><b>Rationale:</b> See document on payload changes</p>	
<p><i>App.1, 2.67 EquipmentType</i></p>	<p>(text above)...</p> <p>Generation 2:</p> <p>The same values as in generation 1 are used with the following additions:</p> <p>--GNSS Facility (8),</p> <p>--Remote Communication Module (9),</p> <p>--ITS interface module (10),</p> <p>--Plaque (11), -- may be used in SealRecord</p> <p>--M1/N1 Adapter (12), -- may be used in SealRecord</p> <p>--European Root CA (ERCA) (13),</p> <p>--Member State CA (MSCA) (14),</p> <p>--External GNSS connection (15), -- may be used in SealRecord</p> <p>--Unused (16), -- used in SealDataVu</p> <p>--RFU (17..255)</p> <p>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.</p> <p><b>Issue:</b> it is not possible to distinguish between digital certificates for Mutual Authentication and digital certificates for signing</p>	<p>(text above) ...</p> <p>Generation 2:</p> <p>The same values as in generation 1 are used with the following additions:</p> <p>--GNSS Facility (8),</p> <p>--Remote Communication Module (9),</p> <p>--ITS interface module (10),</p> <p>--Plaque (11), -- may be used in SealRecord</p> <p>--M1/N1 Adapter (12), -- may be used in SealRecord</p> <p>--European Root CA (ERCA) (13),</p> <p>--Member State CA (MSCA) (14),</p> <p>--External GNSS connection (15), -- may be used in SealRecord</p> <p>--Unused (16), -- used in SealDataVu</p> <p>--Driver Card (Sign) (17), -- only to be used in the CHA field of a signing certificate</p> <p>--Workshop Card (Sign) (18), -- only to be used in the CHA field of a signing certificate</p> <p>--Vehicle Unit (Sign) (19), -- only to be used in the CHA field of a signing certificate</p> <p>--RFU (20..255)</p>	<p>113</p>



		<p>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.</p> <p>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.</p> <p><b>Rationale:</b> the devices can now check that the proper certificate is used</p>	
App. 1 2.70	<b>Issue:</b> A new nomenclature of Event&Faults is introduced by the amendements	<b>Rationale:</b> in Appendix 1, table 2.70 is to be updated, see document for Event&Faults change proposals	115
App. 1 Section 2.86	<p>The first choice is suitable to reference the public key of a Vehicle Unit or of a tachograph card.</p> <p><b>Issue:</b> text does not comprise EGFs</p>	<p>The first choice is suitable to reference the public key of a Vehicle Unit, of a tachograph card or of an external GNSS facility.</p> <p><b>Rationale:</b> missing EGFs added</p>	120
Annex IC Appendix 1 Chapter 2.92	<p>MAC Mac 16 OCTET STRING (SIZE (12))</p> <p><b>Issue:</b> typo</p>	<p>MAC Mac 16 OCTET STRING (SIZE (16))</p> <p><b>Rationale:</b> typo corrected</p>	121
App. 1 2.160	<b>Issue:</b> Revision of DSRC data	<p>Replace existing definition 2.160 with</p> <p>2.160 Reserved for Future Use</p> <p>Update also the table of contents</p> <p><b>Rationale:</b> See document on payload changes</p>	138
App 1	Code for a combined date and time field, where the date and time are expressed as seconds past	Code for a combined date and time field, where the date and time are expressed as seconds past	139

<p>Req 2.162. TimeReal</p>	<p>00h.00m.00s. on 1 January 1970 GMT.</p> <p><b>Value assignment — Octet Aligned:</b> Number of seconds since midnight 1 January 1970 GMT.</p> <p><b>Issue:</b> GMT is not correct and is not used elsewhere.</p>	<p>00h.00m.00s. on 1 January 1970 UTC.</p> <p><b>Value assignment — Octet Aligned:</b> Number of seconds since midnight 1 January 1970 UTC.</p> <p><b>Rationale:</b> typo corrected, time reference harmonized.</p>	
<p>App1 Req 2.179 VuCardRecord</p>	<p><b>2.179 VuCardRecord</b></p> <p>Generation 2:</p> <p>Information, stored in a vehicle unit, about a tachograph card used (Annex 1C requirement 132).</p> <pre>VuCardRecord ::= SEQUENCE {     cardExtendedSerialNumber ExtendedSerialNumber,     cardPersonaliserID       OCTET STRING(SIZE(1)),     typeofTachographCardID  EquipmentType,     cardStructureVersion     CardStructureVersion,     cardNumber               CardNumber }</pre> <p><b>cardExtendedSerialNumber</b> as read from the file EF_ICC under the MF of the card.</p> <p><b>cardPersonaliserID</b> as read from the file EF_ICC under the MF of the card.</p> <p><b>typeofTachographCardId</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2</p> <p><b>cardStructureVersion</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2.</p>	<p><b>2.179VuCardRecord</b></p> <p>Generation 2:</p> <p>Information, stored in a vehicle unit, about a tachograph card used (Annex 1C requirement 132).</p> <pre>VuCardRecord ::= SEQUENCE {     cardNumberAndGenerationInformation FullCardNumberAndGeneration,     cardExtendedSerialNumber ExtendedSerialNumber,     cardStructureVersion CardStructureVersion,     cardNumber CardNumber }</pre> <p><b>cardNumberAndGenerationInformation</b> is the full card number and generation of the card used (data type 2.74).</p> <p><b>cardExtendedSerialNumber</b> as read from the file EF_ICC under the MF of the card.</p> <p><b>cardStructureVersion</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2.</p> <p><b>cardNumber</b> as read from the file EF_Identification under the DF_Tachograph_G2.</p>	<p>145</p>

	<p><b>cardNumber</b> as read from the file EF_Identification under the DF_Tachograph_G2.</p> <p><b>2.179 VuCardRecord</b>  Generation 2:  Information, stored in a vehicle unit, about a tachograph card used (Annex 1C requirement 132).</p> <pre>VuCardRecord ::= SEQUENCE {   cardExtendedSerialNumber ExtendedSerialNumber,   cardPersonaliserID        OCTET STRING (SIZE (1)),   typeOfTachographCardID   EquipmentType,   cardStructureVersion      CardStructureVersion,   cardNumber                CardNumber }</pre> <p><b>cardExtendedSerialNumber</b> as read from the file EF_ICC under the MF of the card.  <b>cardPersonaliserID</b> as read from the file EF_ICC under the MF of the card.  <b>typeOfTachographCardID</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2.  <b>cardStructureVersion</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2.  <b>cardNumber</b> as read from the file EF_Identification under the DF_Tachograph_G2.</p> <p><b>Issue:</b> As it is specified today, cards from different countries could have exactly the same Card numbers.</p> <p>In addition, last card insertion time is missing in the VuCardRecord, so block 23.1 cannot be printed.</p>	<p><b>2.179 VuCardRecord</b>  Generation 2:  Information, stored in a vehicle unit, about a tachograph card used (Annex 1C requirement 132).</p> <pre>VuCardRecord ::= SEQUENCE {   cardNumberAndGenerationInformation FullCardNumberAndGeneration,   cardExtendedSerialNumber           ExtendedSerialNumber,   cardStructureVersion               CardStructureVersion,   cardNumber                         CardNumber }</pre> <p><b>cardNumberAndGenerationInformation</b> is the full card number and generation of the card used (data type 2.74).  <b>cardExtendedSerialNumber</b> as read from the file EF_ICC under the MF of the card.  <b>cardStructureVersion</b> as read from the file EF_Application_Identification under the DF_Tachograph_G2.  <b>cardNumber</b> as read from the file EF_Identification under the DF_Tachograph_G2.</p> <p><b>Rationale:</b> risk of same number is suppressed, block 23.1 can be printed</p>	
<p>App.1, 2.234  WorkshopCardApplicationIdentification</p>	<p>2.234 WorkshopCardApplicationIdentification  ...  Generation 2:  WorkshopCardApplicationIdentification ::= SEQUENCE {    typeOfTachographCardId EquipmentType,    cardStructureVersion CardStructureVersion,    noOfEventsPerType NoOfEventsPerType,    noOfFaultsPerType NoOfFaultsPerType,    activityStructureLength CardActivityLengthRange,    noOfCardVehicleRecords NoOfCardVehicleRecords,</p>	<p>2.234 WorkshopCardApplicationIdentification  ...  Generation 2:  WorkshopCardApplicationIdentification ::= SEQUENCE {    typeOfTachographCardId EquipmentType,    cardStructureVersion CardStructureVersion,    noOfEventsPerType NoOfEventsPerType,    noOfFaultsPerType NoOfFaultsPerType,    activityStructureLength CardActivityLengthRange,    noOfCardVehicleRecords NoOfCardVehicleRecords,</p>	<p>166</p>

	<pre> noOfCardPlaceRecords    NoOfCardPlaceRecords, noOfCalibrationRecords  NoOfCalibrationRecords, noOfGNSSADRecords       NoOfGNSSADRecords, noOfSpecificConditionRecords NoOfSpecificConditionRecords } </pre> <p>In addition to generation 1 the following data elements are used:</p> <p>noOfGNSSADRecords is the number of GNSS accumulated driving records the card can store.</p> <p>noOfSpecificConditionRecords is the number of specific condition records the card can store.</p> <p><b>issue:</b> The record of the Vehicle Units is missing in the data structure</p>	<pre> noOfCardPlaceRecords NoOfCardPlaceRecords, noOfCalibrationRecords    NoOfCalibrationRecords, noOfGNSSADRecords  NoOfGNSSADRecords, noOfSpecificConditionRecords NoOfSpecificConditionRecords, noOfCardVehicleUnitRecords NoOfCardVehicleUnitRecords } </pre> <p>In addition to generation 1 the following data elements are used:</p> <p>noOfGNSSADRecords is the number of GNSS accumulated driving records the card can store.</p> <p>noOfSpecificConditionRecords is the number of specific condition records the card can store.</p> <p>noOfCardVehicleUnitRecords is the number of vehicle units used records the card can store.</p> <p><b>Rationale:</b> missing record added.</p>	
App. 2 Abbreviations	<b>Issue:</b> missing abbreviation	<p>Add:</p> <p><b>CHA</b> : Certificate Holder Authorisation</p> <p><b>Rationale:</b> missing abbreviation added</p>	175
App. 2 Abbreviations	<b>Issue:</b> missing abbreviation	<p>Add:</p> <p><b>DO</b> : Data Object</p> <p><b>Rationale:</b> missing abbreviation added</p>	175
App.2 TCS_24	<p>...</p> <p>The access rules for the file system, i.e. the SELECT, READ BINARY and UPDATE BINARY</p>	<p>...</p> <p>The access rules for the file system, i.e. the SELECT, READ BINARY and UPDATE BINARY</p>	180

	<p>command, are specified in chapter 4. The access rules for the remaining commands are specified in the following tables.</p> <p><b>Issue:</b> the text can generate ambiguities.</p>	<p>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.</p> <p><b>Rationale:</b> no more ambiguity.</p>	
App.2 TCS_25	<p>PSO: Hash of File command do not exist</p> <p><b>Issue:</b> typo</p>	<p>In the table TCS_25, replace PSO: Hash of File with: <b>PERFORM HASH of FILE</b></p> <p><b>Rationale:</b> typo corrected</p>	181
App.2 TCS_26	<p>PSO: Hash of File command do not exist</p> <p><b>Issue:</b> typo</p>	<p>In the table TCS_26, replace PSO: Hash of File with: <b>PERFORM HASH of FILE</b></p> <p><b>Rationale:</b> typo corrected</p>	182
App.2 TCS_27 (First)	<p>PSO: Hash of File command do not exist</p> <p><b>Issue:</b> typo</p>	<p>In the table TCS_27, replace PSO: Hash of File with: <b>PERFORM HASH of FILE</b></p> <p><b>Rationale:</b> typo corrected</p>	183
App.2 TCS_27 (second)	<p>See at the end current TCS_27 as published</p> <p><b>Issue:</b> a row is missing in the table</p>	<p><b>See at the end new TCS_27</b></p> <p><b>Rationale:</b> for completeness the row has been added</p>	182
App.2 TCS_29	...	...	184

	<p>67 00 Wrong length (wrong Lc or Le)  68 82 Secure messaging not supported  68 83 Last command of the chain expected</p> <p><b>Issue:</b> The status word 6882 is never referenced elsewhere.</p>	<p>67 00 Wrong length (wrong Lc or Le)  <del>68 82 Secure messaging not supported</del>  68 83 Last command of the chain expected</p> <p>+ addition after the table:</p> <p><i>Additional status words as defined in ISO/IEC 7816-4 can be returned, if their behavior is not explicitly mentioned in this appendix.</i></p> <p><i>For example the following status words can be optionally returned:</i></p> <p><i>6881: Logical channel not supported</i>  <i>6882: Secure messaging not supported</i></p> <p><b>Rationale:</b> Opening to possible other standardized status word response.</p>	
App.2 TCS 38	<b>Issue:</b> Error in error codes (sic!)	<p>Replace:  — If the selected application is considered corrupted (integrity error is detected within the file attributes), the processing state returned is '6400' or '6581'.  By:  If the selected application is considered corrupted (integrity error is detected within the file attributes), the processing state returned is '6400' or <b>'6500'</b>.</p> <p><b>Rationale:</b> Error corrected</p>	187

App.2 TCS 41	<b>Issue:</b> Error in error codes (sic!)	<p><b>Replace:</b></p> <p>— If the selected application is considered corrupted (integrity error is detected within the file attributes), the processing state returned is '6400' or '6581'.</p> <p><b>By:</b></p> <p>If the selected application is considered corrupted (integrity error is detected within the file attributes), the processing state returned is '6400' or '6500'.</p> <p><b>Rationale:</b> Error corrected</p>	187
App.2 TCS 43	<b>Issue:</b> Error in error codes (sic!)	<p><b>Replace</b></p> <p>If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is '6400' or '6581'.</p> <p><b>By:</b></p> <p>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'.</p> <p><b>Rationale:</b> Error corrected</p>	188
App.2 TCS_45 and TCS_46	<p>See at the end for current text in the table</p> <p><b>Issue:</b> error in the card file access security conditions</p>	<p>See at the end new text for the table</p> <p><b>Rationale:</b> error corrected and ambiguity clarified</p>	189
App.2 TCS 50	<b>Issue:</b> Error in error codes (sic!)	<p><b>Replace:</b></p> <p>— If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing</p>	192

		<p>state returned is '6400' or '6581'.</p> <p>By:</p> <p>– 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'.</p> <p><b>Rationale:</b> Error corrected</p>													
App.2 TCS 52	<p><b>Issue:</b> Explanation was a particular case and could be unclear.</p>	<p>Replace the last row with</p> <table border="1"> <thead> <tr> <th>Byte</th> <th>Length</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td colspan="4">-----</td> </tr> <tr> <td>Le</td> <td>1</td> <td>'xxh'</td> <td>As specified in ISO/IEC 7816-4</td> </tr> </tbody> </table> <p>Add the following explanation before TCS_53:</p> <p>In case of T=0 the card assumes the value Le = '00h' if no secure messaging is applied.</p> <p>In case of T = 1 the processing state returned is '6700' if Le='01h'.</p> <p><b>Rationale:</b> Clearer specification</p>	Byte	Length	Value	Description	-----				Le	1	'xxh'	As specified in ISO/IEC 7816-4	192
Byte	Length	Value	Description												
-----															
Le	1	'xxh'	As specified in ISO/IEC 7816-4												
App.2 TCS 53	<p><b>Issue:</b> Error in error codes (sic!)</p>	<p>Replace:</p> <p>– If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is '6400' or '6581'.</p>	193												





		<p><i>By:</i></p> <p>– 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'.</p> <p><i>Rationale: Error corrected</i></p>	
App.2 TCS 63	<i>Issue: Error in error codes (sic!)</i>	<p><i>Replace:</i></p> <p>– If an integrity error is detected within the file attributes, the card shall consider the file as corrupted and unrecoverable, the processing state returned is '6400' or '6581'.</p> <p><i>By:</i></p> <p>– 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'.</p> <p><i>Rationale: Error corrected</i></p>	198
App. 2 TCS 72	<p>TCS 72: The PIN entered by the user must be ASCII encoded ...</p> <p><b>Issue:</b> typo</p>	<p><i>TCS 72: The PIN entered by the user must be ASCII encoded ...</i></p> <p><i>Rationale: typo corrected</i></p>	201
App. 2 TCS_95	<b>issue:</b> behavior unclear according the DF generation	<p><i>Replace:</i></p> <p><i>TCS_95 If the INTERNAL AUTHENTICATE command is successful, the current session key, if existing, is erased and no longer available. In order to have a new session key available, the EXTERNAL AUTHENTICATE command for the</i></p>	205

		<p>generation 1 authentication mechanism must be successfully performed.</p> <p>By:</p> <p>TCS_95 If the INTERNAL AUTHENTICATE command is successful, the current <b>generation 1</b> session key, if existing, is erased and no longer available. In order to have a new <b>generation 1</b> session key available, the EXTERNAL AUTHENTICATE command for the generation 1 authentication mechanism must be successfully performed.</p> <p>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.</p> <p><b>Rationale:</b> behaviour clearer</p>	
App. 2 TCS_97	<b>issue:</b> behavior unclear according the DF generation	<p>Relpace:</p> <p>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.</p> <p>By:</p> <p>TCS_97 The command variant for the second generation VU-card mutual authentication can be performed in the MF, DF Tachograph and DF</p>	206

		<p>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.</p> <p>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.</p> <p><b>Rationale:</b> behaviour clearer</p>									
App.2 TCS 101	<b>Issue:</b> missing field	<p>Add the following row</p> <table border="1"> <thead> <tr> <th>Byte</th> <th>Length</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>5+L+1</td> <td>1</td> <td>'00h'</td> <td>As specified in ISO/IEC 7816-4</td> </tr> </tbody> </table> <p><b>Rationale:</b> Field added</p>	Byte	Length	Value	Description	5+L+1	1	'00h'	As specified in ISO/IEC 7816-4	207
Byte	Length	Value	Description								
5+L+1	1	'00h'	As specified in ISO/IEC 7816-4								
App.2 TCS_121	<p>The temporarily stored hash of file value shall be deleted if a new hash of file value is computed by means of the PSO: Hash of File command, if a DF is selected, and if the tachograph card is reset.</p> <p><b>Issue:</b> typo</p>	<p>Replace with:</p> <p>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.</p>	212								

		<b>Rationale:</b> typo corrected	
App.2 TCS_123	<p>The Tachograph Generation 2 application shall support SHA-1 and SHA-2 (256, 384 and 512 bits).</p> <p><b>Issue:</b> SHA-1 does not have to be supported in Gen2 application</p>	<p>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.</p> <p><b>Rationale:</b> erroneous requirement removed</p>	212
App.2 TCS_124	<p>See at the end for current text in the table</p> <p><b>Issue:</b> the text can generate ambiguities</p>	<p>See at the end new text for the table</p> <p><b>Rationale:</b> no more ambiguity</p>	212
App.2, Section 3.5.14	<p>...</p> <p>Other types of tachograph cards may or may not implement this command, but shall not have a signature key. Therefore these cards cannot perform the command successfully, but terminate with a suitable error code.</p> <p>...</p> <p><b>Issue:</b> The statement concerning the signature key is true for the Gen2 application but not for the Gen1 application.</p>	<p>...</p> <p>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.</p> <p>...</p> <p><b>Rationale:</b> Erroneous statement corrected.</p>	212
App.2 TCS_133	<p>See at the end for current text in the table</p> <p><b>Issue:</b> error in the table</p>	<p>See at the end for current text in the table</p> <p><b>Rationale:</b> error corrected</p>	214
App.2 TCS_138	<b>Issue:</b> missing field	Add the following row	215

		<p>Byte   Length   Value   Description</p> <p>-----</p> <p>5+L+1   1   '00h'   As specified in ISO/IEC 7816-4</p> <p><b>Rationale:</b> Field added</p>																																																																																																																																																		
<p>App.2 TCS_139</p>	<p><b>Issue:</b> When a Control or Workshop card is expired it would be advisable to block its functionality to decrypt and check DSRC messages. This would limit possible negative effects linked to expired Control and Workshop cards that may remain in circulation. For that reason it is proposed to add an error code in requirement TCS_139 of Appendix 2.</p>	<p>Add the following bullet point at the end of TCS_139:</p> <p>'6985' indicates that the 4-byte time stamp provided in the command data field is earlier than cardValidityBegin or later than cardExpiryDate.</p> <p><b>Rationale:</b> limitation on expired control card</p>	<p>216</p>																																																																																																																																																	
<p>App.2 TCS_154</p>	<table border="1"> <thead> <tr> <th>File / Data element</th> <th>No of Records</th> <th>Size (bytes) Min</th> <th>Max</th> <th>Default Values</th> </tr> </thead> <tbody> <tr> <td>EF Tachograph_G2</td> <td>20266</td> <td>40314</td> <td></td> <td></td> </tr> <tr> <td>EF Application_Identification</td> <td>15</td> <td>15</td> <td></td> <td></td> </tr> <tr> <td>EF DriverCardApplicationIdentification</td> <td>15</td> <td>15</td> <td></td> <td></td> </tr> <tr> <td>  typeOfTachographCardId</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  cardStructureVersion</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfEventsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  noOfFaultsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  activityStructureLength</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfCardVehicleRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfCardPlaceRecords</td> <td>2</td> <td>2</td> <td>{00}</td> <td></td> </tr> <tr> <td>  noOfGNSSADRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfSpecificConditionRecords</td> <td>2</td> <td>2</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF CardMA_Certificate</td> <td>204</td> <td>341</td> <td></td> <td></td> </tr> </tbody> </table> <p><b>issue:</b> The record of the Vehicle Units is missing in the data structure</p>	File / Data element	No of Records	Size (bytes) Min	Max	Default Values	EF Tachograph_G2	20266	40314			EF Application_Identification	15	15			EF DriverCardApplicationIdentification	15	15			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}		noOfGNSSADRecords	2	2	{00 00}		noOfSpecificConditionRecords	2	2	{00}		EF CardMA_Certificate	204	341			<table border="1"> <thead> <tr> <th>File / Data element</th> <th>No of Records</th> <th>Size (bytes) Min</th> <th>Max</th> <th>Default Values</th> </tr> </thead> <tbody> <tr> <td>EF Tachograph_G2</td> <td>20268</td> <td>40316</td> <td></td> <td></td> </tr> <tr> <td>EF Application_Identification</td> <td>15</td> <td>15</td> <td></td> <td></td> </tr> <tr> <td>EF DriverCardApplicationIdentification</td> <td>15</td> <td>15</td> <td></td> <td></td> </tr> <tr> <td>  typeOfTachographCardId</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  cardStructureVersion</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfEventsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  noOfFaultsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>  activityStructureLength</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfCardVehicleRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfCardPlaceRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfGNSSADRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfSpecificConditionRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>  noOfCardVehicleUnitRecords</td> <td>2</td> <td>2</td> <td>{0000}</td> <td></td> </tr> <tr> <td>EF CardMA_Certificate</td> <td>204</td> <td>341</td> <td></td> <td></td> </tr> </tbody> </table> <p><b>Rationale:</b> missing record added.</p>	File / Data element	No of Records	Size (bytes) Min	Max	Default Values	EF Tachograph_G2	20268	40316			EF Application_Identification	15	15			EF DriverCardApplicationIdentification	15	15			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	{0000}		EF CardMA_Certificate	204	341			<p>222</p>
File / Data element	No of Records	Size (bytes) Min	Max	Default Values																																																																																																																																																
EF Tachograph_G2	20266	40314																																																																																																																																																		
EF Application_Identification	15	15																																																																																																																																																		
EF DriverCardApplicationIdentification	15	15																																																																																																																																																		
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}																																																																																																																																																	
noOfGNSSADRecords	2	2	{00 00}																																																																																																																																																	
noOfSpecificConditionRecords	2	2	{00}																																																																																																																																																	
EF CardMA_Certificate	204	341																																																																																																																																																		
File / Data element	No of Records	Size (bytes) Min	Max	Default Values																																																																																																																																																
EF Tachograph_G2	20268	40316																																																																																																																																																		
EF Application_Identification	15	15																																																																																																																																																		
EF DriverCardApplicationIdentification	15	15																																																																																																																																																		
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	{0000}																																																																																																																																																	
EF CardMA_Certificate	204	341																																																																																																																																																		
<p>App.2 TCS_156</p>	<p>For the READ BINARY command with even INS byte: (PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR (SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)</p>	<p>For the READ BINARY command with even INS byte: <del>(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR (SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)</del></p>	<p>224</p>																																																																																																																																																	

	<p><b>Issue:</b> error in the card file access security conditions</p>	<p><b>Rationale:</b> error corrected</p>																																																																																																																																																												
<p>App.2 TCS_162</p>	<table border="1"> <thead> <tr> <th>File / Data element</th> <th>No of Records</th> <th>Size (Bytes) Min</th> <th>Max</th> <th>Default Values</th> </tr> </thead> <tbody> <tr> <td>DF Tachograph_G2</td> <td>17901</td> <td>47235</td> <td></td> <td></td> </tr> <tr> <td>EF Application_Identification</td> <td>17</td> <td>17</td> <td></td> <td></td> </tr> <tr> <td>EF WorkshopCardApplicationIdentification</td> <td>17</td> <td>17</td> <td></td> <td></td> </tr> <tr> <td>EF typeOfTachographCardId</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF cardStructureVersion</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfEventsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF noOfFaultsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF activityStructureLength</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfCardVehicleRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfCardPlaceRecords</td> <td>2</td> <td>2</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF noOfCalibrationRecords</td> <td>2</td> <td>2</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF noOfGNSSADRecords</td> <td>2</td> <td>2</td> <td>{00,00}</td> <td></td> </tr> <tr> <td>EF noOfSpecificConditionRecords</td> <td>2</td> <td>2</td> <td>{00,00}</td> <td></td> </tr> <tr> <td>EF CardMA_Certificate</td> <td>204</td> <td>341</td> <td></td> <td></td> </tr> </tbody> </table> <p>...</p> <p><b>issue:</b> The record of the Vehicle Units is missing in the data structure</p>	File / Data element	No of Records	Size (Bytes) Min	Max	Default Values	DF Tachograph_G2	17901	47235			EF Application_Identification	17	17			EF WorkshopCardApplicationIdentification	17	17			EF typeOfTachographCardId	1	1	{00}		EF cardStructureVersion	2	2	{00 00}		EF noOfEventsPerType	1	1	{00}		EF noOfFaultsPerType	1	1	{00}		EF activityStructureLength	2	2	{00 00}		EF noOfCardVehicleRecords	2	2	{00 00}		EF noOfCardPlaceRecords	2	2	{00}		EF noOfCalibrationRecords	2	2	{00}		EF noOfGNSSADRecords	2	2	{00,00}		EF noOfSpecificConditionRecords	2	2	{00,00}		EF CardMA_Certificate	204	341			<table border="1"> <thead> <tr> <th>File / Data element</th> <th>No of Records</th> <th>Size (Bytes) Min</th> <th>Max</th> <th>Default Values</th> </tr> </thead> <tbody> <tr> <td>DF Tachograph_G2</td> <td>17903</td> <td>47237</td> <td></td> <td></td> </tr> <tr> <td>EF Application_Identification</td> <td>19</td> <td>19</td> <td></td> <td></td> </tr> <tr> <td>EF WorkshopCardApplicationIdentification</td> <td>19</td> <td>19</td> <td></td> <td></td> </tr> <tr> <td>EF typeOfTachographCardId</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF cardStructureVersion</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfEventsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF noOfFaultsPerType</td> <td>1</td> <td>1</td> <td>{00}</td> <td></td> </tr> <tr> <td>EF activityStructureLength</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfCardVehicleRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfCardPlaceRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfCalibrationRecords</td> <td>2</td> <td>2</td> <td>{00 00}</td> <td></td> </tr> <tr> <td>EF noOfGNSSADRecords</td> <td>2</td> <td>2</td> <td>{00,00}</td> <td></td> </tr> <tr> <td>EF noOfSpecificConditionRecords</td> <td>2</td> <td>2</td> <td>{00,00}</td> <td></td> </tr> <tr> <td>EF noOfCardVehicleUnitRecords</td> <td>2</td> <td>2</td> <td>{00,00}</td> <td></td> </tr> <tr> <td>EF CardMA_Certificate</td> <td>204</td> <td>341</td> <td></td> <td></td> </tr> </tbody> </table> <p>...</p> <p><b>Rationale:</b> missing record added.</p>	File / Data element	No of Records	Size (Bytes) Min	Max	Default Values	DF Tachograph_G2	17903	47237			EF Application_Identification	19	19			EF WorkshopCardApplicationIdentification	19	19			EF typeOfTachographCardId	1	1	{00}		EF cardStructureVersion	2	2	{00 00}		EF noOfEventsPerType	1	1	{00}		EF noOfFaultsPerType	1	1	{00}		EF activityStructureLength	2	2	{00 00}		EF noOfCardVehicleRecords	2	2	{00 00}		EF noOfCardPlaceRecords	2	2	{00 00}		EF noOfCalibrationRecords	2	2	{00 00}		EF noOfGNSSADRecords	2	2	{00,00}		EF noOfSpecificConditionRecords	2	2	{00,00}		EF noOfCardVehicleUnitRecords	2	2	{00,00}		EF CardMA_Certificate	204	341			<p>230</p>
File / Data element	No of Records	Size (Bytes) Min	Max	Default Values																																																																																																																																																										
DF Tachograph_G2	17901	47235																																																																																																																																																												
EF Application_Identification	17	17																																																																																																																																																												
EF WorkshopCardApplicationIdentification	17	17																																																																																																																																																												
EF typeOfTachographCardId	1	1	{00}																																																																																																																																																											
EF cardStructureVersion	2	2	{00 00}																																																																																																																																																											
EF noOfEventsPerType	1	1	{00}																																																																																																																																																											
EF noOfFaultsPerType	1	1	{00}																																																																																																																																																											
EF activityStructureLength	2	2	{00 00}																																																																																																																																																											
EF noOfCardVehicleRecords	2	2	{00 00}																																																																																																																																																											
EF noOfCardPlaceRecords	2	2	{00}																																																																																																																																																											
EF noOfCalibrationRecords	2	2	{00}																																																																																																																																																											
EF noOfGNSSADRecords	2	2	{00,00}																																																																																																																																																											
EF noOfSpecificConditionRecords	2	2	{00,00}																																																																																																																																																											
EF CardMA_Certificate	204	341																																																																																																																																																												
File / Data element	No of Records	Size (Bytes) Min	Max	Default Values																																																																																																																																																										
DF Tachograph_G2	17903	47237																																																																																																																																																												
EF Application_Identification	19	19																																																																																																																																																												
EF WorkshopCardApplicationIdentification	19	19																																																																																																																																																												
EF typeOfTachographCardId	1	1	{00}																																																																																																																																																											
EF cardStructureVersion	2	2	{00 00}																																																																																																																																																											
EF noOfEventsPerType	1	1	{00}																																																																																																																																																											
EF noOfFaultsPerType	1	1	{00}																																																																																																																																																											
EF activityStructureLength	2	2	{00 00}																																																																																																																																																											
EF noOfCardVehicleRecords	2	2	{00 00}																																																																																																																																																											
EF noOfCardPlaceRecords	2	2	{00 00}																																																																																																																																																											
EF noOfCalibrationRecords	2	2	{00 00}																																																																																																																																																											
EF noOfGNSSADRecords	2	2	{00,00}																																																																																																																																																											
EF noOfSpecificConditionRecords	2	2	{00,00}																																																																																																																																																											
EF noOfCardVehicleUnitRecords	2	2	{00,00}																																																																																																																																																											
EF CardMA_Certificate	204	341																																																																																																																																																												
<p>App.3</p> <p>2. PICTOGRAM COMBINATIONS</p>	<p><b>issue:</b> Missing pictograms</p>	<p>Add the following combination of pictograms to "Events":</p> <p> - "Absence of position information from GNSS receiver or Communication error with the external GNSS facility"</p> <p> - "Communication error with the remote communication facility"</p>	<p>241</p>																																																																																																																																																											

		<b>Rationale:</b> These events were defined but the corresponding pictograms were not	
App. 4 PRT_014	Card holder identifications (of all cards inserted in the V)  <b>Issue:</b> typo	Card holder identifications (of all cards inserted in the VU)  <b>Rationale:</b> typo corrected	254
App. 8 Chapter 2	ISO 14230-2: Road Vehicles -Diagnostic Systems - Keyword Protocol 2000- Part 2 : Data Link Layer. First edition: 1999. Vehicles – Diagnostic.  <b>Issue:</b> an internal reminder was left in the final text.	ISO 14230-2: Road Vehicles -Diagnostic Systems - Keyword Protocol 2000- Part 2 : Data Link Layer. First edition: 1999. <del>Vehicles—Diagnostic.</del>  <b>Rationale:</b> internal reminder cancelled	284
App. 9 Chapter 1.1	a security certification, based on Common Criteria specifications, against a security target fully compliant with Appendix 10 to this Annex (To be completed/modified),  <b>Issue:</b> an internal reminder was left in the final text.	a security certification, based on Common Criteria specifications, against a security target fully compliant with Appendix 10 to this Annex ( <del>To be completed/modified</del> ),  <b>Rationale:</b> internal reminder cancelled	309
App. 9 Chapter 2	<b>Issue:</b> Some errors in requirement's identifications	See table at the end  <b>rationale:</b> requirements identification corrected	311
App. 9 Chapter 6	<b>issue:</b> functional tests missing + numeration error	See table at the end	331

		<b>rationale:</b> functional tests added and error corrected	
App. 9 Chapter 6 Point 4.1	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)  <b>Issue:</b> an internal reminder was left in the final text.	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)  <b>Rationale:</b> internal reminder cancelled	332
App. 9 Chapter 8	9.1 Interoperability tests between vehicle units and tachograph cards  <b>Issue:</b> typo	<b>8.1</b> Interoperability tests between vehicle units and tachograph cards  <b>Rationale:</b> typo corrected	335
App. 9 Chapter 8	9.2 Interoperability tests between vehicle units and motion sensors  <b>Issue:</b> typo	<b>8.2</b> Interoperability tests between vehicle units and motion sensors  <b>Rationale:</b> typo corrected	335
App. 9 Chapter 8	9.3 Interoperability tests between vehicle units and external GNSS facilities (when applicable)	<b>8.3</b> Interoperability tests between vehicle units and external GNSS facilities (when applicable)	336
App. 9 Chapter 8	Execute a typical activity scenario on the external GNSS.	Execute a typical activity scenario on the external GNSS facility.	336



point 8.3.2		<b>Rationale:</b> typo corrected	
	<b>Issue:</b> typo		
App.11 CSM_49	Vehicle units and tachograph cards shall support the SHA-256, SHA-384 and SHA-512 algorithms specified in [SHS].  <b>Issue:</b> the text can generate ambiguities	Vehicle units, tachograph cards and external GNSS facilities shall support the SHA-256, SHA-384 and SHA-512 algorithms specified in [SHS].  <b>Rationale:</b> no more ambiguity	361
App.11 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. This is shown in Figure 1 in section 9.1.7 as well.  <b>Issue:</b> the link Certificate validity period does not cover entirely the ERCA certificate validity period	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.  <b>Rationale:</b> Now for instance ERCA(2) cards can do data downloads from ERCA(1) VUs in the last three months of the ERCA(1) certificate validity period (for those VUs that are still valid).	362
App. 11 CSM_83	CSM_83: [...] Whenever a card key pair is generated, the party generating the key shall send the public key to the MSCA of the country in which it resides, in order to obtain a corresponding card certificate signed by the MSCA. [...]  <b>Issue:</b> wording is not clear, who is beyond "it" in "... in which <b>it</b> resides," the MSCA?	CSM_83: [...] Whenever a card key pair is generated, the party generating the key shall send the public key to the MSCA of the country in which the card holder resides, in order to obtain a corresponding card certificate signed by the MSCA. [...]  <b>Rationale:</b> Clarify it is the card holder who resides	365

<p>App. 11 CSM_88</p>	<p>The validity period of a Card_MA certificate shall be as follows:</p> <ul style="list-style-type: none"> <li>- For driver cards: 5 years</li> <li>- For company cards: 2 years</li> <li>- For control cards: 2 years</li> <li>- For workshop cards: 1 year</li> </ul> <p><b>Issue:</b> Control and company cards in the current system can have a 5 years validity. For the control cards of the new system, due to the period validity of some cryptographic keys used in the system and stored in their memory, it is required that their validity is 2 years. Anyhow, since company cards do not manage such keys, their validity can remain as in the current system.</p>	<p>The validity period of a Card_MA certificate shall be as follows:</p> <ul style="list-style-type: none"> <li>- For driver cards: 5 years</li> <li>- For company cards: 5 years</li> <li>- For control cards: 2 years</li> <li>- For workshop cards: 1 year</li> </ul> <p><b>Rationale:</b> Company cards back to 5 years validity. 2 years limitation was useless</p>	<p>365</p>
<p>App.11 CSM_91</p>	<p>When issued, tachograph cards shall contain the following cryptographic keys and certificates:</p> <ul style="list-style-type: none"> <li>- The Card_MA private key and corresponding certificate</li> <li>- For driver cards and workshop cards additionally: the Card_Sign private key and</li> </ul>	<p>When issued, tachograph cards shall contain the following cryptographic keys and certificates:</p> <ul style="list-style-type: none"> <li>- The Card_MA private key and corresponding certificate</li> <li>- For driver cards and workshop cards additionally: the Card_Sign private key and</li> </ul>	<p>366</p>

	<p>corresponding certificate</p> <ul style="list-style-type: none"> <li>- The MSCA_Card certificate containing the MSCA_Card.PK public key to be used for verification of the Card_MA certificate and Card_Sign certificate</li> <li>- The EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_Card certificate.</li> <li>- The EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the MSCA_Card certificate, if existing.</li> <li>- The link certificate linking these two EUR certificates, if existing.</li> </ul> <p><b>Issue:</b> some cards would not be able to trigger the data downloading functionality in the last three months of a VU certificate validity period.</p>	<p>corresponding certificate</p> <ul style="list-style-type: none"> <li>- The MSCA_Card certificate containing the MSCA_Card.PK public key to be used for verification of the Card_MA certificate and Card_Sign certificate</li> <li>- The EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_Card certificate.</li> <li>- The EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the MSCA_Card certificate, if existing.</li> <li>- The link certificate linking these two EUR certificates, if existing.</li> </ul> <p>- 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.</p> <p>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</p>	
--	--	---	--

		bullet of requirement 13) in Annex 1C.  <b>Rationale:</b> The added note self-explains how the problem has been solved.	
App. 11 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 and 11.4 of this Appendix.  <b>Issue:</b> typo	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 and 11.4 of this Appendix.  <b>Rationale:</b> typo corrected	366
App.11 Section 9.1.7	Current Figure 1.  ...  6. To save space, the difference in validity period between the Card_MA and Card_Sign certificates and between the VU_MA and VU_Sign certificates is shown only for the first generation.  <b>Issue:</b> Errors in Figure 1 and in the text regarding certificate validity length.	See at the end new Figure 1.  ...  6. To save space, the difference in validity period between the Card_MA and Card_Sign certificates and between the VU_MA and VU_Sign certificates is shown only for the first generation.  <b>Rationale:</b> Errors corrected.	367
App.11 CSM_106	'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'  <b>Issue:</b> typo	'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'  <b>Rationale:</b> typo corrected	370
App.11 CSM_107	Motion sensor manufacturers shall generate a	Each motion sensor manufacturer shall generate	370

	<p>random and unique pairing key KP for every motion sensor, and shall send each pairing key to a Member State Certificate Authority.</p> <p><b>Issue:</b> wording unclear</p>	<p><i>a random and unique pairing key KP for every motion sensor, and shall send each pairing key to <b>its</b> Member State Certificate Authority.</i></p> <p><b>Rationale:</b> no more ambiguity</p>	
App.11 CSM_108	<p>Motion sensor manufacturers shall generate a unique serial number for every motion sensor, and shall send all serial numbers to a Member State Certificate Authority.</p> <p><b>Issue:</b> wording unclear</p>	<p><b>Each motion sensor manufacturer</b> shall generate a unique serial number for every motion sensor, and shall send all serial numbers to <b>its</b> Member State Certificate Authority.</p> <p><b>Rationale:</b> no more ambiguity</p>	370
App.11 CSM_123	<p>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, and the Distinguished Encoding Rules (DER) according to [ISO 8825-1] shall be used for encoding.</p> <p><b>Issue:</b> the text included an unnecessary requirement and another necessary specification was missing.</p>	<p><i>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, <b>and the Distinguished Encoding Rules (DER) according to [ISO 8825-1] shall be used for encoding.</b></i></p> <p><b>Note:</b> This VU serial number shall be identical to the <b>vuSerialNumber</b> element of VuIdentification, see Appendix 1.</p> <p><b>Rationale:</b> unnecessary requirement removed and necessary specification added.</p>	373
App.11 CSM_135	The Distinguished Encoding Rules (DER)	<i>The Distinguished Encoding Rules (DER)</i>	375

	<p>according to [ISO 8825-1] shall be used to encode both ASN.1 data structures and (application specific) data objects within certificates.</p> <p>Note: this encoding results ... etc etc</p> <p><b>Issue:</b> the text can generate ambiguities</p>	<p>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.</p> <p>Note: this encoding results ... etc etc</p> <p><b>Rationale:</b> no more ambiguity</p>	
App.11 CSM_141	<p>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 type of equipment for which the certificate is intended.</p> <p><b>Issue:</b> it is not possible to distinguish between digital certificates for Mutual Authentication and digital certificates for signing</p>	<p>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).</p> <p><b>Rationale:</b> the devices can now check that the proper certificate is used</p>	376
App.11 CSM_146	<p>For vehicle units, the manufacturer, when requesting a certificate, may or may not know the manufacturer-specific serial number of the VU for which that certificate and the associated private key is intended. In the first case, the Certificate Holder Reference shall have the ExtendedSerialNumber data type specified in Appendix 1. In the latter case, the Certificate Holder Reference shall have the CertificateRequestID data type specified in</p>	<p>For vehicle units, the manufacturer, when requesting a certificate, may or may not know the manufacturer-specific serial number of the VU for which that certificate and the associated private key is intended. In the first case, the Certificate Holder Reference shall have the ExtendedSerialNumber data type specified in Appendix 1. In the latter case, the Certificate Holder Reference shall have the CertificateRequestID data type specified in</p>	377

	<p>Appendix 1.</p> <p><b>Issue:</b> A specification was missing.</p>	<p>Appendix 1.</p> <p><b>Note:</b> For a card certificate, the value of the CHR shall be equal to the value of the <code>cardExtendedSerialNumber</code> in EF_ICC; see Appendix 2. For an EGF certificate, the value of the CHR shall be equal to the value of the <code>sensorGNSSSerialNumber</code> in EF_ICC; see Appendix 14. For a VU certificate, the value of the CHR shall be equal to the <code>vuSerialNumber</code> element of <code>VuIdentification</code>, see Appendix 1, unless the manufacturer does not know the manufacturer-specific serial number at the time the certificate is requested.</p> <p><b>Rationale:</b> Specification added.</p>	
App.11 CSM_148	<p>The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate. The Certificate Effective Date shall be the date of the certificate generation.</p> <p><b>Issue:</b> Unecesasry limiting constraint, more details can be given in the certification authority policy. In addition it could generate conflicts with CSM_73 and CSM_84 (impossible to have the same CertificateEffectiveDate for two certificates if it is mandated to use their generation time in such a field).</p>	<p>The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate. <del>The Certificate Effective Date shall be the date of the certificate generation.</del></p> <p><b>Rationale:</b> <i>Unnecessary constraint removed.</i></p>	377
App.11 CSM_151	<p>When requesting a certificate, a requester shall send the following data to its Certificate Authority:</p> <ul style="list-style-type: none"> <li>- The Certificate Profile Identifier of the requested certificate</li> <li>- The Certificate Authority Reference expected to</li> </ul>	<p>When requesting a certificate, <del>an MSCA</del> shall send the following data to <del>the ERCA</del>:</p> <ul style="list-style-type: none"> <li>- The Certificate Profile Identifier of the requested certificate</li> <li>- The Certificate Authority Reference expected to</li> </ul>	377

	<p>be used for signing the certificate.</p> <ul style="list-style-type: none"> <li>- The Public Key to be signed</li> </ul> <p><b>Issue:</b> It was introduced a constraint for interactions between MSCAs and manufacturers/personaliser, but the kind of data communicated can be left up to them.</p>	<p>be used for signing the certificate.</p> <ul style="list-style-type: none"> <li>- The Public Key to be signed</li> </ul> <p><b>Rationale:</b> <i>Constraint kept only between ERCA and MSCAs (such data are already communicated within current MSCA certificate requests).</i></p>	
App.11 CSM_153	<p>In addition to the data in CSM_151, 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:</p> <ul style="list-style-type: none"> <li>- A manufacturer-specific identifier of the equipment type</li> <li>- 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.</li> <li>- The month and the year of equipment manufacturing or of the certificate request.</li> </ul> <p>The manufacturer shall ensure that this data is correct and that the certificate returned by the MSCA is inserted in the intended equipment.</p> <p><b>Issue:</b> according to the amendment for CSM_151 it is no longer "In addition to the data in CSM_151". Moreover, according to the definition of ExtendedSerialNumber in Appendix1 its relevant field 'type' is defined as 'EquipmentType' so, compared to Gen1 DT, is no</p>	<p><del>In addition to the data in CSM_151, a</del>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:</p> <p><del>A manufacturer-specific identifier of the equipment type</del></p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- The month and the year of equipment manufacturing or of the certificate request.</li> </ul> <p>The manufacturer shall ensure that this data is correct and that the certificate returned by the MSCA is inserted in the intended equipment.</p> <p><b>Rationale:</b> <i>Unnecessary specifications and requirements removed.</i></p>	378



	longer required to send a manufacturer specific equipment type.		
App.11 CSM 157	<p>Vehicle units shall use the protocol depicted in Figure 4 for verifying a tachograph card's certificate chain.</p> <p>Notes to Figure 4: ... etc etc</p> <p><b>Issue:</b> it is important to check that the certificate received has the authorization for the role for which it is presented.</p>	<p>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:</p> <ul style="list-style-type: none"> <li>- The CHA field of the Card certificate shall indicate a card certificate for mutual authentication (see Appendix 1, data type EquipmentType).</li> <li>- The CHA of the Card.CA certificate shall indicate an MSCA.</li> <li>- The CHA of the Card.Link certificate shall indicate the ERCA.</li> </ul> <p>Notes to Figure 4: ... etc etc</p> <p><b>Rationale:</b> avoid possible misues of certificates adding the highlighted text to the requirement.</p>	379
App.11 CSM_159	As indicated in Figure 4, once the VU has verified the authenticity and validity of a previously unknown certificate, it may store this certificate for future reference, such that it does not need to verify that certificate's authenticity again if it is presented to the VU again. Instead of storing the entire certificate, a VU may choose to store	As indicated in Figure 4, once the VU has verified the authenticity and validity of a previously unknown certificate, it may store this certificate for future reference, such that it does not need to verify that certificate's authenticity again if it is presented to the VU again. Instead of storing the entire certificate, a VU may choose to store	380

	<p>only the contents of the Certificate Body, as specified in section 9.3.2.</p> <p><b>Issue:</b> Problem linked to the amendment of CSM_91. An ERCA(3) card wouldn't be accepted by an ERCA(1) VU.</p>	<p>only the contents of the Certificate Body, as specified in section 9.3.2. 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.</p> <p><b>Rationale:</b> If an ERCA(1) VU has stored in its lifetime the ERCA(2)-&gt;ERCA(1) link certificate, this certificate will be used to verify the ERCA(3)-&gt;ERCA(2) link certificate received by an ERCA(3) card.</p>	
<p>App.11 CSM 161</p>	<p>Tachograph cards shall use the protocol depicted in Figure 5 for verifying a VU's certificate chain.</p> <p>Notes to <b>Error! Reference source not found.:</b> ... etc etc</p> <p><b>Issue:</b> it is important to check that the certificate received has the authorization for the role for which it is presented.</p>	<p><i>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:</i></p> <ul style="list-style-type: none"> <li>- The CHA of the VU.Link certificate shall indicate the ERCA.</li> <li>- The CHA of the VU.CA certificate shall indicate an MSCA.</li> <li>- The CHA field of the VU certificate shall indicate a VU certificate for mutual authentication (see Appendix 1, data type EquipmentType).</li> </ul> <p>Notes to <b>Error! Reference source not found.:</b> ... etc etc</p> <p><b>Rationale:</b> avoid possible misues of certificates adding the highlighted text to the requirement.</p>	<p>381</p>
<p>App. 11 CSM_165</p>	<p>If the MSE: Set AT command is successful, the</p>	<p>If the MSE: Set AT command is successful, the</p>	<p>383</p>

	<p>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> <p><b>Issue:</b> to specify a security aspect.</p>	<p>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> <p><b>Rationale:</b> this clarifies that before each EXTERNAL AUTHENTICATE (so before each new mutual authentication) a new ephemeral key pair has to be generated.</p>	
App.11 CSM_170	<p>Next to the card challenge, the VU shall include in the signature the card holder reference taken from the card certificate.</p> <p>Note: This ensures that the card to which the VU authenticates itself is the same card whose certificate chain the VU has verified previously.</p> <p><b>Issue:</b> Terminology error.</p>	<p>Next to the card challenge, the VU shall include in the signature the <b>certificate</b> holder reference taken from the card certificate.</p> <p>Note: This ensures that the card to which the VU authenticates itself is the same card whose certificate chain the VU has verified previously.</p> <p><b>Rationale:</b> Error corrected.</p>	384
App. 11 CSM_171	<p>Current Figure 6.</p> <p><b>Issue:</b> Part of the figure was misleading.</p>	<p>See at the end for new Figure 6.</p> <p><b>Rationale:</b> Figure now clear.</p>	385
App. 11 CSM 174	<p>Upon receiving the VU's signature in an EXTERNAL AUTHENTICATE command, the card shall</p> <p>— Calculate the authentication token by concatenating Card.CHR, the card challenge rcard and the identifier of the VU ephemeral public key Comp(VU.PKeph),</p>	<p>Upon receiving the VU's signature in an EXTERNAL AUTHENTICATE command, the card shall</p> <p>- Calculate the authentication token by concatenating Card.CHR, the card challenge rcard and the identifier of the VU ephemeral public key Comp(VU.PKeph),</p>	385

	<p>— Calculate the hash over the authentication token, using the hashing algorithm linked to the key size of the VU's VU_MA key pair, as specified in CSM_50,</p> <p>— Verify the VU's signature using the ECDSA algorithm in combination with VU.PK and the calculated hash.</p> <p><b>Issue:</b> Part of the text was misleading.</p>	<p><del>— Calculate the hash over the authentication token, using the hashing algorithm linked to the key size of the VU's VU_MA key pair, as specified in CSM_50,</del></p> <p>- 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.</p> <p><b>Rationale:</b> Text now clear.</p>	
<p>App.11 CSM_176</p>	<p>...</p> <p>2. The VU sends the public point <math>VU.PK_{eph}</math> of its ephemeral key pair to the card. 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 <math>Comp(VU.PK_{eph})</math> to the card, and the card stored it.</p> <p>...</p> <p>6. Using <math>K_{MAC}</math>, the card computes an authentication token over the VU ephemeral public key identifier: <math>T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})</math>. The card sends <math>N_{PICC}</math> and <math>T_{PICC}</math> to the vehicle unit.</p> <p>...</p>	<p>...</p> <p>2. The VU sends the public point <math>VU.PK_{eph}</math> of its ephemeral key pair to the card. <b>The public point shall be converted to an octet string as specified in [TR-03111]. The uncompressed encoding format shall be used.</b> 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 <math>Comp(VU.PK_{eph})</math> to the card, and the card stored it.</p> <p>...</p> <p>6. Using <math>K_{MAC}</math>, the card computes an authentication token over the VU ephemeral public <del>key—identifier—point</del>: <math>T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})</math>. <b>The public point shall be in the format used by the VU (see bullet 2 above).</b> The card sends <math>N_{PICC}</math> and <math>T_{PICC}</math> to the vehicle unit.</p>	<p>386</p>

	<p><b>Issue:</b> format of the public key not clearly specified</p>	<p>...</p> <p><b>Rationale:</b> format well specified</p>	
<p>App.11 CSM_191</p>	<p>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, each data object in the APDU shall also be separately padded according to [ISO 7816-4].</p> <p>...</p> <p>Case 2 or 4 (even INS byte) with encryption: DO '81'    DO '99'    DO '8E'    SW1SW2</p> <p>Case 2 or 4 (even INS byte) without encryption: DO '87'    DO '99'    DO '8E'    SW1SW2</p> <p>...</p> <p>Current Figure 8, 9, 10.</p> <p><b>Issue:</b> errors in secure messaging specifications</p>	<p>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, <b>each data objects</b> in the APDU shall <b>also</b> be <b>separately</b> padded according to [ISO 7816-4].</p> <p>...</p> <p>Case 2 or 4 (even INS byte) with<b>out</b> encryption: DO '81'    DO '99'    DO '8E'    SW1SW2</p> <p>Case 2 or 4 (even INS byte) with<b>out</b> encryption: DO '87'    DO '99'    DO '8E'    SW1SW2</p> <p>....</p> <p><b>See below for new Figures 8, 9, 10.</b></p> <p><b>Rationale:</b> errors corrected</p>	<p>389</p>
<p>App.11 CSM_193</p>	<p>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,</p>	<p>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,</p>	<p>391</p>

	<ul style="list-style-type: none"> <li>- it detects a Secure Messaging error in a command APDU: <ul style="list-style-type: none"> <li>o An expected Secure Messaging data object is missing, the order of data objects is incorrect, or an unknown data object is included.</li> <li>o A Secure Messaging data object is incorrect, e.g. the MAC value is incorrect or the TLV structure is incorrect.</li> </ul> </li> <li>- it is depowered or reset,</li> <li>- the VU selects an application on the card,</li> <li>- the VU starts the VU Authentication process,</li> <li>- 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.</li> </ul> <p><b>Issue:</b> the Gen2 Secure Messaging status would be lost Selecting the Gen1 Application and this is an undesired effect (there is the need to manage Gen1 files while authenticated under the Gen2 mechanisms).</p>	<ul style="list-style-type: none"> <li>- it detects a Secure Messaging error in a command APDU: <ul style="list-style-type: none"> <li>o An expected Secure Messaging data object is missing, the order of data objects is incorrect, or an unknown data object is included.</li> <li>o A Secure Messaging data object is incorrect, e.g. the MAC value is incorrect or the TLV structure is incorrect.</li> </ul> </li> <li>- it is depowered or reset,</li> <li><del>the VU selects an application on the card,</del></li> <li>- the VU starts the VU Authentication process,</li> <li>- 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.</li> </ul> <p><b>Rationale:</b> It is possible to retain the Gen2 Secure Messaging status.</p>	
<p>App.11 CSM_211</p>	<p>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 and VU_MA certificates and for setting the VU_MA public key for subsequent VU</p>	<p>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 <del>and VU_MA</del> certificates and for setting the VU_MA public key for subsequent VU</p>	<p>394</p>

	<p>Authentication. No further mutual verification of the certificate chains shall take place during normal operation.</p> <p><b>Issue:</b> the VU_MA certificate is not verified in that situation.</p>	<p><i>Authentication. No further mutual verification of the certificate chains shall take place during normal operation.</i></p> <p><b>Rationale:</b> removal of a verification that does not take place</p>	
App.11 CSM_208	<p>... external GNSS unit...</p> <p><b>Issue:</b> typo</p>	<p>... external GNSS <b>facility</b>...</p> <p><b>Rationale:</b> typo corrected</p>	394
App.11 CSM_210	<p>... external GNSS unit...</p> <p><b>Issue:</b> typo</p>	<p>... external GNSS <b>facility</b>...</p> <p><b>Rationale:</b> typo corrected</p>	394
App.11 CSM_218	<p>See at the end the old Table 6 of CSM_218</p> <p><b>Issue:</b> error in the number of encrypted data bytes</p>	<p>See at the end the new Table 6 of CSM_218</p> <p><b>Rationale:</b> error corrected</p>	398
App.11 CSM_234	<p>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 <b>Error! Reference source not found..</b> 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].</p> <p>Notes to Figure 13: ... etc etc</p>	<p><i>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 <b>Error! Reference source not found..</b> 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].</i> <b>In both cases, for every certificate read from the data file, it is necessary to verify that the Certificate Holder Authorisation</b></p>	402

	<p><b>Issue:</b> it is not possible to distinguish between digital certificates for Mutual Authentication and digital certificates for signing</p>	<p><i>(CHA) field is correct:</i></p> <ul style="list-style-type: none"> <li>- The CHA field of the EQT certificate shall indicate a VU or Card (as applicable) certificate for signing (see Appendix 1, data type EquipmentType).</li> <li>- The CHA of the EQT.CA certificate shall indicate an MSCA.</li> <li>- The CHA of the EQT.Link certificate shall indicate the ERCA.</li> </ul> <p>Notes to Figure 13: ... etc etc</p> <p><b>Rationale:</b> the devices can now check that the proper certificate is used</p>	
<p>App.11 Sec.14 – Fig.13</p>	<p>See at the end Current Figure 13 of Appendix 11.</p> <p><b>Issue:</b> the equivalent of a 'typo' for a figure.</p>	<p>See at the end new figure 13 of Appendix 11.</p> <p><b>Rationale:</b> 'typo' corrected</p>	403
<p>App. 12 GNS_4</p>	<p>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) (the first two numbers) 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).</p> <p><b>Issue:</b> typo</p>	<p>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) (the first two numbers) 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).</p> <p><b>Rationale:</b> redundant information</p>	407
<p>Appendix 12 GNS_6</p>	<p>The GSA sentence shall be stored with record number '06'.</p> <p><b>Issue:</b> typo</p>	<p>The GSA sentence shall be stored with record number '02' to '05'.</p> <p><b>Rationale:</b> corrected typo. The record ids for GSA are clearly and correctly defined in Table 1, but this requirement GNS_6</p>	408



		<i>was not updated.</i>	
<i>App. 12 GNS_16</i>	In the communication protocol, extended length fields shall not supported  <b>Issue:</b> typo	<i>In the communication protocol, extended length fields shall not <b>be</b> supported</i>  <b>Rationale:</b> typo corrected	409
<i>App. 12 GNS_20</i>	The GNSS Secure Transceiver shall use a memory to store the data able to perform...  <b>Issue:</b> typo	<i>The GNSS Secure Transceiver shall use a memory to store the data <b>and be</b> able to perform...</i>  <b>Rationale:</b> typo corrected	409
<i>App. 12 GNS_18</i>	... composed by a Master File (MF), a Directory File (DF) with Application Identifier ...  <b>Issue:</b> typo	<i>... composed by a Master File (MF), a <b>Dedicated</b> File (DF) with Application Identifier ...</i>  <b>Rationale:</b> typo corrected	409
<i>Appendix 12 GNS_20</i>	The mapping of record numbers and data is provided in Table 1. Note that there are four GSA sentences for the four satellite systems and Satellite-Based Augmentation System (SBAS).  <b>Issue:</b> unclear	<i>The mapping of record numbers and data is provided in Table 1. Note that there are four GSA sentences for the four satellite systems and Satellite-Based Augmentation System (SBAS). <b>The recording order is: Galileo, GPS, GLONASS, Beidou.</b></i>  <b>Rationale:</b> It is better to clarify and define the order of the satellite systems.	409
<i>Appendix 12 GNS_23</i>	If the position is valid, the VU processor also extracts the values of HDOP from GSA NMEA sentences and calculate the average value on the available satellite systems (i.e., when the fix is available)  <b>Issue:</b> typo	<i>If the position is valid, the VU processor also extracts the values of HDOP from GSA NMEA sentences and calculate the <b>minimum</b> value on the available satellite systems (i.e., when the fix is available)</i>  <b>Rationale:</b> It is the minimum value to consider, as described in the following paragraphs.	411
<i>Appendix 12</i>	If the external GNSS facility has been breached, the GNSS Secure Transceiver shall erase all its	<i>GNS_29 If the external GNSS facility has been breached, the GNSS Secure Transceiver shall</i>	413

GNS_29	<p>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 '55'H Tamper detection of GNSS.</p> <p><b>Issue:</b> GNSS Secure Transceiver may not be able to answer the request after tampering</p>	<p><i>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 '55'H Tamper detection of GNSS. Alternately, the external GNSS facility may not respond to any external request anymore.</i></p> <p><b>Rationale:</b> Clarification on the possibility that the GNSS facility may not answer to commands from the VU if it has been breached.</p>	
App. 12 GNS_31	<p>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 fault of typeEventFaultType enum '56'H</p> <p><b>Issue:</b> typo</p>	<p><i>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 fault of type EventFaultType enum '56'H</i></p> <p><b>Rationale:</b> typo corrected</p>	414
App 12. 5.2.1 Section GNSS Time Conflict	<p>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). 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 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. However, when the position information from the GNSS receiver is available again, the automatic time adjustment shall be done</p>	<p>GNS_36 <i>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). 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 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. However, when the position information from the GNSS receiver is available again, the</i></p>	414

		<del>automatic time adjustment shall be done</del>	
		Rationale: consequence of the change in Annex 1. The GNSS requirement was also missing.	
App. 13 Chapter 2	For clarification, this Annex does not specify:  <b>Issue:</b> typo	<i>For clarification, this <b>Appendix</b> does not specify:</i>  <b>Rationale:</b> typo corrected	417
App. 13 Chapter 2	- 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 10 Common Security Mechanisms]).  <b>Issue:</b> obsolete reference left in the text	- <i>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 <b>11</b> Common Security Mechanisms]).</i>  <b>Rationale:</b> reference is up-dated	417
App. 13 Chapter 4.2	... However, if additional security mechanisms are needed, this will be done in accordance with Appendix 10 Common Security Mechanisms.  <b>Issue: obsolete reference left in the text</b>	<i>... However, if additional security mechanisms are needed, this will be done in accordance with Appendix <b>11</b> Common Security Mechanisms.</i>  <b>Rationale: reference is up-dated</b>	419
App. 13 Chapter 4.3	For security reasons, the VU shall inforce a PIN code authorization system separated from the Bluetooth pairing...  <b>Issue:</b> unclear wording	<i>For security reasons, the VU <b>will require</b> a PIN code authorization system separated from the Bluetooth pairing...</i>  <b>Rationale:</b> better wording	419
App. 13 Chapter 4.3	While the manufacturer may offers an option to change the PIN code directly through the VU, the PUC code shall not be alterable...  <b>Issue:</b> typo	<i>While the manufacturer may <b>offer</b> an option to change the PIN code directly through the VU, the PUC code shall not be alterable...</i>  <b>Rationale:</b> corrected typo	420

<p>App. 13 Chapter 4.4</p>	<p>If the data which need to be carried is too long than the available space in one message, it will be split in several submessage...</p> <p><b>Issue:</b> unclear wording</p>	<p>If the data <b>to be handled is larger</b> than the available space for one message, it will be splitted in several submessages...</p> <p><b>Rationale:</b> better wording</p>	<p>421</p>
<p>App. 13 Annex 1</p>	<p><b>LIST OF AVAILABLE DATA THROUGH THE ITS INTERFACE</b></p> <p><b>Issue:</b> typo</p>	<p><b>1°) LIST OF AVAILABLE DATA THROUGH THE ITS INTERFACE</b></p> <p><b>Rationale:</b> typo corrected</p>	<p>427</p>
<p>Appendix 14 DSC 19</p>	<p>The DSRC-VU antenna shall be positioned at a location where it optimizes the DSRC communication between the vehicle and the roadside antenna (in general in or close to the centre of the vehicle windshield ...). For light vehicles an installation corresponding to the upper part of the windscreen is suitable.</p> <p><b>Issue:</b> unclear</p>	<p>The DSRC-VU antenna shall be installed where it optimizes the DSRC communication between the vehicle and the roadside <b>reader antenna, when the reader is installed 15 meters distance in front of the vehicle and 2 meters height, targetting the horizontal and vertical center of the windscreen.</b></p> <p>For light vehicles an installation corresponding to the upper part of the windscreen is suitable. <b>For all the other vehicles the DSRC antenna shall be installed either near the lower or near the upper part of the windscreen.</b></p> <p><b>Rationale:</b> Clarification on the antenna position</p>	<p>457</p>
<p>Appendix 14 DSC 22</p>	<p>The antenna shall be positioned as determined in DSC_19 and shown in figure 14.4 (oval line) and it efficiently supports the use cases described in in 4.1.2 and 4.1.3.</p> <p><b>Issue:</b> redundant information</p>	<p>The antenna shall be positioned as determined in DSC_19 <b>and shown in figure 14.4 (oval line)</b> and it efficiently supports the use cases described in in 4.1.2 and 4.1.3.</p> <p><b>Rationale:</b> figure 14.4 is just an example and it should not be in a requirement.</p>	<p>458</p>
<p>App. 14 DCS_36 seq 7</p>	<p>Sends GET.request for data other Attribute (if appropriate)"</p> <p><b>Issue:</b> typo</p>	<p>Sends GET.request for data <b>of</b> other Attribute (if appropriate)"</p> <p><b>Rationale:</b> typo corrected</p>	<p>470</p>

<p>Appendix 14 DSC 40 5.4.4</p>	<p><i>Timestamp of current record</i><sup>2</sup>'</p> <p><b>Issue:</b> typo</p>	<p><i>Timestamp of current record</i><sup>2</sup>'</p> <p><b>Rationale:</b> Typo. Remove <sup>2</sup> at the end of 'Timestamp of current record'</p>	<p>471</p>
<p>Appendix 14 DSC 40 5.4.4</p>	<pre>RtmCommProfile      INTEGER {                     C1 (1),                     C2 (2)                     } (0..255)  DEFAULT 1 }</pre> <p><b>Issue:</b> redundant information</p>	<pre>Rtm-ContextMark ::= SEQUENCE {     standardIdentifier      StandardIdentifier, --     identifier of the TARV part and its version }  <del>RtmCommProfile      INTEGER {     C1 (1),     C2 (2)     } (0..255) DEFAULT 1 }</del>  RtmTransferAck ::= INTEGER {     Ok (1),     NoK (2)     } (1..255)</pre> <p><b>Rationale:</b> RtmCommProfile is not needed</p>	<p>470</p>
<p>Appendix 14 DSC 40 5.4.4</p>	<pre>RtmTransferAck ::= INTEGER {     Ok (1),     NoK (2)     } SIZE (1..255)</pre> <p><b>Issue:</b> integer already defines the size</p>	<pre>RtmTransferAck ::= INTEGER {     Ok (1),     NoK (2)     } <del>SIZE</del> (1..255)</pre> <p><b>Rationale:</b> Removal of SIZE in RtmTransferAck</p>	<p>471</p>

		<i>because already defined in INTEGER.</i>	
Appendix 14	<p>DSC_40 ... TachographPayload ::= SEQUENCE {</p> <p>tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509....</p> <p><b>Issue:</b> the mapping of characters based on LatinAlphabetNo2 or latinCyrillicAlphabet was missing</p>	<p>DSC_40 ... TachographPayload ::= SEQUENCE {</p> <p>tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509<sup>1</sup>....</p> <p><b>1.</b> 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 14906.2</p> <p><b>Rationale: A footnote</b> is inserted in DSC_40 in relation of the LPN to clarify that the mapping of characters based on LatinAlphabetNo2 or latinCyrillicAlphabet will be done on the basis of ISO/DIS 14906.2. This is the similar approach to the one adopted for electronic tolling in Europe.</p>	471
Appendix 14 DSC_43	<p>DSC 43 should be modified to “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)”.</p> <p><b>Issue:</b> Lack of clarification</p>	<p>Replace current requirement with:</p> <p>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.</p> <p><b>Issue:</b> Clarification on the encoding of TachographPayload (which must be within the constraints of DSRC frame) and the PER, which can be ALIGNED and UNALIGNED. From the examples provided in the current published version of the specifications (2016-799), it is clear that it is PER UNALIGNED, but this is further clarified with these changes.</p>	476
Appendix 14 DSC 48 Table 14.9	<p>The sentence “(the optional RtmCommProfile element is omitted)” should be removed.</p> <p><b>Issue:</b> Lack of clarification</p>	<p>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.</p>	481

		<p>Note that only one element of the sequence is present (the optional RtmCommProfile element is omitted)</p> <p>Issue: Sentence is removed because it is a consequence of the removal of the RtmCommProfile in a previous comment.</p>	
<p>Appendix 14 DSC 68</p>	<p>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 shall be an open standard connection</p> <p><b>Issue:</b> unclear</p>	<p><i>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'</i></p> <p><b>Rationale:</b> this is just a clarification that an open connection does not exist when the DSRC-VU is internal to the VU.</p>	492
<p>App. 15 Chapter 2.2</p>	<p>It is understood that first generation tachograph cards are interoperable with first generation vehicle units (in compliance with Annex 1B of this Regulation), while second generation tachograph cards are interoperable with second generation vehicle units (in compliance with Annex 1C of this Regulation). In addition, the requirements below shall apply.</p> <p><b>Issue:</b> confusion on regulation to refer to</p>	<p>"It is understood that first generation tachograph cards are interoperable with first generation vehicle units (in compliance with Annex 1B of Regulation (EEC) No 3821/85), while second generation tachograph cards are interoperable with second generation vehicle units (in compliance with Annex 1C of this Regulation). In addition, the requirements below shall apply.</p> <p><b>Rationale:</b> corrected reference to regulation</p>	498
<p>App. 15 MIG_11</p>	<p>— the other application data EFs (within TACHO DF) requested by the first generation card download protocol. This information shall be secured with a digital signature, according to the first generation security mechanisms.</p> <p>Such download shall not include application data EFs only present in second generation driver (and workshop) cards (application data EFs within TACHO_G2 DF).</p> <p>Issue: typo</p>	<p>— 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.</p> <p>Such download shall not include application data EFs only present in second generation driver (and workshop) cards (application data EFs within DF Tachograph_G2).</p> <p><b>Rationale:</b> typo corrected</p>	499

*CHECKLIST OF CHANGES FOR AMENDED ANNEX IC and APPENDIXES*  
**IMPLEMENTING REGULATION, ANNEX IC and APPENDIXES**

<b>Ref (section/page/req)</b>	<b>Published Text + Issue</b>	<b>New text + Rationale</b>	L139/
<i>Reg.(EU) n° 799/2016 Whereas (4)</i>	<p>New security mechanisms for maintaining the level of security of the digital tachograph should be introduced with the smart tachograph to address current security vulnerabilities. One of such vulnerabilities is the absence of expiry dates of digital certificates. In order to comply with the best practices in security matters, it is recommended that the use of digital certificates without expiry dates should be avoided. The normal operation validity period of vehicle units should be 15 years, starting on the issuing date of the vehicle unit digital certificates. Vehicle units should be replaced after that validity period.</p> <p><i>Issue: terminology error, it is the effective date that is stored in the certificate and not the issuing date. The issuing date and the effective dates may also differ.</i></p>	<p><i>New security mechanisms for maintaining the level of security of the digital tachograph should be introduced with the smart tachograph to address current security vulnerabilities. One of such vulnerabilities is the absence of expiry dates of digital certificates. In order to comply with the best practices in security matters, it is recommended that the use of digital certificates without expiry dates should be avoided. The normal operation validity period of vehicle units should be 15 years, starting on the <b>issuingeffective</b> date of the vehicle unit digital certificates. Vehicle units should be replaced after that validity period.</i></p> <p><i>Rationale: terminology corrected.</i></p>	1
<i>Annex 1 C req. 13</i>	<p>...</p> <p>the vehicle units have a normal operations validity period of 15 years, starting with the vehicle unit certificates issuing date, but vehicle units can be</p>	<p>...</p> <p>the vehicle units have a normal operations validity period of 15 years, starting with the vehicle unit certificates <b>issuingeffective</b> date, but vehicle units</p>	22



	<p>used for additional 3 months, for data downloading only.</p> <p><i>Issue: terminology error, it is the effective date that is stored in the certificate and not the issuing date. The issuing date and the effective dates may also differ.</i></p>	<p><i>can be used for additional 3 months, for data downloading only.</i></p> <p><i>Rationale: terminology corrected.</i></p>	
App.2 TCS 114	<p><i>Issue: additional error code necessary. Also added a Note to be sure that the commands MSE: SET AT and MSE: SET DST pick up the correct certificate, that is respectively MA certificate and a Sign certificate. If the commands pick up the wrong certificate the system returns errors.</i></p>	<p><i>-If the currentAuthenticatedTime of the card is later than the Expiration Date of the selected public key, the processing state returned is '6A88'.</i></p> <p><i>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.</i></p> <p><i>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</i></p>	210

		<p>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.</p> <p>Rationale: error code added (see Figure 5 of Appendix 11, it is explicitly necessary to check the public key validity and to return an error in case of expiration). Additional note added to avoid errors.</p>	
App.2 TCS 134	Issue: additional error code necessary	<p>-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'.</p> <p>Rationale: error code added</p>	214
App.7 DDP 035	<p>The download of a tachograph card includes the following steps:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- Download the EFs Card_Certificate (or CardSignCertificate) and CA_Certificate. This information is not secured with a digital signature.</li> </ul> <p>It is mandatory to download these files for each download session.</p> <ul style="list-style-type: none"> <li>- Download the other application data EFs (within Tachograph DF and Tachograph_G2 DF if relevant) except EF Card_Download. This information is</li> </ul>	<p>The download of a tachograph card includes the following steps:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- (for first and second generation tachograph cards) Download EFs within Tachograph DF: <ul style="list-style-type: none"> <li>- 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.</li> <li>- Download the other application data EFs (within Tachograph DF)except EF Card_Download.</li> </ul> </li> </ul>	277

	<p>secured with a digital signature.</p> <ul style="list-style-type: none"> <li>- It is mandatory to download at least the EFs Application_Identification and ID for each download session.</li> <li>-- When downloading a driver card it is also mandatory to download the following EFs: <ul style="list-style-type: none"> <li>--- Events_Data,</li> <li>--- Faults_Data,</li> <li>--- Driver_Activity_Data,</li> <li>--- Vehicles_Used,</li> <li>--- Places,</li> <li>--- GNSS_Places (if relevant),</li> <li>--- Control_Activity_Data,</li> <li>--- Specific_Conditions.</li> </ul> </li> <li>- When downloading a driver card, update the LastCardDownload date in EF Card_Download,</li> <li>- When downloading a workshop card, reset the calibration counter in EF Card_Download.</li> <li>- When downloading a workshop card the EF Sensor_Installation_Data shall not be downloaded.</li> </ul> <p><i>Issue: amibiguity in the text and/or erroneous terminology</i></p>	<p><i>This information is secured with a digital signature, using Appendix 11 Common Security Mechanisms Part A.</i></p> <ul style="list-style-type: none"> <li>- <i>It is mandatory to download at least the EFs Application_Identification and Identificatio for each download session.</i></li> <li>- <i>When downloading a driver card it is also mandatory to download the following EFs:</i> <ul style="list-style-type: none"> <li>- <i>Events_Data,</i></li> <li>- <i>Faults_Data,</i></li> <li>- <i>Driver_Activity_Data,</i></li> <li>- <i>Vehicles_Used,</i></li> <li>- <i>Places,</i></li> <li>- <i>Control_Activity_Data,</i></li> <li>- <i>Specific_Conditions.</i></li> </ul> </li> <li>- <i>(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:</i> <ul style="list-style-type: none"> <li>- <i>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.</i></li> <li>- <i>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.</i></li> </ul> </li> </ul>	
--	--	--	--

		<ul style="list-style-type: none"><li>- It is mandatory to download at least the EFs <i>Application_Identification</i> and <i>Identification</i> for each download session.</li><li>- When downloading a driver card it is also mandatory to download the following EFs:<ul style="list-style-type: none"><li>- <i>Events_Data</i>,</li><li>- <i>Faults_Data</i>,</li><li>- <i>Driver_Activity_Data</i>,</li><li>- <i>Vehicles_Used</i>,</li><li>- <i>Places</i>,</li><li>- <i>Control_Activity_Data</i>,</li><li>- <i>Specific_Conditions</i>,</li><li>- <i>VehicleUnits_Used</i>,</li><li>- <i>GNSS Places</i>.</li></ul></li><li>- When downloading a driver card, update the <i>LastCardDownload</i> date in EF <i>Card_Download</i>, in the <i>Tachograph</i> and, if applicable, <i>Tachograph_G2</i> DFs.</li><li>- When downloading a workshop card, reset the calibration counter in EF <i>Card_Download</i> in the <i>Tachograph</i> and, if applicable, <i>Tachograph_G2</i> DFs.</li><li>- When downloading a workshop card the EF <i>Sensor_Installation_Data</i> in the <i>Tachograph</i> and, if applicable, <i>Tachograph_G2</i> DFs shall not be downloaded.';</li></ul> <p><i>Rationale: text made clearer and terminology corrected</i></p>	
--	--	--	--

<p>App.7 DDP 037</p>	<p>The sequence to download the EFs ICC, IC, Card_Certificate (or CardSignCertificate) and CA_Certificate is as follows:</p> <p>...</p> <p><i>Issue: amibiguity in the text and/or erroneous terminology</i></p>	<p><i>The sequence to download the EFs ICC, IC, Card_Certificate (or CardSignCertificate for DF Tachograph_G2) and, CA_Certificate and Link_Certificate (for DF Tachograph_G2 only) is as follows:</i></p> <p>...</p> <p><i>Rationale: text made clearer and terminology corrected</i></p>	<p>278</p>
<p>App.11 CSM_234</p>	<p>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 <b>Error! Reference source not found.</b> 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].</p> <p>Notes to Figure 13: ... etc etc</p> <p><i>Issue: it is not possible to distinguish between digital certificates for Mutual Authentication and digital certificates for signing. In addition to ERCA and MSCA certificates, also the Card_Sign and VU_Sign certificates verified during the process can be used to update the card internal clock.</i></p>	<p><i>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 <b>Error! Reference source not found.</b> 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:</i></p> <ul style="list-style-type: none"> <li><i>- Second-generation ERCA link certificates</i></li> <li><i>- Second-generation MSCA certificates</i></li> <li><i>- Second-generation VU_Sign or Card_Sign certificates issued by the same country as the control card's own card certificate.</i></li> </ul> <p><i>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</i></p>	<p>402</p>

		<p>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:</p> <ul style="list-style-type: none"> <li>- The CHA field of the EQT certificate shall indicate a VU or Card (as applicable) certificate for signing (see Appendix 1, data type EquipmentType).</li> <li>- The CHA of the EQT.CA certificate shall indicate an MSCA.</li> <li>- The CHA of the EQT.Link certificate shall indicate the ERCA.</li> </ul> <p>Notes to Figure 13: ... etc etc</p> <p>Rationale: the devices can now check that the proper certificate is used and the ERCA, MSCA and VU_Sign and Card_Sign certificates can be used to internally update the card clock.</p>	
App.11 CSM_123	<p>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, and the Distinguished Encoding Rules (DER) according to [ISO 8825-1] shall be used for encoding.</p> <p>Issue: the text included an unnecessary</p>	<p>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, and the Distinguished Encoding Rules (DER) according to [ISO 8825-1] shall be used for encoding.</p>	373

	<p>requirement and another necessary specification was missing. Indeed it is important to remark the link between the VU serial number used for the DSRC keys generation and the CHR. In addition, if the VU serial number is not available, the Certificate Request serial number shall be used to derive the VU specific DSRC keys.</p>	<p><b>Note:</b></p> <p>-This VU serial number shall be identical to the <code>vuSerialNumber</code> element of <code>VuIdentification</code>, see Appendix 1, and to the Certificate Holder Reference in the VU's certificates.</p> <p>-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.</p> <p><i>Rationale: unnecessary requirement removed and necessary specification added.</i></p>	
App.11 CSM_124	<p>...</p> <p>info = VU serial number as specified in CSM_123</p> <p>...</p> <p><i>Issue: linked to amendment of CSM_123</i></p>	<p>...</p> <p>info = VU serial number <b>or certificate request ID,</b> as specified in CSM_123</p> <p>...</p> <p><i>Rationale: linked to amendment of CSM_123</i></p>	373
App.11 CSM_128	<p>The MSCA shall keep records of all VU-specific DSRC keys it generated, their version number and the identification of the VU for which each set of keys is intended.</p> <p><i>Issue: linked to amendment of CSM_123</i></p>	<p><i>The MSCA shall keep records of all VU-specific DSRC keys it generated, their version number and <b>the identification of the VU serial number or certificate request ID used in deriving them</b> for which each set of keys is intended.</i></p> <p><i>Rationale: linked to amendment of CSM_123</i></p>	374

App.11 CSM_224	<p>...</p> <p>VU serial number the VU's serial number (data type VuSerialNumber)</p> <p>...</p> <p><i>Issue: linked to amendment of CSM_123</i></p>	<p>...</p> <p>VU serial number the VU's serial number or certificate request ID (data type VuSerialNumber or CertificateRequestID) - see CSM_123</p> <p>...</p> <p><i>Rationale: linked to amendment of CSM_123</i></p>	400
App.11 CSM_228	<p>2.The control card shall use the indicated DSRC master key in combination with the VU serial number in the DSRC security data to derive the VU-specific DSRC keys K_VUDSRC_ENC and K_VUDSRC_MAC, as specified in CSM_124.</p> <p><i>Issue: linked to amendment of CSM_123</i></p>	<p>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_VUDSRC_ENC and K_VUDSRC_MAC, as specified in CSM_124.</p> <p><i>Rationale: linked to amendment of CSM_123</i></p>	401
App. 11 CSM_72	<p>CSM_72: [...]Whenever a VU key pair is generated, the party generating the key shall send the public key to the MSCA of the country in which it resides, in order to obtain a corresponding VU certificate signed by the MSCA. [...]</p> <p><b>Issue:</b> wording is not clear and can create useless constraint</p>	<p>CSM_83: [...]Whenever a VU key pair is generated, the party generating the key shall send the public key to theits MSCA-of the country in which it resides, in order to obtain a corresponding VU certificate signed by the MSCA. [...]</p> <p><b>Rationale:</b> text more in line with real scenarios</p>	363
App. 11 CSM_83	<p>CSM_83: [...] Whenever a card key pair is generated, the party generating the key shall send the public key to the MSCA of the country in which it resides, in order to obtain a corresponding card</p>	<p>CSM_83: [...] Whenever a card key pair is generated, the party generating the key shall send the public key to theits MSCA-of the country in which it resides, in order to obtain a</p>	365



	<p>certificate signed by the MSCA. [...]</p> <p><b>Issue:</b> wording is not clear and can create useless constraint</p>	<p><i>corresponding card certificate signed by the MSCA. [...]</i></p> <p><b>Rationale:</b> text more in line with real scenarios</p>	
<p>App. 11 CSM_93</p>	<p>CSM_93: [...]Whenever an EGF_MA key pair is generated, the public key shall be sent to the MSCA of the country in which it resides, in order to obtain a corresponding EGF_MA certificate signed by the MSCA. [...]</p> <p><b>Issue:</b> wording is not clear and can create useless constraint</p>	<p><i>CSM_83: [...]Whenever an EGF_MA key pair is generated,—the party generating the key shall send the public key to its MSCA in order to obtain a corresponding EGF_MA certificate signed by the MSCA. [...]</i></p> <p><b>Rationale:</b> text more in line with real scenarios</p>	366

**Published TCS\_45 :**

<b>Byte</b>	<b>Length</b>	<b>Value</b>	<b>Description</b>
#1	1	'99h'	Tag for Processing Status (SW1-SW2) - optional for generation 1 secure messaging
#2	1	'02h'	Length of Processing Status
#3 - #4	2	'XX XXh'	Processing Status of the unprotected response APDU
#5	1	'81h'	TPV : Tag for plain value data
#6	L	'NNh' or	LPV : length of returned data (=original Le).
		'81 NNh'	L is 2 bytes if $L_{PV} > 127$ bytes.
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Plain Data value
#(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)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	'08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B)
SW	2	'XXXXh'	Cryptographic checksum Status Words (SW1,SW2)

---

**Published TCS\_46:**

Byte	Length	Value	Description
#1	1	'87h'	T <sub>PI CG</sub> : Tag for encrypted data (cryptogram)
#2	L	'MMh' or	L <sub>PI CG</sub> : length of returned encrypted data (different of original L <sub>e</sub> of the command due to padding).
		'81 MMh'	L is 2 bytes if L <sub>PI CG</sub> > 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
#(4+L+MM) - #(5+L+MM)	2	'XX XXh'	Processing Status of the unprotected response APDU
#(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)

---

**New TCS\_45 :**

Byte	Length	Value	Description
#1	1	'81h'	T <sub>PV</sub> : Tag for plain value data
#2	L	'NNh' or '81 NNh'	L <sub>PV</sub> : length of returned data (=original Le). L is 2 bytes if L <sub>PV</sub> >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)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	'08h', '0Ch' or '10h' depending on AES key length for Generation 2 secure messaging (see Appendix 11 Part B) Cryptographic checksum
SW	2	'XXXXh'	Status Words (SW1,SW2)

---

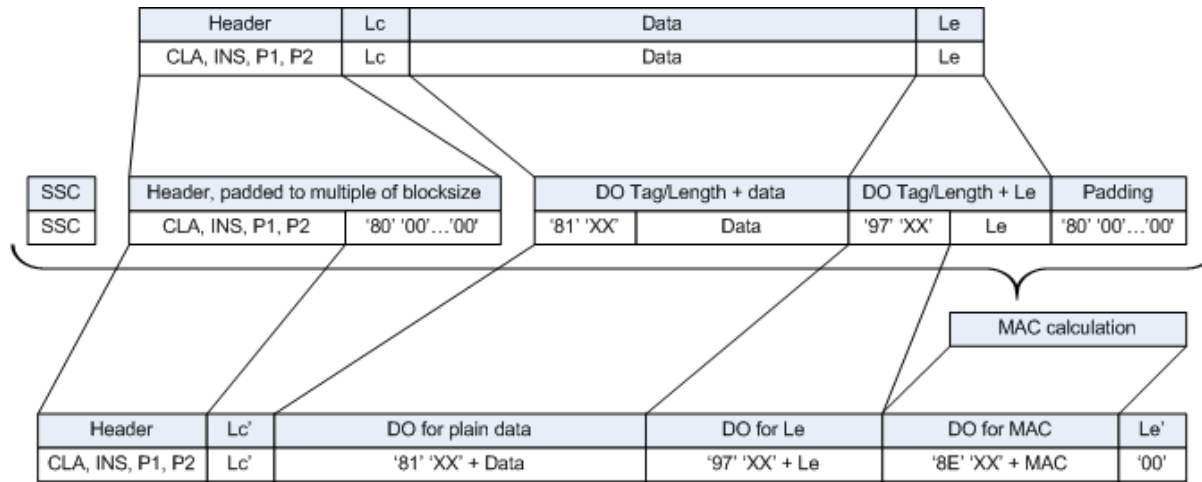
**New TCS\_46 :**

<b>Byte</b>	<b>Length</b>	<b>Value</b>	<b>Description</b>
#1	1	'87h'	T <sub>PI CG</sub> : Tag for encrypted data (cryptogram)
#2	L	'MMh' or	L <sub>PI CG</sub> : length of returned encrypted data (different of original Le of the command due to padding).
		'81 MMh'	L is 2 bytes if L <sub>PI CG</sub> > 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)

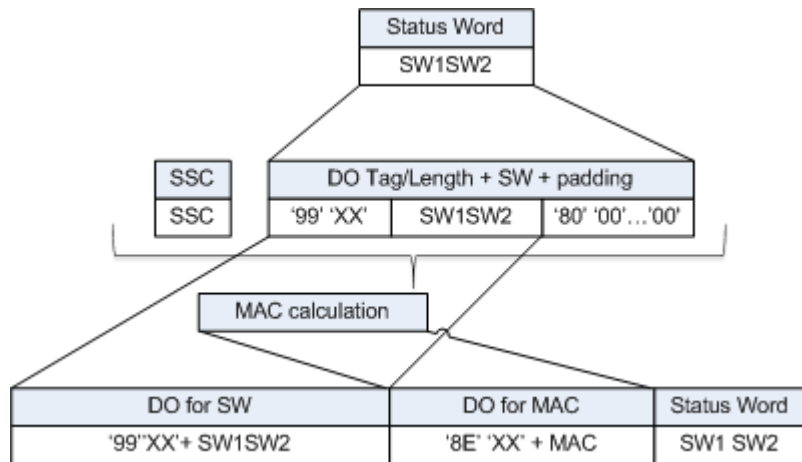
---

---

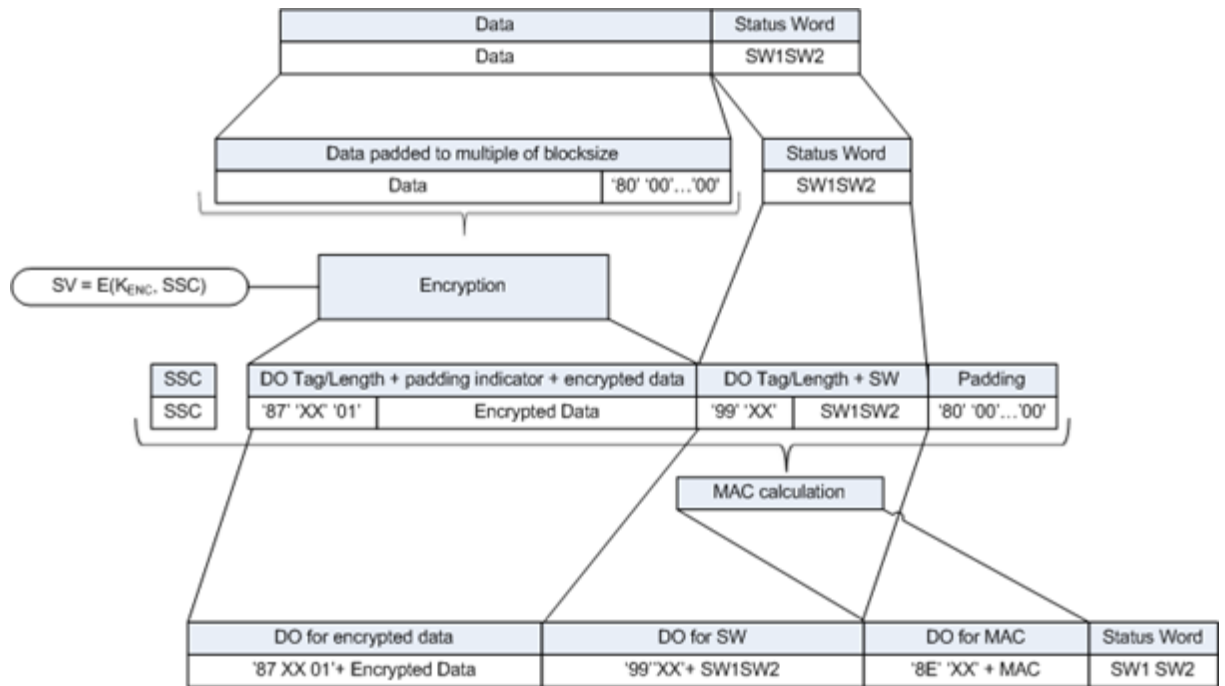
**New Figure 8 for CSM\_191 :**



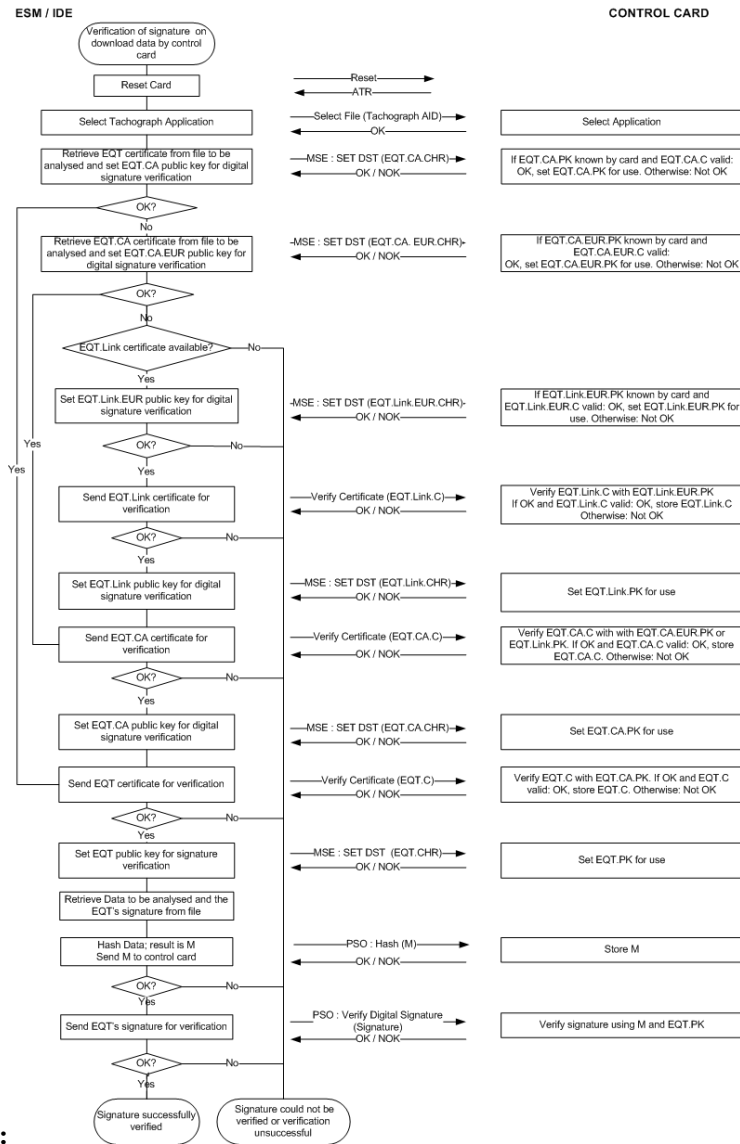
New Figure 9 for CSM\_191 :



New Figure 10 for CSM\_191 :







**New Figure 13 for Appendix 11, Section 14:**

Old Table 6 for CSM\_218

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 or 32, depend on file	16 / 32	16 / 32	16 / 32
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

New Table 6 for CSM\_218

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 or 32, 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

**Published TCS\_133:**

<b>Byte</b>	<b>Length</b>	<b>Value</b>	<b>Description</b>
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	Tag : data field contains DOs relevant for verification
Lc	1	'83h'	Length Lc of the subsequent data field
6	1	'9Eh'	Tag for Digital Signature
#7-#8	2	'81 XXh'	Length of digital signature: 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)
#9-#(8+L)	L	'XX..XXh'	Digital signature content

**New TCS\_133:**

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

**Published TCS\_124:**

<b>Byte</b>	<b>Length</b>	<b>Value</b>	<b>Description</b>
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tag: Hash
P2	1	'XXh'	P2 : Indicates the algorithm to be used for hashing of the data of the currently selected transparent file: '00h' for SHA-1 '01h' for SHA-256 '02h' for SHA-384 '03h' for SHA-512

**New TCS\_124:**

Byte	Length	Value	Description
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tag: Hash
P2	1	'00h'	<p>Algorithm implicitly known</p> <p>For the Tachograph Generation 1 application: SHA-1</p> <p>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</p>

**Published TCS\_27:**

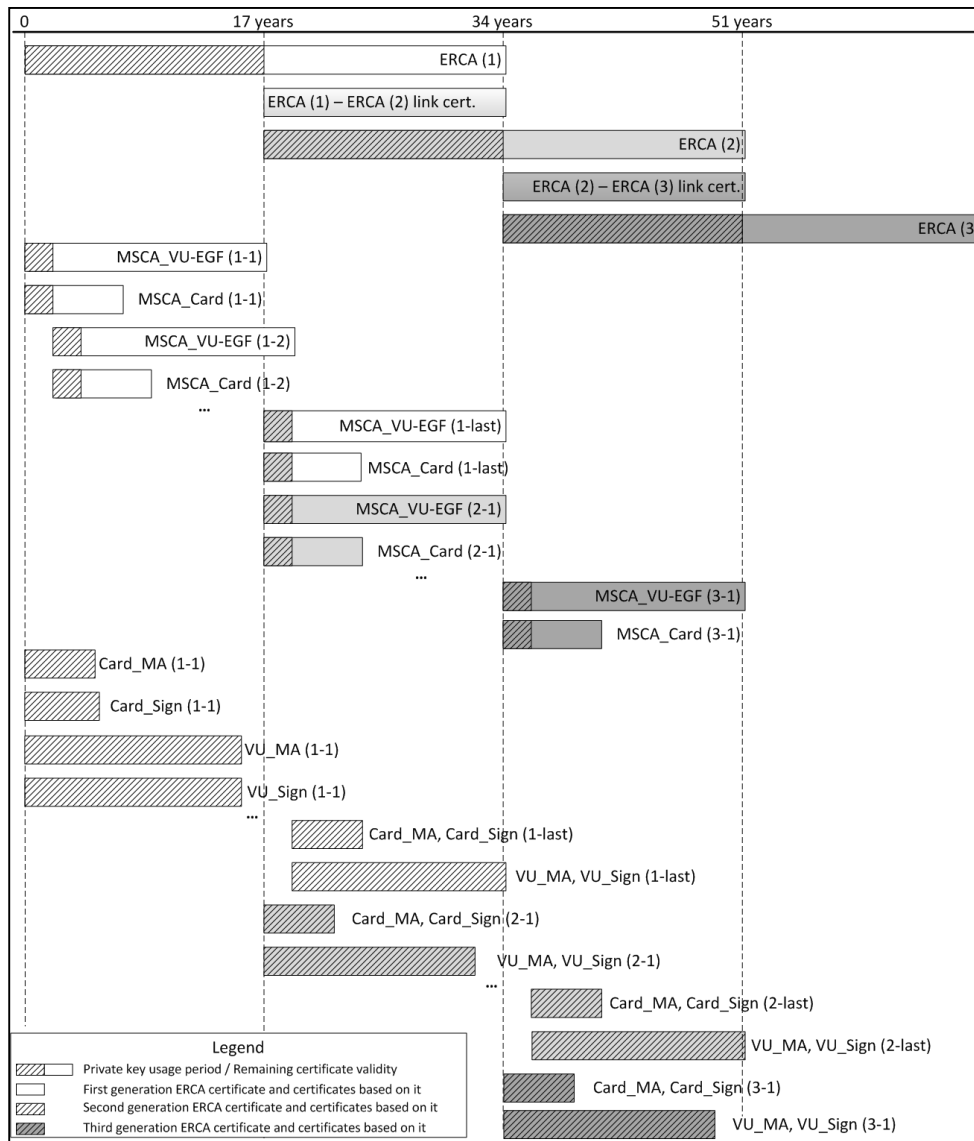
<b>Command</b>	<b>Driver Card</b>	<b>Workshop Card</b>	<b>Control Card</b>	<b>Company Card</b>
External Authenticate				
<input type="checkbox"/> For generation 1 authentication	Not applicable	Not applicable	Not applicable	Not applicable
<input type="checkbox"/> For generation 2 authentication	ALW	PWD	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
PSO: Hash of File	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Not applicable	ALW	Not applicable	Not applicable



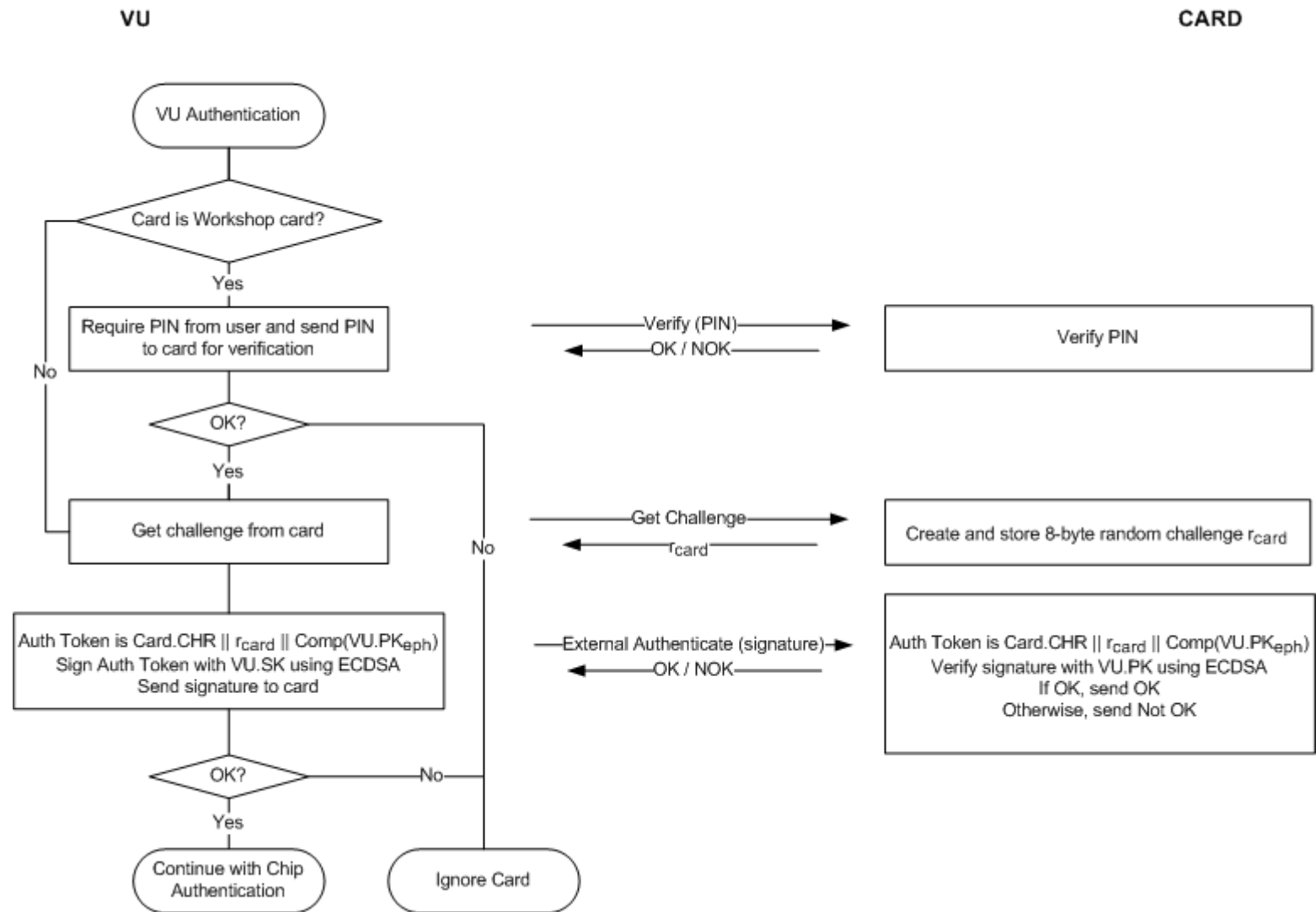
**New TCS\_27:**

<b>Command</b>	<b>Driver Card</b>	<b>Workshop Card</b>	<b>Control Card</b>	<b>Company Card</b>
External Authenticate				
<input type="checkbox"/> For generation 1 authentication	Not applicable	Not applicable	Not applicable	Not applicable
<input type="checkbox"/> For generation 2 authentication	ALW	PWD	ALW	ALW
Internal Authenticate				
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
PSO: Hash of File	Not applicable	Not applicable	Not applicable	Not applicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
<b>PSO: Verify Digital Signature</b>	<b>Not applicable</b>	<b>Not applicable</b>	<b>Not applicable</b>	<b>Not applicable</b>
Verify	Not applicable	ALW	Not applicable	Not applicable

**New Figure 1 for Section 9.1.7:**



New Figure 6 for CSM\_171:



**In Appendix 9:**

**Chapter 2 Vehicle unit functional tests**

**Error corrections in related requirements numbers**

**New table is:**

<b>No</b>	<b>Test</b>	<b>Description</b>	<b>Related requirements</b>
<b>1</b>	<b>Administrative examination</b>		
1.1	Documentation	Correctness of documentation	
1.2	Manufacturer test results	Results of manufacturer test performed during integration. Paper demonstrations.	88, 89,91
<b>2</b>	<b>Visual inspection</b>		
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		
<b>3</b>	<b>Functional tests</b>		

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
3.1 0	Company locks management	63 to 68
3.1 1	Monitoring control activities	69, 70
3.1 2	Detection of events and/or faults	71 to 88, 134

3.1 3	Equipment identification data	93*, 94*, 97, 100
3.1 4	Driver card insertion and withdrawal data	102* to 104*
3.1 5	Driver activity data	105* to 107*
3.1 6	Places and positions data	108* to 112*
3.1 7	Odometer data	113* to 115*
3.1 8	Detailed speed data	116*
3.1 9	Events data	117*
3.2 0	Faults data	118*
3.2 1	Calibration data	119* to 121*
3.2 2	Time adjustment data	124*, 125*
3.2 3	Control activity data	126*, 127*

3.2 4	Company locks data	128*
3.2 5	Download activity data	129*
3.2 6	Specific conditions data	130*, 131*
3.2 7	Recording and storing on tachographs cards	136, 137, 138*, 139*, 141*, 142, 143  144, 145, 146*, 147*, 148*, 149, 150
3.2 8	Displaying	90, 134, 151 to 168, PIC_001, DIS_001
3.2 9	Printing	90, 134, 169 to 181, PIC_001, PRT_001 to PRT_014
3.3 0	Warning	134, 182 to 191, PIC_001

3.3 1	Data downloading to external media	90, 134, 192 to 196
3.3 2	Remote communication for targeted roadside checks	197 to 199
3.3 3	Output data to additional external devices	200, 201
3.3 4	Calibration	202 to 206*, 383, 384, 386 to 391
3.3 5	Roadside calibration checking	207 to 209
3.3 6	Time adjustment	210 to 212*
3.3 7	Non-interference of additional functions	06, 425
3.3 8	Motion sensor interface	02, 122
3.3 9	External GNSS facility	03, 123
3.4 0	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



3.4 1	Cypher suite and standardized domain parameters		CSM_48, CSM_50
<b>4</b>	<b>Environmental tests</b>		
4.1	Temperature	<p>Verify functionality through:</p> <p>Test according to ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ -20 °C)</p> <p>This test refers to IEC 60068-2-1 : Environmental testing - Part 2-1: Tests - Test A: Cold</p> <p>Test according to ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h at 70 °C)</p> <p>This test refers to IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat</p> <p>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)</p> <p>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</p>	213

4.2	Humidity	Verify that the vehicle unit can withstand a cyclic damp (heat test) through IEC 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	<p>1. <b>Sinusoidal vibrations.</b>  verify that the vehicle unit can withstand sinusoidal vibrations with the following characteristics:</p> <p>constant displacement between 5 and 11 Hz: 10mm peak</p> <p>constant acceleration between 11 and 300 Hz: 5g</p> <p>This requirement is verified through IEC 60068-2-6, test Fc, with a minimum test duration of 3x12 hours (12 hours per axis)</p> <p>ISO 16750-3 does not require a sinusoidal vibration test for devices located in the decoupled vehicle cab.</p> <p>2. <b>Random vibrations:</b>  Test according to ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab</p> <p>Random vibration test, 10...2000 Hz, RMS vertical 21.3 m/s<sup>2</sup>, RMS longitudinal 11.8 m/s<sup>2</sup>, RMS lateral 13.1 m/s<sup>2</sup>, 3 axes, 32 h per axis, including temperature cycle -20...70°C.</p> <p>This test refers to IEC 60068-2-64: Environmental testing - Part 2-64: Tests - Test Fh: Vibration, broadband random and guidance</p> <p>3. <b>Shocks:</b>  mechanical shock with 3g half sinus according ISO 16750.</p> <p>The tests described above are performed on different samples of the equipment type being tested.</p>	219

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
<b>5</b>	<b>EMC tests</b>		
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: +/- 4kV for contact and +/- 8kV for air discharge	218

5.3	Conducted transient susceptibility on power supply	<p>For 24V versions: compliance with ISO 7637-2 + ECE Regulation No. 10 Rev. 3:</p> <p>pulse 1a: <math>V_s = -450V</math> <math>R_i = 50</math> ohms  pulse 2a: <math>V_s = +37V</math> <math>R_i = 2</math> ohms  pulse 2b: <math>V_s = +20V</math> <math>R_i = 0,05</math> ohms  pulse 3a: <math>V_s = -150V</math> <math>R_i = 50</math> ohms  pulse 3b: <math>V_s = +150V</math> <math>R_i = 50</math> ohms  pulse 4: <math>V_s = -16V</math> <math>V_a = -12V</math> <math>t_6 = 100ms</math>  pulse 5: <math>V_s = +120V</math> <math>R_i = 2,2</math> ohms <math>t_d = 250ms</math></p> <p>For 12V versions: compliance with ISO 7637-1 + ECE Regulation No. 10 Rev. 3:</p> <p>pulse 1: <math>V_s = -75V</math> <math>R_i = 10</math> ohms  pulse 2a: <math>V_s = +37V</math> <math>R_i = 2</math> ohms  pulse 2b: <math>V_s = +10V</math> <math>R_i = 0,05</math> ohms  pulse 3a: <math>V_s = -112V</math> <math>R_i = 50</math> ohms  pulse 3b: <math>V_s = +75V</math> <math>R_i = 50</math> ohms  pulse 4: <math>V_s = -6V</math> <math>V_a = -5V</math> <math>t_6 = 15ms</math>  pulse 5: <math>V_s = +65V</math> <math>R_i = 3ohms</math> <math>t_d = 100ms</math></p> <p>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</p> <p>For load dump proposal, refer to ISO 16750-2, 4th edition, chapter 4.6.4.</p>	218
-----	--	--	-----

## Chapter 4 Remote communication facility tests

### Section 3 Functional tests is missing

New table is:

#### 4. External remote communication facility tests

No	Test	Description	Related requirements
<b>1.</b>	<b>Administrative examination</b>		
1.1	Documentation	Correctness of documentation	
<b>2.</b>	<b>Visual inspection</b>		
2.1.	Compliance with documentation		
2.2.	Identification / markings		225, 226
2.3	Materials		219 to 223
<b>3.</b>	<b>Functional tests</b>		
3.1	Remote communication for targeted roadside checks		4, 197 to 199
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
<b>4. Environmental tests</b>			
4.1	Temperature	<p>Verify functionality through:</p> <p>Test according to ISO 16750-4, Chapter 5.1.1.2: Low temperature operation test (72 h @ -20 °C)</p> <p>This test refers to IEC 60068-2-1: Environmental testing - Part 2-1: Tests - Test A: Cold</p> <p>Test according to ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 h @ 70 °C)</p> <p>This test refers to IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat</p> <p>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)</p> <p>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</p>	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
<b>5</b>	<b>EMC tests</b>		
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: +/- 4kV for contact and +/- 8kV for air discharge	218

5.3	Conducted transient susceptibility on power supply	<p>For 24V versions: compliance with ISO 7637-2 + ECE Regulation No. 10 Rev. 3:</p> <p>pulse 1a: <math>V_s = -450V</math> <math>R_i = 50</math> ohms</p> <p>pulse 2a: <math>V_s = +37V</math> <math>R_i = 2</math> ohms</p> <p>pulse 2b: <math>V_s = +20V</math> <math>R_i = 0,05</math> ohms</p> <p>pulse 3a: <math>V_s = -150V</math> <math>R_i = 50</math> ohms</p> <p>pulse 3b: <math>V_s = +150V</math> <math>R_i = 50</math> ohms</p> <p>pulse 4: <math>V_s = -16V</math> <math>V_a = -12V</math> <math>t_6 = 100ms</math></p> <p>pulse 5: <math>V_s = +120V</math> <math>R_i = 2,2</math> ohms <math>t_d = 250ms</math></p> <p>For 12V versions: compliance with ISO 7637-1 + ECE Regulation No. 10 Rev. 3:</p> <p>pulse 1: <math>V_s = -75V</math> <math>R_i = 10</math> ohms</p> <p>pulse 2a: <math>V_s = +37V</math> <math>R_i = 2</math> ohms</p> <p>pulse 2b: <math>V_s = +10V</math> <math>R_i = 0,05</math> ohms</p> <p>pulse 3a: <math>V_s = -112V</math> <math>R_i = 50</math> ohms</p> <p>pulse 3b: <math>V_s = +75V</math> <math>R_i = 50</math> ohms</p> <p>pulse 4: <math>V_s = -6V</math> <math>V_a = -5V</math> <math>t_6 = 15ms</math></p> <p>pulse 5: <math>V_s = +65V</math> <math>R_i = 3ohms</math> <math>t_d = 100ms</math></p> <p>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</p> <p>For load dump proposal, refer to ISO 16750-2, 4th edition, chapter 4.6.4.</p>	218
-----	--	--	-----



## JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**  
[ec.europa.eu/jrc](https://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub

