European Commission

JRC TECHNICAL REPORTS

Smart Tachograph Components Interoperability Test Specification

Version 1.00

Michel Chiaramello (JRC)
Luigi Sportiello (JRC)
David Bakker (UL)

July 2018

Smart Tachograph Components
Interoperability Test Specification
Version 1.00 – July 2018

Contact information
E-mail: jrc-iot@ec.europa.eu

JRC Science Hub
https://ec.europa.eu/jrc

JRC112773

Ispra: European Commission, 2018

Contents

Abstract

This publication describes the interoperability test procedure for Smart Tachograph components, as defined in the REGULATION (EU) No 165/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL and in the technical specifications included in the COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 amended by the COMMISSION IMPLEMENTING REGULATION (EU) 2018/502.

Interoperability certification is one of the three certifications required for type approval of Smart Tachograph components. The other two certifications concern functional testing and security evaluation.

1 Introduction

1.1 Scope and background of this document

This publication describes the interoperability test procedure for Smart Tachograph Components, also called second-generation components. Interoperability testing must be carried out on smart tachograph components (i.e. a vehicle unit paired with a motion sensor and potentially with external GNSS facilities) and tachograph cards, with a view to obtain an interoperability certification. An interoperability certification is one of three certifications required for type approval of Smart Tachograph components. The other two certifications are functional testing and security evaluation.

The type approval procedure is defined in the Regulation (EU) No 165/2014 of the European Parliament and of the Council [1] (referred to hereinafter as the Regulation), in the technical specifications included in the Commission Implementing Regulation (EU) 2016/799 [2] amended by the Commission Implementing Regulation (EU) 2018/502 [3] (referred to hereinafter as Annex IC). In particular, the type approval process, including an exceptional procedure for the first type approvals, is contained in Chapter 8 of Annex IC. For convenience, this text is reproduced in Chapter 11 of the current document.

1.2 Intended audience

This document is intended for stakeholders in the development and interoperability testing of Smart Tachograph components.

Readers of this document are supposed to be familiar with the contents of Annex IC.

2 Interoperability Certification

2.1. The interoperability tests defined in this document aim to demonstrate that combinations of smart tachograph components conform to a specific subset of requirements drawn from Annex IC. This chapter gives an overview of these requirements.

2.2. Chapter 8 of Annex IC, Appendix 9 defines the requirements for interoperability tests. The contents of this Appendix are reproduced below:

No	Test	Description
8.1 Interoperability tests between vehicle units and tachograph cards		
1	Mutual authentication	Check that the mutual authentication between the vehicle unit and the tachograph card runs normally
2	Write/read tests	Execute a typical activity scenario on the vehicle unit. The scenario shall be adapted to the type of card being tested and involve writings in as many EFs as possible in the card Verify through a vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through daily printouts that all corresponding recordings can be properly read
8.2 Interoperability tests between vehicle units and motion sensors		
1	Pairing	Check that the pairing between the vehicle units and the motion sensors runs normally
2	Activity tests	Execute a typical activity scenario on the motion sensor. The scenario shall involve a normal activity and creating as many events or faults as possible. Verify through a vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through a daily printout that all corresponding recordings can be properly read
8.3 Interoperability tests between vehicle units and external GNSS facilities (when applicable)		
1	Mutual Authentication	Check that the mutual authentication (coupling) between the vehicle unit and the external GNSS module runs normally.
2	Activity tests	Execute a typical activity scenario on the external GNSS. The scenario shall involve a normal activity and creating as many events or faults as possible. Verify through a vehicle unit downloading that all corresponding recordings have been properly made Verify through a card downloading that all corresponding recordings have been properly made Verify through a daily printout that all corresponding recordings can be properly read

Table 1: Interoperability tests requirements

2.3 As stated in the Introduction of Annex IC, starting from the introduction date of this Annex, second-generation equipment shall be installed in vehicles registered for the first time and second-generation tachograph cards shall be used. However, first-generation digital tachograph components may be used until their end of life for domestic

transportation[1]. This implies that first-generation (Digital Tachograph) and second-generation (Smart Tachograph) components need to be interoperable.

2.4 Clause (446) of Annex IC states that the interoperability tests shall cover all generations of recording equipment or tachograph cards still in use.

2.5 The co-existence of tachograph card and vehicle unit generations is specified in detail in Appendix 15 to Annex IC:

- First-generation tachograph cards shall be interoperable with first-generation vehicle units.
- Second-generation tachograph cards shall be interoperable with second-generation vehicle units.
- First-generation vehicle units shall be able to use any valid second-generation tachograph card.
- Second-generation vehicle units shall be able to use any valid first-generation driver, control and company card, but shall not be able to use a valid first-generation workshop card.
- The capability of second-generation vehicle units to use first-generation tachograph cards may be suppressed once and forever by workshops.

2.6 The co-existence of motion sensor and vehicle unit generations is also specified in detail in Appendix 15 to Annex IC:

- First-generation motion sensors shall be interoperable with first-generation vehicle units.
- Second-generation motion sensors shall be interoperable with second-generation vehicle units.
- First-generation motion sensors shall not be interoperable with second-generation vehicle units.
- Second-generation motion sensors may be interoperable with second-generation vehicle units only, or with both generations of vehicle units. Requirement CSM_111 in Appendix 11 makes clear that this is dependent on a choice by the motion sensor manufacturer.

2.7. The type approval process as defined in Annex IC concerns only smart tachograph recording equipment (i.e. a vehicle unit paired with a motion sensor and potentially with an external GNSS facility) and tachograph cards. This implies that no interoperability requirements are defined for ancillary equipment (e.g. the calibration equipment used by workshops and the intelligent dedicated equipment used by controllers), even though successful implementation of the smart tachograph system depends on such equipment.

According to chapter 8 of Annex IC the following requirements have to be satisfied:

2.8. Requirement 443 requires that interoperability tests be performed on components which have received both a security and a functional certification. This implies that the interoperability tests shall be performed on samples of tachograph components identical in all respects to those certified for functionality and security.

2.9. According to requirement 440, the interoperability tests shall be limited to a series of manipulations performed on smart tachograph components at the Digital Tachograph Laboratory, which is, as specified by requirement 447, enabled to deliver the interoperability certificate.

[1] For international transportation, instead, 15 years after the entry into force of the Regulation, all vehicles shall be equipped with a compliant second-generation smart tachograph.

2.10. As specified by requirement 444, the smart tachograph components submitted for interoperability testing shall remain at the Digital Tachograph Laboratory and constitute the reference set against which new components will be tested.

2.11. Requirement 428 states that any changes to a type-approved tachograph component may necessitate re-certification, i.e. a complete or partial repetition of the type approval tests. The needs for re-certification shall be established on a case-by-case basis by the type approval authority, in co-operation with the functional testing laboratory, the security certification authority and the Digital Tachograph Laboratory.

2.12. Requirement 454 states that the Digital Tachograph Laboratory shall maintain a public website describing the state of a component's type approval. The URL of this website is: https://dtc.jrc.ec.europa.eu/.

3 Roles and Responsibilities

3.1. The European Commission service responsible for appointing the Digital Tachograph Laboratory (see Annex IC requirement 440) is:

European Commission
DG MOVE
Rue de Mot, 24
B-1040 Bruxelles

3.2. The interoperability test procedure is maintained by, implemented at, and available from:

Digital Tachograph Laboratory
Dir.E - SPACE, SECURITY AND MIGRATION
Cyber and Digital Citizen Security Unit (JRC.E.3)
European Commission
Joint Research Centre, Ispra Establishment (TP.361)
Via E. Fermi, 2749
I-21027 Ispra (VA)

3.3. The Digital Tachograph Laboratory assigns ManufacturerCodes (see Annex IC Appendix 1) to tachograph components manufacturers. This information is published on the public web site at the following address:

https://dtc.jrc.ec.europa.eu/dtc_manufacturer_code.php.

3.3. Each Member State of the European Union designates an authority responsible for approving smart tachograph system components (i.e vehicle units, motion sensors, potentially external GNSS facilities and external remote communication facilities, and tachograph cards) for use in the enforcement of European Union legislation.

3.4. Each non EU – AETR state designates an authority responsible for approving smart tachograph system components (i.e vehicle units, motion sensors, potentially external GNSS facilities and external remote communication facilities, and tachograph cards) for use in the enforcement of European Agreement concerning the work of crews of vehicles engaged in International road transport (AETR).

3.5. As stated in the requirement 428 of Annex IC, the Member/National State type approval authority may require an update or a confirmation of the functional, security, or interoperability certification whenever a type-approved component is changed.

3.6. The test requests are introduced in the chronological order of their arrival and they are officially registered only when the Digital Tachograph Laboratory is in possession of:

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

See Annex IC requirements 441 and 442.

3.7. The manufacturer or personaliser of a smart tachograph component is responsible for implementing the corrective actions required to resolve an interoperability failure found in that component.

3.8. If a smart tachograph component successfully passes all interoperability tests, the Digital Tachograph Laboratory shall deliver an interoperability certificate to its manufacturer; see Annex IC requirement 447.

3.9. The manufacturer shall present the interoperability certificate to the type approval authority in its State in order to obtain a type approval certificate.

3.10. A type approval national authority shall provide to the Digital Tachograph Lab a copy of any type approval certificate it grants (see Annex IC requirement 453).

3.11. The delivery of an interoperability certificate for a smart tachograph component shall be performed under a contractual agreement between the Digital Tachograph Laboratory and the entity which shall present the interoperability certificate to the National type approval authority.

4 Assumptions

4.1 Annex IC is assumed to define only minimum requirements for smart tachograph components.

4.2 The security-enforcing functions of the first-generation and second-generation tachograph systems are likely to prevent the analysis or debugging of equipment in the field. Interoperability tests shall therefore consider components under test as 'black boxes' whose internal workings are unknown.

For more information about these functions, see the respective Protection Profiles:

First generation components[2]:

- BSI-CC-PP-0057 Digital Tachograph – Vehicle Unit Protection Profile
- BSI-CC-PP-0070 Digital Tachograph – Tachograph Card Protection Profile

Second generation components:

- BSI-CC-PP-0091 Digital Tachograph – Tachograph Card Protection Profile
- BSI-CC-PP-0092 Digital Tachograph – EGF Protection Profile
- BSI-CC-PP-0093 Digital Tachograph – Motion Sensor Protection Profile
- BSI-CC-PP-0094 Digital Tachograph – Vehicle Unit Protection Profile

4.3 Annex IC refers to ancillary equipment for calibration (intended for use by approved workshops) and for data downloading (enforcement). These items are not part of the interoperability type approval defined in Annex IC, but issues of their interoperability with different recording equipment are likely to arise.

4.4 Prior to performing interoperability tests for the purposes of equipment type approval, with the collaboration of the component personalisers, using pre-production equipment, the Digital Tachograph Laboratory shall have validated the interoperability tests on such pre-production equipment. Results obtained during validation of methods may be covered by a non-disclosure agreement stipulated by the component personaliser.

4.5 Member/National State authorities may request tests on personalised equipment as part of their tendering process for suppliers of the material and / or services required to implement the smart tachograph infrastructure.

4.6 The security-enforcing functions of the smart tachograph system require symmetric and/or asymmetric keys and certificates to be present in each of the components. These keys and certificates are generated and managed in a cryptographic infrastructure complying to specifications laid down in Annex IC and in the ERCA Certificate Policy [4]. In order to allow components to function correctly during the interoperability tests, they will be provided with test keys and certificates that are generated and managed in a parallel test cryptographic infrastructure. The test infrastructure will function in largely the same way as the production infrastructure (see Section 10.2.1.1).

[2] There is no Common Criteria Protection Profile for first-generation motion sensors. However, security requirements for such motion sensors are included in Appendix 10 of Annex 1B.

5 Risks and mitigations

5.1. Risk: Errors in the conception of a single interoperability test may lead to the deployment of smart tachograph equipment that is incompatible with existing equipment.

Mitigation: Component personalisers shall be consulted during interoperability test definition.

5.2. Risk: Errors in the execution of a single interoperability test may lead to the deployment of smart tachograph equipment that is incompatible with existing equipment.

Mitigation: Component personalisers shall be invited to provide training in the use of their products for Digital Tachograph Laboratory staff prior to type approval tests.

5.3. Risk: A component personaliser enters the type approval process with samples of components whose specifications differ from the models which will eventually enter production.

Mitigation: Access to the reference set of tachograph components maintained at the Digital Tachograph Laboratory shall be granted to Member State type approval authorities and to the Common Criteria authorities should need arise.

5.4. Risk: Smart tachograph component presented for type approval testing does not implement all functionality defined in Annex IC. For example: Annex IC Appendix 2 TCS_11, the card shall provide both protocol T=0 and protocol T=1 implies that vehicle units will offer either the T = 0 or the T = 1 protocol. If the initial interoperability tests are performed only with vehicle units implementing T = 0, interoperability is certifiable only for T = 0. Interoperability problems arising from the untested T = 1 protocol (i.e. on a tachograph card) might remain undetected.

Mitigation: During functional testing, all functionality defined in Annex IC should be explicitly addressed, and this should be clear from the functional certificate.

5.5. Risk: A component personaliser is granted a functional certificate that did not reveal some functional issues and enters the interoperability certification process with samples of components working imperfectly.

Mitigations:

- If, using the standard procedures, interoperability cannot be demonstrated, the Digital Tachograph Laboratory will not grant any interoperability certificate.
- If interoperability can be demonstrated, but the interoperability tests reveal some functional issues, the interoperability certificate will indicate such issues. The type approval authority shall evaluate these issues and may require the personaliser to correct the issues.
- If another component personaliser enters the interoperability certification process but fails because of the previous personaliser's functional issues, the Digital Tachograph Laboratory will not grant any interoperability certificate and shall invite both personalisers to apply corrective measures.

6 Requirements for test samples

6.1 General

6.1.1 Depending on the type of product, a component personaliser seeking interoperability certification shall provide the material listed in one of the sections 6.2 to 6.6 (as applicable) to the Digital Tachograph Laboratory.

6.1.2 The component personaliser shall install Generation-1 and/or Generation-2 cryptographic keys and/or certificates in each component provided to the Digital Tachograph Laboratory, as indicated in the applicable section 6.2 to 6.6.

6.1.3 The material shall be accompanied by a copy of the functional test certificate issued by a Member/National State's type approval authority, and a copy of the security certificate issued by a Common Criteria authority.

6.1.4 The smart tachograph components (i.e. vehicle units and/or motion sensors and/or potential external GNSS facilities and/or external remote communication facilities) and tachograph cards shall remain at the Digital Tachograph Laboratory and shall constitute the reference set of components against which future products shall be compared.

6.1.5 The component personaliser shall provide training in the correct use of the components for Digital Tachograph Laboratory staff. The training shall cover installation, calibration and operation.

6.2 Recording Equipment

6.2.1 Manufacturers of recording equipment wishing to obtain interoperability certification shall supply the following items to the Digital Tachograph Laboratory for the purposes of the interoperability test:

- Six vehicle units (VUs).
- Six motion sensors compatible with the vehicle unit, if such motion sensors are not yet in possession of the Digital Tachograph Laboratory[3]
- Six EGFs compatible with the vehicle unit, if applicable, and if such EGFs are not yet in possession of the Digital Tachograph Laboratory[4].
- Six external remote communication facilities compatible with the vehicle unit, if applicable, and if such EGFs are not yet in possession of the Digital Tachograph Laboratory.

6.2.2 The vehicle units shall comply with all requirements in section 6.3.

6.2.3 The motion sensors shall comply with all requirements in section 6.4.

6.2.4 The External GNSS Facilities (if applicable) shall comply with all requirements in section 6.5.

[3] In case the motions sensors cannot be paired successfully with several vehicle units, the manufacturer shall bring at least two motion sensors for each vehicle units.

[4] In case the EGFs cannot be coupled successfully with several vehicle units, the manufacturer shall bring at least two EGFs for each vehicle units.

6.3 Vehicle Unit

6.3.1 Manufacturers of vehicle units wishing to obtain interoperability certification shall supply two sets of three vehicle units (labelled VU_1.1, VU_2.1 and VU_3.1 for the first set and VU_1.2, VU_2.2 and VU_3.2 for the second set), to the Digital Tachograph Laboratory for the purposes of the interoperability test.

Both sets will be used during the interoperability certification. One set will be used as reference for further certifications and the second set as spare part in case of failure of one equipment of the first set.

6.3.2 Each vehicle unit shall be marked according to Annex IC requirement 225 or 226, with the exception of the approval mark for the equipment type, which is not applicable.

6.3.3 Cryptographic material from the Generation-1 interoperability test set defined in section 10.1 shall be distributed over the six VUs supplied by the manufacturer as shown in Table 2.

	ERCA public key profile	**MSCA certificate profile**	**VU key pair + certificate profile**	**KmVU**
VU_1.x	EUR 01	MSCA 01	VU 01	KmVU_Test
VU_2.x	EUR 01	MSCA 01	VU 02	KmVU_Test
VU_3.x	EUR 01	MSCA 01	VU 03	KmVU_Test

Table 2 Distribution of Gen-1 cryptographic test material over supplied VUs

6.3.4 Cryptographic material from the Generation-2 interoperability test set defined in section 10.2 shall be distributed over the three VUs supplied by the manufacturer as shown in Table 3.

	ERCA certificate profile	**MSCA_VU-EGF certificate profile**	**VU_MA and VU_Sign key pair + certificate profile**	**VU-specific DSRC keys version**	**$K_{M\text{-}VU}$ version**
VU_1.x	EUR_01	MSCA_VU-EGF_01	VU_01	'01'	'01'
VU_2.x	EUR_02	MSCA_VU-EGF_02	VU_02	'02'	'02'
VU_3.x	EUR_03	MSCA_VU-EGF_03	VU_03	'03'	'03'

Table 3 Distribution of Gen-2 cryptographic test material over supplied VUs

6.3.5 No additional ERCA root certificates, link certificates, MSCA certificates, VU_MA and VU_Sign keys, VU-specific DSRC keys and KM-VU keys other than the ones specified above shall be present in the Vehicle Units. Note that DSRC keys are not currently used for any test but they are included for completeness.

6.3.6 The manufacturer shall clearly label each of the supplied Vehicle Units as VU_1.x, VU_2.x or VU_3.x.

6.3.7 The manufacturer shall provide the Digital Tachograph Laboratory with an overview of the cryptographic keys and certificates and personalisation data included in each of the supplied vehicle units, including:

- The clear contents of the first-generation MSCA and VU certificates, in a table formatted according to Table 20: Smart tachograph certificate content
- The plain-text value of the first-generation KmVU
- The clear contents of the second-generation ERCA, MSCA_VU-EGF, VU_MA and VU_Sign certificates, in a table formatted according to Table 24: Smart Tachograph certificate format
- The plain-text value of the second-generation KM-VU
- The plain-text value of the VU-specific DSRC keys
- The VU serial number.

6.3.8 The vehicle unit manufacturer shall indicate if the vehicle unit shall be interoperable with all motions sensors or only with a selected subset of motion sensors. For motion sensors which are not in the possession of the Digital Tachograph Laboratory, the vehicle unit manufacturer shall supply one motion sensor with each vehicle unit. The cables connecting the motion sensor to the vehicle unit shall be 2 metres in length, and shall be supplied complete with connectors.

In case the motions sensors cannot be paired successfully with several vehicle units, the manufacturer shall bring at least two motion sensors for each vehicle units.

The motion sensors shall comply with all requirements in section 6.4.

6.3.9 If applicable, the vehicle unit manufacturer shall indicate if the vehicle unit shall be interoperable with all external GNSS facilities or only with a selected subset of external GNSS facilities. For external GNSS facilities which are not in the possession of the Digital Tachograph Laboratory, the vehicle unit manufacturer shall supply one external GNSS facility with each vehicle unit. The cables connecting the external GNSS facility to the vehicle unit shall be 2 metres in length, and shall be supplied complete with connectors and antennas if applicable.

In case the EGFs cannot be coupled successfully with several vehicle units, the manufacturer shall bring at least two EGFs for each vehicle units.

The External GNSS Facilities (if applicable) shall comply with all requirements in section 6.5.

6.3.10 If applicable, for external remote communication facilities which are not in the possession of the Digital Tachograph Laboratory, the vehicle unit manufacturer shall supply one external remote communication facility with each vehicle unit. The cables connecting the external remote communication facility to the vehicle unit shall be 2 metres in length, and shall be supplied complete with connectors and antennas if applicable.

6.3.11 The manufacturer may provide one calibration equipment and / or one intelligent dedicated equipment (IDE) complete with cable(s) and downloading / calibration connector(s) described in Annex IC Appendix 6. These items will not be subjected to any interoperability test.

6.3.12 The VUs provided by the manufacturer to the Digital Tachograph Laboratory shall be fully personalised. All data structures on the VU shall comply with Appendix 1 of Annex IC.

6.3.13 The VUs provided by the manufacturer to the Digital Tachograph Laboratory shall not be activated.

6.4 Motion Sensor

6.4.1 Manufacturers of motion sensors wishing to obtain interoperability certification shall supply two sets of three motion sensors (labelled MS_1.1, MS_2.1 and MS_3.1 for the first set and MS_1.2, MS_2.2 and MS_3.2 for the second set) to the Digital Tachograph Laboratory for the purposes of the type approval test, including the cables connecting the motion sensor to vehicle unit. These cables shall be 2 metres in length, and shall be supplied complete with connectors.

Both sets will be used during the interoperability certification. One set will be used as reference for further certifications and the second set as spare part in case of failure of one equipment of the first set.

6.4.2 Each motion sensor shall be marked according to Annex IC requirement 225 or 226, with the exception of the approval mark for the equipment type, which is not applicable.

6.4.3 The motion sensor manufacturer shall indicate if the motion sensor shall be interoperable with all type-approved vehicle units or only with a selected subset of type-approved vehicle units.

6.4.4 Each motion sensor shall contain the following Generation-1 security data elements if the motion sensor will also offer the possibility to be paired with a Gen-1 Vehicle Unit, according to req. CSM_111 in Appendix 11:

- The Gen-1 motion sensor pairing key (Kp) shall be encrypted with the Km_Test motion sensor master key from the interoperability test set.
- The motion sensor extended serial number (Ns) shall be encrypted with the identification key derived from the Km_Test motion sensor master key from the interoperability test set.

6.4.5 Each motion sensor shall contain the following Generation-2 security data elements, based on the corresponding version of the motion sensor master key from the Gen-2 test set defined in section 10.2.1.2, as shown in Table 4:

- The Gen-2 motion sensor pairing key K_P shall be encrypted with the corresponding version of the motion sensor master key K_M from the interoperability test set.
- The motion sensor extended serial number (Ns) shall be encrypted with the corresponding version of the identification key K_{ID}.

	Pairing key K_P length	**K_P encrypted with K_M version**	**Ns encrypted with K_{ID} version**
MS_1.x	AES-128	'01'	'01'
MS_2.x	AES-192	'02'	'02'
MS_3.x	AES-256	'03'	'03'

Table 4 Distribution of Gen-2 cryptographic test material over supplied motion sensors

6.4.6 The manufacturer shall clearly label each of the supplied motion sensors as MS_1.x, MS_2.x or MS_3.x.

6.4.7 The manufacturer shall provide the Digital Tachograph Laboratory with an overview of the cryptographic keys included in each of the supplied motion sensors, including:

- The plain-text value of the first-generation TDES pairing key (Kp),
- The plain-text value of the second-generation AES pairing key K_P, see Table 4,
- The unique motion sensor extended serial number (Ns).

6.5 External GNSS Facility

6.5.1 Manufacturers of external GNSS facilities shall supply two sets of three EGFs(labelled EGF_1.1, EGF_2.1 and EGF_3.1 for the first set and EGF_1.2, EGF_2.2 and EGF_3.2 for the second set) to the Digital Tachograph Laboratory for the purposes of the type approval test, including the cables connecting the EGF to the vehicle unit. These cables shall be 2 metres in length, and shall be supplied complete with connectors.

Both sets will be used during the interoperability certification. One set will be used as reference for further certifications and the second set as spare part in case of failure of one equipment of the first set.

6.5.2 Each external GNSS facility shall be marked according to Annex IC requirement 225 or 226, with the exception of the approval mark for the equipment type, which is not applicable.

6.5.3 The external GNSS facility manufacturer shall indicate if the EGF shall be interoperable with all type-approved vehicle units or only with a selected subset of type-approved vehicle units.

6.5.4 Cryptographic material from the Generation-2 interoperability test set defined in section 10.2 shall be distributed over the six EGFs supplied by the manufacturer as shown in Table 5.

	ERCA certificate profile	**MSCA_VU-EGF certificate profile**	**EGF_MA key pair + certificate profile**
EGF_1.x	EUR_01	MSCA_VU-EGF_01	EGF_01
EGF_2.x	EUR_02	MSCA_VU-EGF_02	EGF_02
EGF_3.x	EUR_03	MSCA_VU-EGF_03	EGF_03

Table 5 Distribution of Gen-2 cryptographic test material over supplied EGFs

6.5.5 No additional ERCA root certificates and link certificates, EGF_MA keys other than the ones specified above shall be present in the EGFs.

6.5.6 The manufacturer shall clearly label each of the supplied EGFs as EGF_1.x, EGF_2.x or EGF_3.x.

6.5.7 The manufacturer shall provide the Digital Tachograph Laboratory with an overview of the cryptographic keys and certificates and personalisation data included in each of the supplied vehicle units, including:

- The clear contents of the second-generation ERCA, MSCA_VU-EGF and EGF_MA certificates, in a table formatted according to Table 24: Smart Tachograph certificate format
- The EGF serial number.

6.5.8 The EGFs provided by the manufacturer to the Digital Tachograph Laboratory shall be fully personalised. All data structures on the EGF shall comply with Appendix 1 of Annex IC.

6.6 Tachograph Cards

6.6.1 Suppliers of tachograph cards wishing to obtain interoperability certification shall supply six sets of four tachograph cards (one each of driver, control, company, and workshop card) to the Digital Tachograph Laboratory for the purposes of the type approval test.

6.6.2 Cryptographic material from the Generation-1 interoperability test set defined in section 10.1 shall be distributed over the six sets of cards supplied by the card personaliser as shown in Table 6.

	ERCA public key profile	**MSCA certificate profile**	**Card key pair + certificate profile**	**KmWC (workshop cards only)**
Set 1 and 4	EUR_01	MSCA 02	Driver Card: TC 01 Company Card: TC 01 Control Card: TC 02 Workshop Card: TC 03	KmWC_Test
Set 2 and 5	EUR_01	MSCA 03	Driver Card: TC 04 Company Card: TC 05 Control Card: TC 05 Workshop Card: TC 06	KmWC_Test
Set 3 and 6	EUR_01	MSCA 04	Driver Card: TC 07 Company Card: TC 08 Control Card: TC 09 Workshop Card: TC 09	KmWC_Test

Table 6 Distribution of Gen-1 cryptographic test material over supplied card sets

6.6.3 Cryptographic material from the Generation-2 interoperability test set defined in section 10.2 shall be distributed over the six sets of cards supplied by the card personaliser as shown in Table 3.

	ERCA certificate profile	**MSCA_Card certificate profile**	**Card_MA and Card_Sign[5] key pair + certificate profile**	**$K_{M\text{-}DSRC}$ version (workshop and control cards only)**	**$K_{M\text{-}WC}$ version (workshop cards only)**
Set 1 and 4	EUR_01	MSCA_Card_01	Card_01	'01'	'01'
Set 2 and 5	EUR_02	MSCA_Card_02	Card_02	'02'	'02'
Set 3 and 6	EUR_03	MSCA_Card_03	Card_03	'03'	'03'

Table 7 Distribution of Gen-2 cryptographic test material over supplied VUs

6.6.4 No additional ERCA root certificates, link certificates, MSCA certificates, Card_MA and Card_Sign keys, DSRC master keys and $K_{M\text{-}WC}$ keys other than the ones specified above shall be present in the cards. Note that DSRC keys are not currently used for any test but they are included for completeness.

6.6.5 The card personaliser shall clearly label each of the supplied Cards as Set_1, Set_2, Set_3, Set_4, Set_5 or Set_6.

6.6.6 The card personaliser shall provide the Digital Tachograph Laboratory with an overview of the cryptographic keys and certificates and personalisation data included in each of the supplied cards, including:

- The clear contents of the first-generation MSCA and Card certificates, in a table formatted according to Table 20: Smart tachograph certificate content
- The plain-text value of the first-generation KmWC,
- The clear contents of the second-generation ERCA, MSCA_Card, Card_MA and Card_Sign certificates, in a table formatted according to Table 24: Smart Tachograph certificate format
- The plain-text value of the second-generation $K_{M\text{-}WC,}$
- The PIN value of the workshop cards,
- The Cards serial number.

6.6.7 The characters required to compose the workshop card PIN shall be restricted to the decimal ASCII codes 48 to 57, to ensure that PIN entry into the VU can be achieved using only the numerals 0-9.

6.6.8 The card personaliser shall provide the Digital Tachograph Laboratory with fully personalised cards. All data structures on the card shall comply with Appendix 1 of Annex IC.

[5] Only for Driver Cards and Workshop Cards

7 Test Procedures

7.1 General Considerations

The security-enforcing functions of the smart tachograph system are likely to prevent the use of protocol analysers for recording data exchanged between a vehicle unit and a card. Components under test are therefore considered as "black boxes" whose internal workings are unknown.

Each test description consists of an objective, a rationale, and a description of the expected behaviour. Objectives refer to requirements in Annex IC and Appendices.

The tests are intended to create records and events that will be recorded in the data memories of the vehicle unit and the tachograph card. Therefore each interoperability test sequence shall be preceded and followed by a download of vehicle unit and tachograph card memories. The differences in the contents of the data memories before and after each test sequence shall be compared with the expected behaviour.

Both the vehicle unit and the tachograph card data memories shall be downloaded via the intelligent dedicated equipment (IDE) interface on the front panel of the vehicle unit (see Annex IC Appendix 6).

Interoperability tests involving driver, control, and company cards shall only be performed with complete recording equipment i.e. a vehicle unit paired to its motion sensor and potentially coupled to its external GNSS facility when applicable.

Note: The Digital Tachograph Laboratory may also use software tools provided by component personalisers to facilitate the management of the equipment (e.g. software for preloading activity data on a driver card, or for interpreting the contents of a vehicle unit memory).

7.2 Test Conditions

7.2.1 The interoperability tests are performed in the Digital Tachograph Laboratory of the JRC in Ispra, Italy.

7.2.2 Unless otherwise specified, interoperability tests will be carried out under the following climatic conditions:

- ambient temperature 15°C to 35°C
- relative humidity 30% to 75%
- atmospheric pressure 860 mbar to 1060 mbar

7.2.3 If needed, recording equipment shall be powered on for a warm-up period of approximately 30 minutes prior to commencement of interoperability tests.

7.2.4 Vehicle units shall be installed in an open framework permitting unobstructed air flow around the sides, top, bottom, and rear of the unit housing while ensuring a correct mechanical support.

7.2.5 Prior to starting the interoperability tests, the reference set of cards is tested and downloaded to be sure that the cards are free of major errors which can interfere with the interoperability tests.

7.2.6 Manual operations on the vehicle unit front-panel controls are recorded on an appropriate registration form:

- DTC for the tests on the smart tachograph cards;
- DTVU for the tests on the smart tachograph recording equipment or vehicle unit;
- DTMS for the tests on the smart tachograph motion sensor.
- DTGNSS for the tests on the smart tachograph external GNSS facility.

The data recorded shall include vehicle unit time, card identity, card slot, activity performed and observations of the test engineer.

7.2.7 The interoperability tests are performed following the DTLab test procedures.

7.3 Technical reception and preliminary operations

The technical reception consists in verifying that the component(s) under tests fulfil the requirements of chapter 6 Requirements for test samples.

As vehicle units are supplied not activated, vehicle units under test will be activated and be calibrated for first use in the current vehicle (CalibrationPurpose 3, first calibration in the current vehicle, also called "installation"). The workshop card used for these first calibrations is not relevant.

An initial download of the memory of all the components used (including the cards) is also performed to compare the results of each individual tests to the initial state. The content of the tachograph cards will be wiped before their initial download.

Applicable Components
- Recording Equipment,
- Vehicle Unit,
- tachograph cards.

Objectives
- to check the use of the components,
- to clear the memory (when possible) before to start the tests.
- to get an identical and knows initial state before starting the test.

Rationale
The workshop card pairs the vehicle unit with the motion sensor, couples the vehicle unit with an external GNSS facility if applicable, and activates the recording equipment. This is a necessary preparatory step for all subsequent interoperability tests and provides an opportunity for checking the components under test.
The initial state of all cards used is known and can be compared after the tests with the final states.

Remarks

None

Action in case of failure

Card Rejected: Record card identity and any useful information on the test module. The test is stopped.

Other failure case(s): Record card identity and any useful information on the test module. The test is stopped.

7.4 Calibration Test

According to the definition (*f*) of Annex IC, "calibration" means: *updating or confirming vehicle parameters to be held in the data memory. Vehicle parameters include vehicle identification (VIN, VRN and registering Member State) and vehicle characteristics (w, k, l, tyre size, speed limiting device setting (if applicable), current UTC time, current odometer value); during the calibration of a recording equipment, the types and identifiers of all type approval relevant seals in place shall also be stored in the data memory;*

Calibration Test
Use each workshop card of the reference set to calibrate the recording equipment.

Applicable Component under Test
- Recording Equipment: test to be carried out with all workshop cards of the Set of Reference.
- Vehicle Units: test to be carried out with all workshop cards of the Set of Reference.
- Workshop cards: test to be carried out with all Recording Equipment in the Set of Reference.
- Motion Sensors: test to be carried out with all Vehicle Units in the Set of Reference or with the subset thereof specified by the manufacturer (see req. 6.4.3).
- External GNSS Facilities: test to be carried out with all Vehicle Units in the Set of Reference or with the subset thereof specified by the manufacturer (see req. 6.5.3).

Objectives
According to the requirement 202 of Annex IC, the calibration function shall allow:
- to automatically pair the motion sensor with the VU,
- to automatically couple the external GNSS facility with the VU if applicable,
- to digitally adapt the constant of the recording equipment (k) to the characteristic coefficient of the vehicle (w),
- to adjust the current time within the validity period of the inserted workshop card,
- to adjust the current odometer value,
- to update motion sensor identification data stored in the data memory,
- to update, if applicable, external GNSS facility identification data stored in the data memory,
- to update the types and identifiers of all the seals in place,
- to update or confirm other parameters known to the recording equipment: vehicle identification, w, l, tyre size and speed limiting device setting if applicable.

Rationale
The workshop card pairs the vehicle unit with the motion sensor, couples the vehicle unit with an external GNSS facility if applicable, and activates the recording equipment. This is a necessary preparatory step for all subsequent interoperability tests and provides an opportunity for checking the workshop card.

Req.	Description
385	Vehicle manufacturers or fitters shall activate the installed recording equipment at the latest before the vehicle is used in scope of Regulation (EC) N°. 561/2006.
389	After its activation, the recording equipment shall fully enforce functions and data access rights.
391	The recording and storing functions of the recording equipment shall be fully operational after its activation.

Table 8: Rationale of calibration tests

Expected behavior

Req.	Description
120 **121**	Vehicle unit records calibration activity data: • purpose of calibration; • workshop name and address; • workshop card number, card issuing Member State and card expiry date; • vehicle identification; • parameters updated or confirmed; • seal type and identifier of all seals in place, • ability of the VU to use first generation tachograph cards (enabled or not).
314 **377**	Workshop card records calibration and time adjustment data: • purpose of calibration; • vehicle identification; • parameters updated or confirmed • recording equipment identification (VU part number, VU serial number, motion sensor serial number, remote communication facility serial number* and external GNSS facility serial number if applicable*), • seal type and identifier of all seals in place*, • ability of the VU to use first generation tachograph cards (enabled or not)*.

Table 9: Expected behaviour of VU and workshop cards during calibration tests

* This information is available only in the Tachograph Generation 2 application of a smart tachograph card

Remarks

Use of each Generation-2 workshop card demonstrates that the ECDSA and ECDH algorithms in the vehicle unit and the workshop card operate correctly for all standardised ECC domain parameters used by the card (see section 10.2).

Successful pairing of the vehicle unit and the motion sensor demonstrates that the motion sensor master keys are correctly encoded in the vehicle unit and the workshop card; and that the motion sensor data are correctly encrypted within the motion sensor.

Successful coupling of the vehicle unit and the external GNSS facility (if applicable) demonstrates that the ECDSA and ECDH algorithms in the vehicle unit and the EGF operate correctly for all standardised ECC domain parameters used by the card EGF (see section 10.2).

Generation 1 workshop cards shall be used to calibrate only Generation 1 recording equipment.

Generation 2 workshop cards shall be used to calibrate both Generation 1 and Generation 2 recording equipment.

Action in case of failure

Card Rejected: Record card identity and any useful information on the test module. The test is stopped.

Other failure case(s): Record card identity and any useful information on the test module. The test is stopped.

7.5 Activity Simulation

Description
Use driver, company and control cards in a simulation of system operation to create activity data in the vehicle unit data memory and on the tachograph cards.

Applicable Component under Test
- Recording Equipment: test to be carried out with all cards in the Set of Reference.
- Vehicle Units: test to be carried out with all cards in the Set of Reference.
- Driver, company and control cards: test to be carried out with all Recording Equipment in the Set of Reference.
- Motion Sensors: test to be carried out with all Vehicle Units in the Set of Reference or with the subset thereof specified by the manufacturer (see req. 6.4.3).
- External GNSS Facilities: test to be carried out with all Vehicle Units in the Set of Reference or with the subset thereof specified by the manufacturer (see req. 6.5.3).

Objectives
To create driving activity record, including one over-speeding event and one motion conflict event. To perform company actions. To perform control actions.

The relevant chapters of Annex IC, rather than specific requirements, are referenced in the following table.

Chapter	Description
3.4	Monitoring driver activities
3.7	Company locks management
3.8	Monitoring control activities

Table 10: Objective of activity simulation

Rationale
Creation of activity data records in the vehicle unit memory and in the tachograph cards provide documentary evidence of correct operation of the system components.

Expected behaviour

Req.	Description
46	It shall be possible for the driver and/or the co-driver to manually select WORK, AVAILABILITY, or BREAK/REST.
47	When the vehicle is moving, DRIVING shall be selected automatically for the driver and AVAILABILITY shall be selected automatically for the co-driver.
48	When the vehicle stops, WORK shall be selected automatically for the driver.
49	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).
50	This function shall output activity changes to the recording functions at a resolution of one minute.
63	This function shall allow the management of the locks placed by a company to restrict data access in company mode to itself.

Req.	Description
64	Company locks consist in a start date/time (lock-in) and an end date/time (lock-out) associated with the identification of the company as denoted by the company card number (at lock-in).
65	Locks may be turned 'in' or 'out' in real time only
66	Locking-out shall only be possible for the company whose lock is 'in' (as identified by the first 13 digits of the company card number), or,
67	Locking-out shall be automatic if another company locks in.
68	In the case where a company locks in and where the previous lock was for the same company, then it will be assumed that the previous lock has not been turned 'out' and is still 'in'.
69	This function shall monitor DISPLAYING, PRINTING, VU and card DOWNLOADING, and ROADSIDE CALIBRATION check activities carried while in control mode.
70	This function shall also monitor OVER SPEEDING CONTROL activities while in control mode. An over speeding control is deemed to have happened when, in control mode, the 'over speeding' printout has been sent to the printer or to the display, or when 'events and faults' data have been downloaded from the VU data memory.
105	Vehicle unit records changes of activity, driving status, and driver card insertions or withdrawals: • driving status (*Crew*, *Single*) • slot (*Driver*, *Co-Driver*), • card status in the relevant slot (*Inserted*, *Not Inserted*); • activity (*Driving*, *Availability*, *Work*, *Break/Rest*); • date and time of change.
117	The recording equipment shall record and store in its data memory • Over speeding • Vehicle motion conflict
126	Vehicle unit records control activity data: • date and time of control; • control card number, card issuing Member State and card generation; • type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or roadside calibration checking).
128	The recording equipment shall record and store in its data memory the following data relevant to the 255 most recent company locks: • lock-in date and time, • lock-out date and time, • company card number, card issuing Member State and card generation, • company name and address. Data previously locked by a lock removed from memory due to the limit above, shall be treated as not locked.

Req.	Description

266
291
	Driver card records driver activity data:
	• date;
	• daily presence counter ;
	• total distance travelled by the driver during this day;
	• driver status at 00:00;
	• whenever the driver has changed activity, and/or has changed driving status, and/or has inserted or withdrawn his card:
	  • driving status (*Crew*, *Single*);
	  • slot (*Driver*, *Co-Driver*);
	  • card status in the relevant slot (*Inserted*, *Not Inserted*);
	  • activity (*Driving*, *Availability*, *Work*, *Break/Rest*);
	  • time of the change.

361 **367**	Control card records control activity data: • date and time of control; • type of the control (displaying and/or printing and/or VU downloading and/or card downloading and/or roadside calibration checking); • period downloaded (if any); • VRN and Member State registering authority of vehicle; • card number and card issuing Member State of the driver card controlled.
373 **379**	The company card shall be able to store the following company activity data: • date and time of the activity, • type of the activity (VU locking in and/or out, and/or VU downloading and/or card downloading) • period downloaded (if any), • VRN and Member State registering authority of vehicle, • — card number and card issuing Member State (in case of card downloading).

Table 11: Expected behaviour of VU and cards during simulation activity test

Remarks
Vehicle motion is simulated by a servo motor actuating the motion sensor according to a programmed speed cycle. Simultaneously, a corresponding GNSS signal is generated as input to the GNSS receiver, which is located either in the VU or in an EGF.

During test execution, one over-speeding event shall be generated. Also, one motion conflict shall be generated by actuating the motion sensor without generating a corresponding GNSS signal.

The following sequence of card insertions and operations shall be performed using cards from the same set:

Step		**Card**	**Operation**
1		Driver	Vehicle motion simulation changes of driver activity
2		Company	Lock in Card download VU download lock out
3		Control	VU download Card download Printouts: Driver activities from card daily printout Overspeeding printout Event and faults printout from Card Event and faults printout from VU

Table 12: Sequence of operation for the activity simulation.

Action in case of failure
This test is performed after recognition of the different types of tachograph card by the vehicle unit has been demonstrated. Possible failure modes are not known *a priori*. Record card identity and any useful information on the test module. The test is stopped.

7.6 Cross Check Test

Description
Insert a driver card into a vehicle unit under test, and simulate driver activity. Repeat this operation introducing each driver card in each vehicle unit in one sequence.
Please note that the cards and the VU under tests will have the same key length. The test will be repeated for all key lengths. No cross-check will be carried out between components with different key lengths. It has also to be noted that Generation-2 components will be tested for interoperability against Generation-1 components.

Applicable Component under Test
- Recording Equipment: test to be carried out with all cards in the Set of Reference.
- Vehicle Units: test to be carried out with all cards in the Set of Reference.
- Driver cards: test to be carried out with all Recording Equipment in the Set of Reference.

Objectives
At the end of the sequence, verify that the driving activity records are correctly recorded on the card and in the vehicle unit memories.

Expected behaviour

Req.	Description
46	It shall be possible for the driver and/or the co-driver to manually select WORK, AVAILABILITY, or BREAK/REST.
47	When the vehicle is moving, DRIVING shall be selected automatically for the driver and AVAILABILITY shall be selected automatically for the co-driver.
48	When the vehicle stops, WORK shall be selected automatically for the driver.
49	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).
50	This function shall output activity changes to the recording functions at a resolution of one minute.
102	For each insertion and withdrawal cycle of a driver or workshop card in the equipment, the recording equipment shall record and store in its data memory: • the card holder's surname and first name(s) as stored in the card, • the card's number, issuing Member State and expiry date as stored in the card, • the card generation, • the insertion date and time, • the vehicle odometer value at card insertion, • the slot in which the card is inserted, • the withdrawal date and time, • the vehicle odometer value at card withdrawal, • the following information about the previous vehicle used by the driver, as stored in the card: • VRN and registering Member State, • VU generation (when available), • card withdrawal date and time, • a flag indicating whether, at card insertion, the card holder has manually entered activities or not.

Req.	Description
105	Vehicle unit records changes of activity, driving status, and driver card insertions or withdrawals: • driving status (*Crew*, *Single*) • slot (*Driver*, *Co-Driver*), • card status in the relevant slot (*Inserted*, *Not Inserted*); • activity (*Driving*, *Availability*, *Work*, *Break/Rest*); • date and time of change.

266
291
	Driver card records driver activity data:
	• date;
	• daily presence counter ;
	• total distance travelled by the driver during this day;
	• driver status at 00:00;
	• whenever the driver has changed activity, and/or has changed driving status, and/or has inserted or withdrawn his card:
	  • driving status (*Crew*, *Single*);
	  • slot (*Driver*, *Co-Driver*);
	  • card status in the relevant slot (*Inserted*, *Not Inserted*);
	  • activity (*Driving*, *Availability*, *Work*, *Break/Rest*);
	  • time of the change.

269 **294**	The driver card shall be able to store, for each calendar day where the card has been used, and for each period of use of a given vehicle that day (a period of use includes all consecutive insertion / withdrawal cycle of the card in the vehicle, as seen from the card point of view), the following data: • date and time of first use of the vehicle (i.e. first card insertion for this period of use of the vehicle, or 00h00 if the period of use is on-going at that time), • vehicle odometer value at that time, • date and time of last use of the vehicle, (i.e. last card withdrawal for this period of use of the vehicle, or 23h59 if the period of use is on-going at that time), • vehicle odometer value at that time, • VRN and registering Member State of the vehicle, • VIN of the vehicle (Generation 2 data structure only).

Table 13: Expected behaviour of VU and cards during Cross check test

All driving activities must be printed on the ticket of each vehicle unit.

8 Smart tachograph cards analysis

The tachograph cards are analyzed using a dedicated application, before and after each of the tests described above.

The following tables highlight the tachograph card elementary files (EFs) which are analysed according the test performed.

8.1 Master File

File ID	Elementary File		All types of cards
00 02	EF ICC		X
00 05	EF IC		X
2F 00	EF DIR		X
2F 01	EF ATR / INFO	(presence conditional)	X
00 06	EF Extended_Length	(presence conditional)	X

Table 14: Card elementary file test on files in the MF

8.2 Gen-1 application

File ID	Elementary File	Driver Card	Workshop Card	Control Card	Company Card
05 01	EF APPLICATION_IDENTIFICATION	X	X	X	X
C1 00	EF CARD_CERTIFICATE	X	X	X	X
C1 08	EF CA_CERTIFICATE	X	X	X	X
05 20	EF IDENTIFICATION	X	X	X	X
05 0E	EF CARD_DOWNLOAD	X			
05 09	EF CARD_DOWNLOAD		X		
05 21	EF DRIVING_LICENCE_INFO	X			
05 0A	EF CALIBRATION		X		
05 0B	EF SENSOR_INSTALLATION_DATA				
05 02	EF EVENTS_DATA	X	X		
05 03	EF FAULTS_DATA	X	X		
05 04	EF DRIVER_ACTIVITY_DATA	X	X		
05 05	EF VEHICLES_USED	X	X		
05 06	EF PLACES	X	X		
05 07	EF CURRENT_USAGE	X	X		
05 08	EF CONTROL_ACTIVITY_DATA	X	X		
05 22	EF SPECIFIC_CONDITIONS	X	X		
05 0C	EF CONTROLLER_ACTIVITY_DATA			X	
05 0D	EF COMPANY_ACTIVITY_DATA				X

Table 15: Card elementary file test on files in DF Tachograph

8.3 Gen-2 application

File ID	Elementary File	Driver Card	Workshop Card	Control Card	Company Card
05 01	EF APPLICATION_IDENTIFICATION	X	X	X	X
C1 00	EF CARDMA_CERTIFICATE	X	X	X	X
C1 01	EF CARDSIGNCERTIFICATE	X	X	X	X
C1 08	EF CA_CERTIFICATE	X	X	X	X
C1 09	EF LINK_CERTIFICATE	X	X	X	X
05 20	EF IDENTIFICATION	X	X	X	X
05 0E	EF CARD_DOWNLOAD	X			
05 09	EF CARD_DOWNLOAD		X		
05 21	EF DRIVING_LICENCE_INFO	X			
05 0A	EF CALIBRATION		X		
05 0B	EF SENSOR_INSTALLATION_DATA				
05 02	EF EVENTS_DATA	X	X		
05 03	EF FAULTS_DATA	X	X		
05 04	EF DRIVER_ACTIVITY_DATA	X	X		
05 05	EF VEHICLES_USED	X	X		
05 06	EF PLACES	X	X		
05 07	EF CURRENT_USAGE	X	X		
05 08	EF CONTROL_ACTIVITY_DATA	X	X		
05 22	EF SPECIFIC_CONDITIONS	X	X		
05 23	EF VEHICLEUNITS_USED	X	X		
05 24	EF GNSS_PLACES	X	X		
05 0C	EF CONTROLLER_ACTIVITY_DATA			X	
05 0D	EF COMPANY_ACTIVITY_DATA				X

Table 16: Card elementary file test on files in DF Tachograph_G2

9 Mutual Authentication protocols

The scope of this document includes second-generation (smart) tachograph equipment only. However, since second-generation tachograph equipment has to be interoperable with first-generation tachograph equipment, both the Generation-1 and Generation-2 mutual authentication protocols have to be taken into account during the interoperability tests. These protocols are summarised below, where the description focuses on the different keys that are used during the cryptographic operations that are part of each protocol.

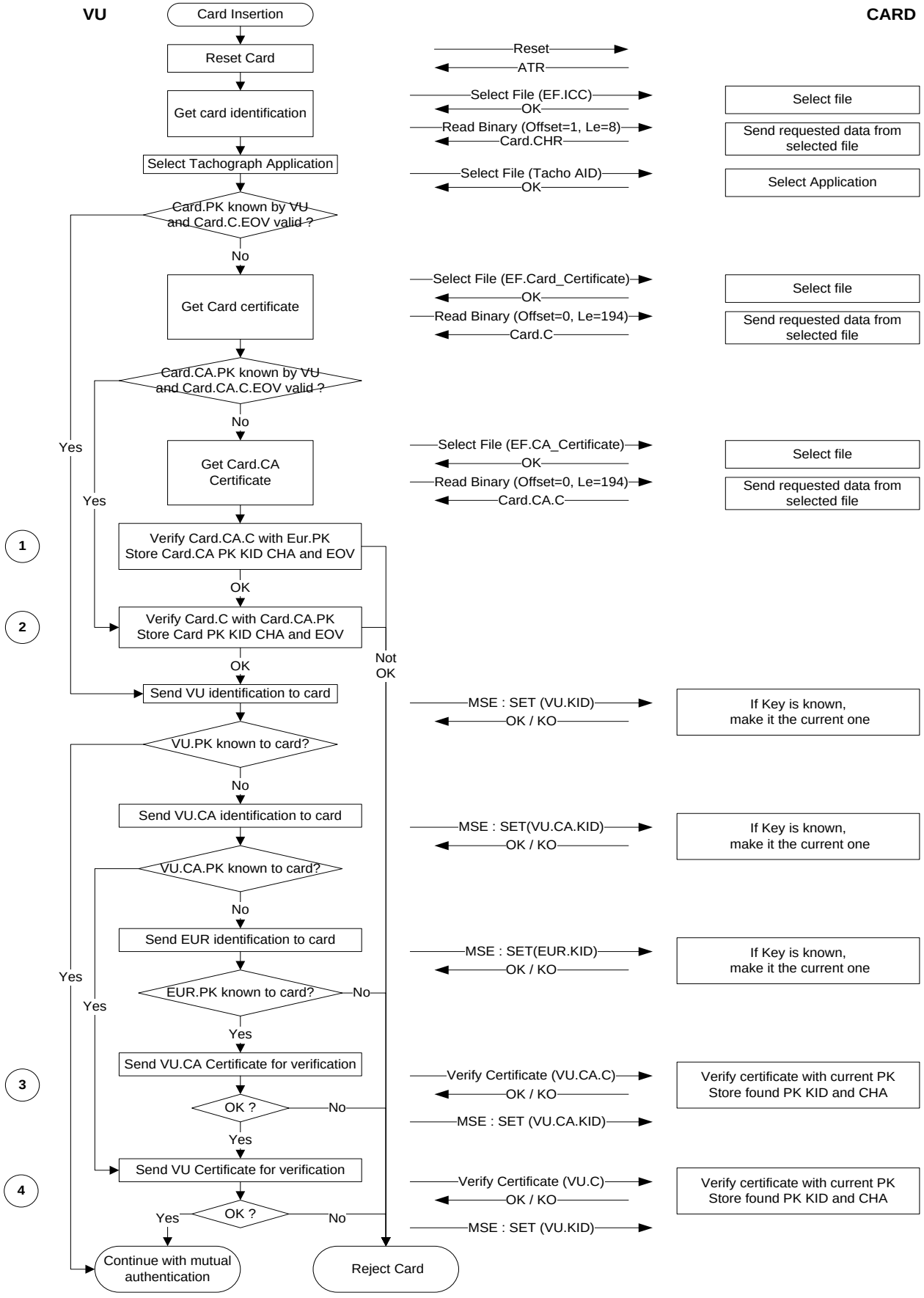
Note that during the interoperability testing the general structure of the Mutual Authentication process is tested, but that specific use cases (e.g. certificate expiration, card internal time management (Gen-2 only), the link certificate mechanism (Gen-2 only) are not covered. Such detailed testing of the Mutual Authentication process should be done during functional testing.

9.1 Generation-1

Annex IC, Appendix 11, requirement CSM_020 defines the Generation-1 mutual authentication protocol that is required before data can be exchanged between a tachograph card and a VU. It is reproduced in Figure 1. The protocol requires the successful completion of at most 12 RSA operations, indicated by circled numbers in the left margin of Figure 1 and summarised in Table 17.

RSA operation	Executed by	Key used, see Section 10.1.1 (PK = public key; SK = private key)
1	VU	EUR.PK
2	VU	MSCA.PK (from Card)
3	Card	EUR.PK
4	Card	MSCA.PK (from VU)
5	Card	Card.SK
6	Card	VU.PK
7	VU	VU.SK
8	VU	Card.PK
9	VU	VU.SK
10	VU	Card.PK
11	Card	Card.SK
12	Card	VU.PK

Table 17: Summary of RSA operations in the Generation-1 mutual authentication protocol


VU
CARD
Card Insertion
Reset Card
Reset
ATR
Get card identification
Select File (EF.ICC)
OK
Select file
Read Binary (Offset=1, Le=8)
Card.CHR
Send requested data from selected file
Select Tachograph Application
Select File (Tacho AID)
OK
Select Application
Card.PK known by VU and Card.C.EOV valid ?
No
Get Card certificate
Select File (EF.Card_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.C
Send requested data from selected file
Card.CA.PK known by VU and Card.CA.C.EOV valid ?
No
Yes
Get Card.CA Certificate
Select File (EF.CA_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.CA.C
Send requested data from selected file
Yes
1
Verify Card.CA.C with Eur.PK
Store Card.CA PK KID CHA and EOV
OK
2
Verify Card.C with Card.CA.PK
Store Card PK KID CHA and EOV
OK
Not OK
Send VU identification to card
MSE : SET (VU.KID)
OK / KO
If Key is known, make it the current one
VU.PK known to card?
No
Send VU.CA identification to card
MSE : SET(VU.CA.KID)
OK / KO
If Key is known, make it the current one
VU.CA.PK known to card?
No
Send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
Yes
Yes
EUR.PK known to card?
No
Yes
Send VU.CA Certificate for verification
3
Verify Certificate (VU.CA.C)
OK / KO
Verify certificate with current PK
Store found PK KID and CHA
OK ?
No
MSE : SET (VU.CA.KID)
Yes
Send VU Certificate for verification
4
Verify Certificate (VU.C)
OK / KO
Verify certificate with current PK
Store found PK KID and CHA
Yes
OK ?
No
MSE : SET (VU.KID)
Continue with mutual authentication
Reject Card

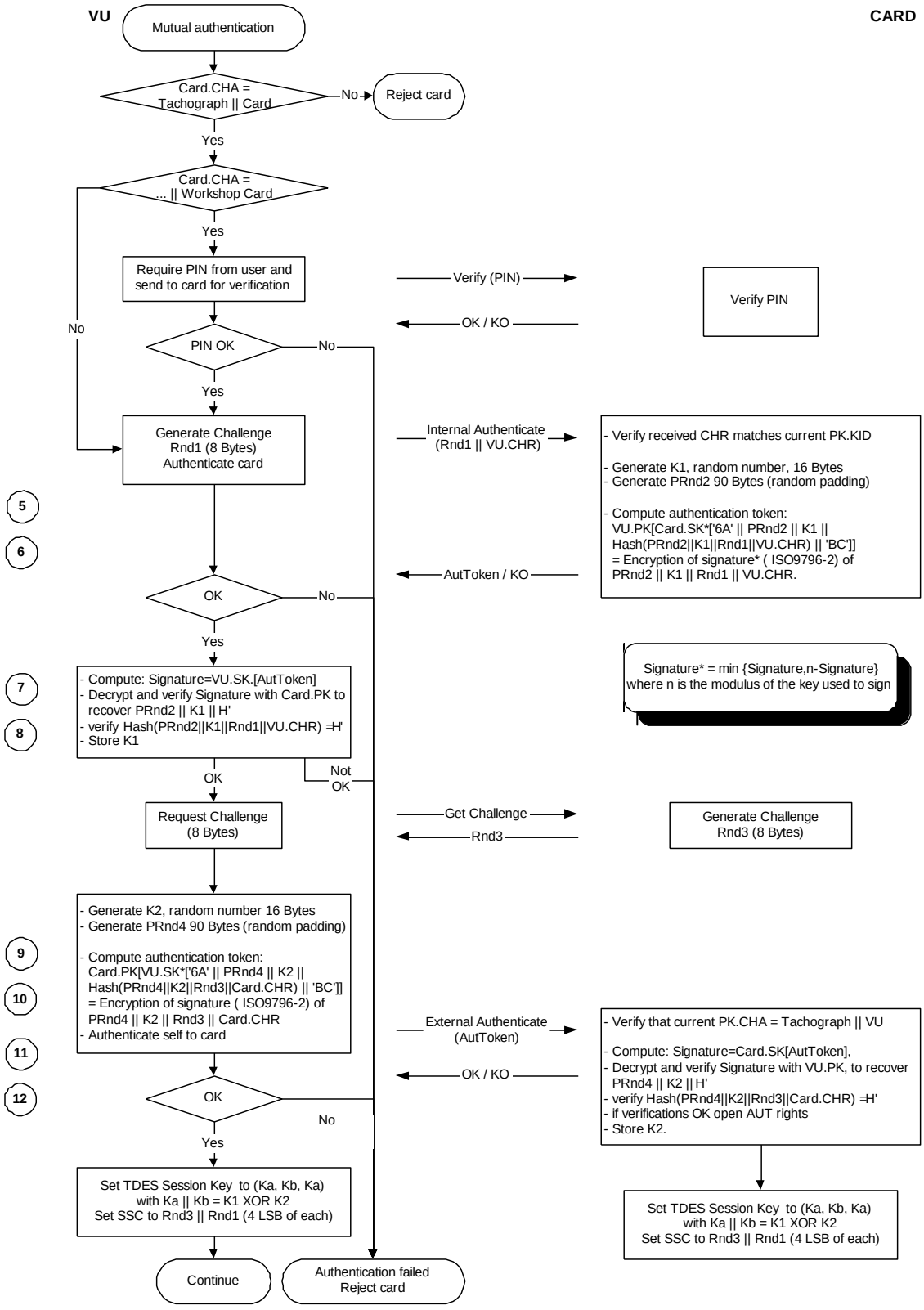


Figure 1 Generation-1 mutual authentication protocol

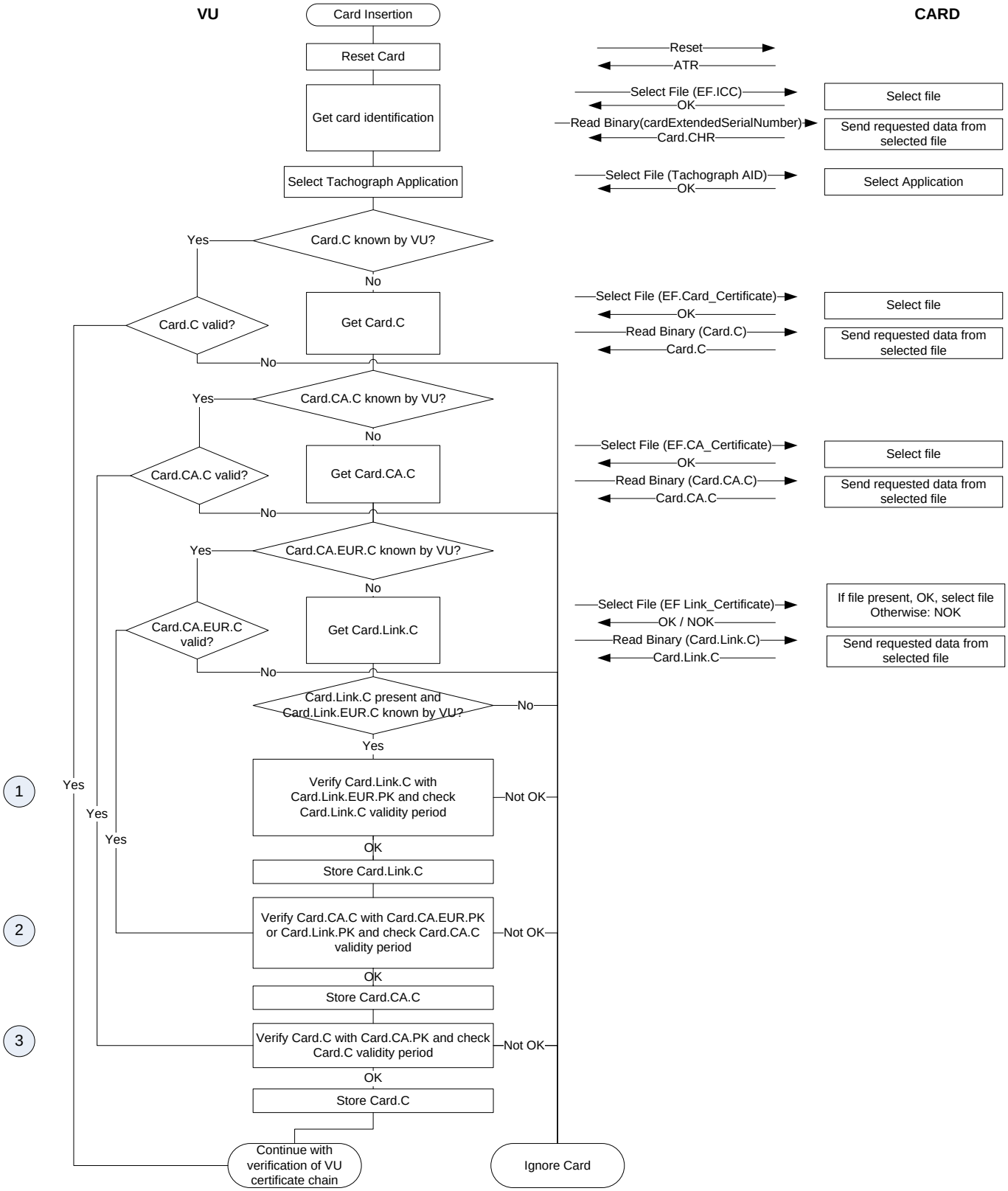
9.2 Generation-2

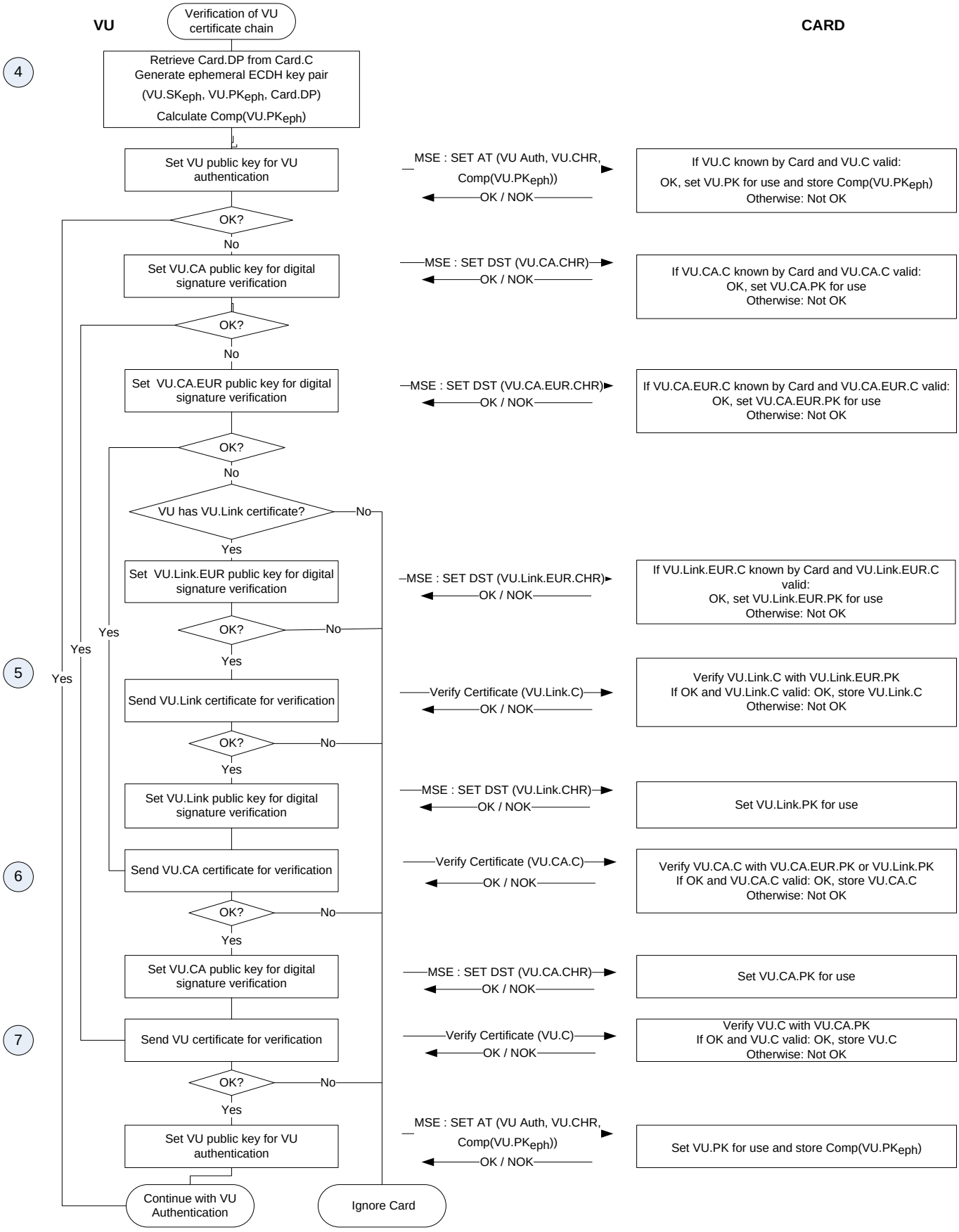
Annex IC, Appendix 11, Sections 10 and 11 define the Generation-2 mutual authentication protocol that is required before data can be exchanged between a VU and a Card or between a VU and an External GNSS Facility. This protocol is reproduced in Figure 2 below.

The protocol requires the successful completion of at most 11 ECC operations, indicated by circled numbers in the left margin of Figure 2 and summarised in Table 18.

ECC operation	**Executed by**	**Key used, see** Table 23: Distribution of ECC domain parameters over test certificates **in Section 10.2.1** **(PK = public key; SK = private key)**	**Notes**
1	VU	EUR.PK	Link certificates will not be used during interoperability test, so this operation will not be tested
2	VU	EUR.PK	
3	VU	MSCA_Card.PK	
4	VU	($VU.PK_{eph}$, $VU.SK_{eph}$)	VU generates ephemeral key pair based on ECC domain parameters used by card.
5	Card / EGF	EUR.PK	Link certificates will not be used during interoperability test, so this operation will not be tested
6	Card / EGF	EUR.PK	-
7	Card / EGF	MSCA_VU-EGF.PK	-
8	VU	VU_MA.SK	-
9	Card / EGF	VU_MA.PK	-
10	Card / EGF	$VU.PK_{eph}$ Card_MA.SK	DH key agreement
11	VU	$VU.SK_{eph}$ Card_MA.PK	DH key agreement

Table 18: Summary of ECC operations in the Generation-2 mutual authentication protocol


VU
CARD
Card Insertion
Reset Card
Get card identification
Select Tachograph Application
Card.C known by VU?
Yes
No
Card.C valid?
Get Card.C
Card.CA.C known by VU?
Card.CA.C valid?
Get Card.CA.C
Card.CA.EUR.C known by VU?
Card.CA.EUR.C valid?
Get Card.Link.C
Card.Link.C present and Card.Link.EUR.C known by VU?
Verify Card.Link.C with Card.Link.EUR.PK and check Card.Link.C validity period
Not OK
OK
Store Card.Link.C
Verify Card.CA.C with Card.CA.EUR.PK or Card.Link.PK and check Card.CA.C validity period
Store Card.CA.C
Verify Card.C with Card.CA.PK and check Card.C validity period
Store Card.C
1
2
3
Continue with verification of VU certificate chain
Ignore Card
Reset
ATR
Select File (EF.ICC)
OK
Select file
Read Binary(cardExtendedSerialNumber)
Card.CHR
Send requested data from selected file
Select File (Tachograph AID)
OK
Select Application
Select File (EF.Card_Certificate)
OK
Select file
Read Binary (Card.C)
Card.C
Send requested data from selected file
Select File (EF.CA_Certificate)
OK
Select file
Read Binary (Card.CA.C)
Card.CA.C
Send requested data from selected file
Select File (EF Link_Certificate)
OK / NOK
If file present, OK, select file
Otherwise: NOK
Read Binary (Card.Link.C)
Card.Link.C
Send requested data from selected file


VU
CARD
Verification of VU certificate chain
4
Retrieve Card.DP from Card.C
Generate ephemeral ECDH key pair
(VU.SKeph, VU.PKeph, Card.DP)
Calculate Comp(VU.PKeph)
Set VU public key for VU authentication
MSE : SET AT (VU Auth, VU.CHR, Comp(VU.PKeph))
OK / NOK
If VU.C known by Card and VU.C valid:
OK, set VU.PK for use and store Comp(VU.PKeph)
Otherwise: Not OK
OK?
No
Set VU.CA public key for digital signature verification
MSE : SET DST (VU.CA.CHR)
OK / NOK
If VU.CA.C known by Card and VU.CA.C valid:
OK, set VU.CA.PK for use
Otherwise: Not OK
OK?
No
Set VU.CA.EUR public key for digital signature verification
MSE : SET DST (VU.CA.EUR.CHR)
OK / NOK
If VU.CA.EUR.C known by Card and VU.CA.EUR.C valid:
OK, set VU.CA.EUR.PK for use
Otherwise: Not OK
OK?
No
VU has VU.Link certificate?
No
Yes
Set VU.Link.EUR public key for digital signature verification
MSE : SET DST (VU.Link.EUR.CHR)
OK / NOK
If VU.Link.EUR.C known by Card and VU.Link.EUR.C valid:
OK, set VU.Link.EUR.PK for use
Otherwise: Not OK
OK?
No
Yes
Yes
Yes
5
Send VU.Link certificate for verification
Verify Certificate (VU.Link.C)
OK / NOK
Verify VU.Link.C with VU.Link.EUR.PK
If OK and VU.Link.C valid: OK, store VU.Link.C
Otherwise: Not OK
OK?
No
Yes
Set VU.Link public key for digital signature verification
MSE : SET DST (VU.Link.CHR)
OK / NOK
Set VU.Link.PK for use
6
Send VU.CA certificate for verification
Verify Certificate (VU.CA.C)
OK / NOK
Verify VU.CA.C with VU.CA.EUR.PK or VU.Link.PK
If OK and VU.CA.C valid: OK, store VU.CA.C
Otherwise: Not OK
OK?
No
Yes
Set VU.CA public key for digital signature verification
MSE : SET DST (VU.CA.CHR)
OK / NOK
Set VU.CA.PK for use
7
Send VU certificate for verification
Verify Certificate (VU.C)
OK / NOK
Verify VU.C with VU.CA.PK
If OK and VU.C valid: OK, store VU.C
Otherwise: Not OK
OK?
No
Yes
Set VU public key for VU authentication
MSE : SET AT (VU Auth, VU.CHR, Comp(VU.PKeph))
OK / NOK
Set VU.PK for use and store Comp(VU.PKeph)
Continue with VU Authentication
Ignore Card

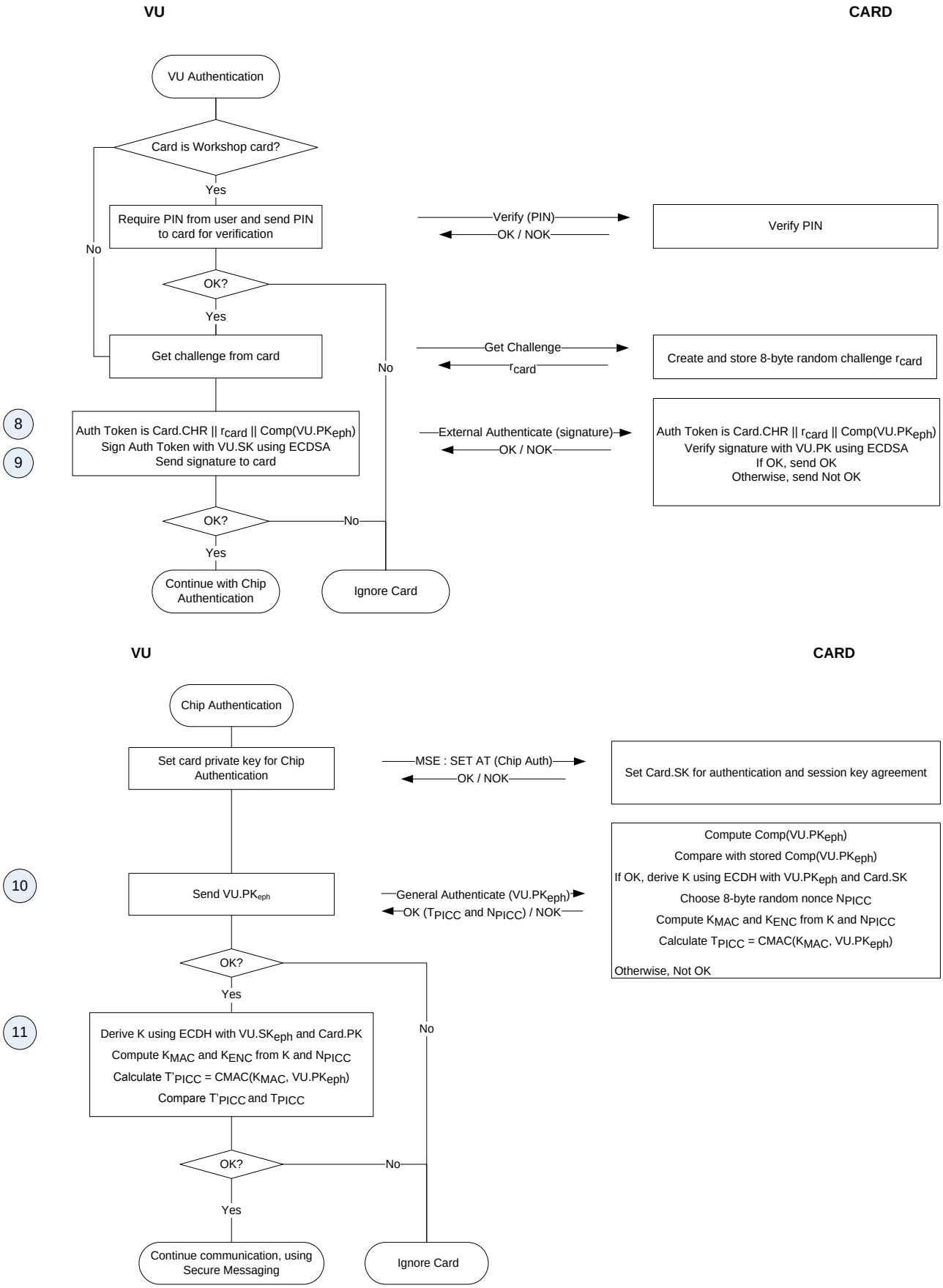


Figure 2 Generation-2 mutual authentication protocol

10 Interoperability Test Keys and Certificates

This section describes the collection of keys and tachograph certificates requested by the Digital Tachograph Laboratory for testing purposes. They are organised in Generation-1 and Generation-2 keys and certificates, necessary for the execution of the two generations of the mutual authentication protocol in the test environment.

10.1 Generation-1

To provide component personalisers with a common basis for testing their implementations of the mutual authentication and pairing protocols, equipment test keys are available from the Digital Tachograph Laboratory (DTLab).

Component personalisers may opt for internal generation of equipment keys. This process ensures confidentiality of the equipment private key. Internally generated keys shall require certification by one of the Member/National State keys.

Alternatively, component personalisers may opt for external generation of equipment keys. In this case, component personalisers may use equipment keys and certificates provided by the Digital Tachograph Laboratory.

This section describes the collection of RSA keys, TDES keys, and smart tachograph certificates created by the Test ERCA for testing purposes. The collection is available from the website of the Digital Tachograph Laboratory (https://dtc.jrc.ec.europa.eu/dtc_interoperability_laboratory.php) or by sending an email to jrc-iot@ec.europa.eu.

The test set consists of chains of public key and certificates linked by the Certification Authority Reference (CAR, see Annex IC Appendix 11 CSM_018).

The keys and certificates in the interoperability test set are registered in the database of the ERCA. Test certificates are identified by the ASCII characters 'T' and 'K' (hexadecimal values 54h and 4Bh) in the AdditionalInfo fields of the Certification Authority Reference.

10.1.1 Interoperability Test Keys

The RSA parameters of the test keys are chosen to exercise the implementations of the RSA algorithm developed by the different equipment manufacturers.
Annex IC Appendix 11 CSM_014 states:
RSA keys shall have (whatever the level) the following lengths: modulus n 1024 bits, public exponent e 64 bits maximum, private exponent d 1024 bits.

This implies the following conditions on the RSA parameters:
The modulus *n* and the private exponent *d* shall be odd integers, falling within the range

$$2^{1023} + 1 \leq n \leq 2^{1024} - 1$$

The public exponent *e* shall be an odd integer, falling within the range

$$3 \leq e \leq 2^{64} - 1$$

As shown in Table 17, public keys (*n, e*) are used in RSA operations 1, 2, 3, 4, 6, 8, 10 and 12 indicated in Figure 1 in section 9.1. Private keys (*n, d*) are used in the operations 5, 7, 9, and 11.

Correct implementation of the RSA algorithm against extreme values of the public exponent *e* can therefore be tested by appropriate Member State CA keys. Correct operation of the digital signature algorithm can be tested by extreme values of the modulus *n* in equipment keys.

To ensure that implementations of the RSA algorithm are correct and complete, the interoperability test set includes keys with randomly generated and deliberately selected values of *e* and *n*.

As shown in Table 19, extreme values of the public exponent e (3 and 2^{64}-1) are used in Member State keys. Extreme values of the modulus n (close to 2^{1023} + 1 or 2^{1024} - 1) are used in equipment keys. Such keys are obtained by constraining the ranges of values from which the prime factors *p* and *q* are drawn (*n* = *p q*). Note that, having selected values for *e* and *n*, the values of the private exponent *d* are determined by the condition:

$$e \cdot d \equiv 1 \, mod\big((p-1)(q-1)\big)$$

Key/Certificate Profile	e	n	EOV	Used to sign
EUR 01	Random	Random	N/A	MSCA 01 / 02 / 03 / 04
MSCA 01	Random		Undefined	VU 01 / 02 / 03
MSCA 02	3		Defined	TC 01 / 02 / 03
MSCA 03	Random			TC 04 / 05 / 06
MSCA 04	2^{64} - 1			TC 07 / 08 / 09
VU 01	65537	Low	Undefined	Authentication tokens (digital signatures)
VU 02		Random		
VU 03		High		
TC 01 / 04 / 07		Low	Defined	
TC 02 / 05 / 08		Random		
TC 03 / 06 / 09		High		

Table 19: Distribution of values for RSA parameters *e, n* and for EOV over test certificates

Note that Table 19 identifies key and certificate profiles, not unique certificates. As shown in Table 20: Smart tachograph certificate content, each certificate is identified by means of a certificate holder reference (CHR), encoded as data type `KeyIdentifier` described in Annex IC, Appendix 1. To avoid possible management problems, the CHR of any certificate

used during interoperability testing must be unique. The Digital Tachograph Laboratory shall keep track of the profile associated with each device.

Table 19 shows how a Member State private key is used to sign a batch of equipment key certificates. Within each batch of equipment keys, there are keys with low, random, and high moduli.

Certain values of the public exponent *e* reduce the time required to perform RSA computations. These are prime numbers in whose binary representation only two bits are set, e.g. 3 (11_2), 17 (10001_2), and 65537 (10000000000000001_2). To take advantage of this fact, the value 65537 is used for *e* in all equipment level keys.

In addition to the RSA keys described above, a single unique TDES motion sensor master key Km is available for testing purposes. This key has been derived by XOR-ing two keys KmWC and KmVU, as specified in Appendix 11.

10.1.2 Identification of Public Keys

Smart tachograph Generation-1 certificate contents are defined in Annex IC Appendix 11 CSM_017 and summarised in. The certificate format is defined in Annex IC Appendix 11 CSM_018.

Name	Full Name	Length [bytes]	Remarks
CPI	Certificate Profile Identifier	1	Certificate structure descriptor value 01 for current version
CAR	Certification Authority Reference	8	Identifier of CA key used to produce the certificate.
CHA	Certificate Holder Authorisation	6	Fixed part: FFh TACHO
	Equipment Type	1	Variable part: equipment type
EOV	End of validity	4	32-bit integer: seconds elapsed since midnight 1970-01-01
CHR	Certificate Holder Reference	8	Identifier of RSA key encoded in the certificate
n	Modulus	128	Public Key (modulus)
e	Public exponent	8	Public Key (exponent)
	Total	164	

Table 20: Smart tachograph certificate content

The certificate issued is a digital signature with partial recovery of the certificate content in accordance with ISO/IEC 9796-2, with the Certification Authority Reference appended. The rationale for appending the CAR is given in Annex IC Appendix 11 CSM_018 Note 2: *CAR, being hidden by the signature, is also appended to the signature, such that the Public Key of the Certification Authority may be selected for the verification of the certificate.*

The format of a `KeyIdentifier` (CHR) appropriate for Member State certificates permits the identification of the Member State (data type `NationNumeric` and `NationAlpha`, see definitions in Annex IC Appendix 1).

The format of the CHR appropriate for equipment certificates identifies the equipment manufacturer (data type `ManufacturerCode`, see definition in Annex IC Appendix 1). The

assignment of manufacturer codes is the responsibility of the Digital Tachograph Laboratory.

The Certificate Holder Authorisation permits the identification of the equipment type.

The possible values for *e* and *n* in test certificates are specified in section 10.1.1.

10.1.3 Validity Period Assignment

As required by Annex IC Appendix 11 CSM_017, smart tachograph Generation-1 public key certificates contain an end-of-validity date (see EOV, Table 19).

During a mutual authentication exchange (Annex IC Appendix CSM_020 and Figure 1) the vehicle unit checks the validity of the tachograph card by comparing UTC date and time from its internal clock (Annex IC requirement 027) with the EOV dates encoded in the MSCA public key certificate (MSCA.C) and the tachograph card public key certificate (TC.C). To avoid problems related to expired Test certificates, all Test certificates for Tachograph cards and MSCAs for those cards will have an expiry date at 01-01-2100. This expiry date is identical to the expiry date of Gen-2 certificates (which will reside in the same cards supplied by the component personaliser for interoperability testing), see section 10.2.3.

Tachograph cards have no independent source of time, and Generation-1 cards therefore cannot check the validity of a public key certificate received from an alleged vehicle unit. The EOV date encoded in Generation-1 vehicle unit certificates is therefore set to an undefined value ('FF FF FF FF'h; 32 bits all set to 1) according to Annex IC Appendix 11 CSM_017.

10.2 Generation-2

In order to have a common basis for testing the implementations of the mutual authentication and pairing protocols, component personalisers wishing to obtain an interoperability certificate for a Smart Tachograph component shall ensure that the components they supply to the Digital Tachograph Laboratory contain the necessary keys and certificates.

10.2.1 Interoperability Test Keys

Second-generation public/private key pairs are based on Elliptic Curve Cryptography (ECC), symmetric keys are based on the AES algorithm, whereas SHA-2 has been adopted as hash algorithm.

All Generation-2 Test keys and certificates shall comply with all applicable requirements in Appendix 11 Part B, with the exception of the validity periods, as stated in section 10.2.3.

A number of pre-defined key lengths and hash sizes have been specified and combined to form cipher suites, which ensure a consistent level of security for all interactions of the Smart Tachograph components. The cipher suites are summarised in Table 21: Cipher

suites defined for the Smart Tachograph system. All system components must support all cipher suites.

Cipher suite	ECC key size (bits)	AES key length (bits)	Hashing algorithm
CS#1	256	128	SHA-256
CS#2	384	192	SHA-384
CS#3	512/521	256	SHA-512

Table 21: Cipher suites defined for the Smart Tachograph system

For Elliptic Curve Cryptography there is the need to choose domain parameters. Appendix 11 of Annex IC allows two sets of standardised domain parameters, the NIST and Brainpool domain parameters. Both for the NIST and the Brainpool standard a set of domain parameters for each of the key sizes specified in table 21 has been selected.

The complete set is shown in Table 22: Allowed standardised domain parameters for ECC

Name	Key size (bits)
NIST P-256	256
BrainpoolP256r1	256
NIST P-384	384
BrainpoolP384r1	384
BrainpoolP512r1	512
NIST P-521	521

Table 22: Allowed standardised domain parameters for ECC

The following principles have been established regarding the use of generation-2 cryptography during interoperability testing:

- Either all three Brainpool elliptic curve standardised domain parameters or all three NIST elliptic curve standardised domain parameters specified in Appendix 11 must be used in VUs, cards and (if applicable) EGFs, so as to test the three possible key lengths in the Smart Tachograph system. For the same reason, all of the three lengths for AES keys defined in Appendix 11 will be used in VUs, cards and motion sensors.
- The Link certificate mechanism will not be used during the interoperability test, i.e. equipment will only be cross-tested (see section 7.6) with equipment using cryptographic keys and certificates of the same length.

For the purposes of the interoperability test, a number of profiles have been defined for ERCA, MSCA and equipment test certificates. These are summarised in Table 23: Distribution of ECC domain parameters over test certificates. Their usage is clarified in Sections 10.2.1.2, 10.2.1.3 and 10.2.1.4.

Key/Certificate Profile	Standardised Domain Parameters	Used to sign
EUR_01	BrainpoolP256r1 or NIST P-256, see section 10.2.1.2	MSCA_01
EUR_02	BrainpoolP384r1 or NIST P-384, see section 10.2.1.2	MSCA_02
EUR_03	BrainpoolP512r1 or NIST P-521, see section 10.2.1.2	MSCA_03
MSCA_Card_01	BrainpoolP256r1 or NIST P-256, see section 10.2.1.3	Card_01
MSCA_Card_02	BrainpoolP384r1 or NIST P-384, see section 10.2.1.3	Card_02
MSCA_Card_03	BrainpoolP512r1 or NIST P-521, see section 10.2.1.3	Card_03
MSCA_VU-EGF_01	BrainpoolP256r1 or NIST P-256, see section 10.2.1.3	VU_01, EGF_01
MSCA_VU-EGF_02	BrainpoolP384r1 or NIST P-384, see section 10.2.1.3	VU_02, EGF_02
MSCA_VU-EGF_03	BrainpoolP512r1 or NIST P-521, see section 10.2.1.3	VU_03, EGF_03
Card_01	BrainpoolP256r1 or NIST P-256, see section 10.2.1.4	-
Card_02	BrainpoolP384r1 or NIST P-384, see section 10.2.1.4	-
Card_03	BrainpoolP512r1 or NIST P-521, see section 10.2.1.4	-
VU_01	BrainpoolP256r1 or NIST P-256r1, see section 10.2.1.4	-
VU_02	BrainpoolP384r1 or NIST P-384r1, see section 10.2.1.4	-
VU_03	BrainpoolP512r1 or NIST P-521r1, see section 10.2.1.4	-
EGF_01	BrainpoolP256r1 or NIST P-256r1, see section 10.2.1.4	-
EGF_02	BrainpoolP384r1 or NIST P-384r1, see section 10.2.1.4	-
EGF_03	BrainpoolP512r1 or NIST P-521r1, see section 10.2.1.4	-

Table 23: Distribution of ECC domain parameters over test certificates

Note that Table 23: Distribution of ECC domain parameters over test certificates identifies certificate profiles, not unique certificates. As shown in Section 10.2.2, each certificate is identified by means of a certificate holder reference (CHR), encoded as data type `KeyIdentifier` described in Annex IC, Appendix 1. To avoid possible management problems, the CHR of any certificate used during interoperability testing must be unique. The CHR of a Test MSCA certificate is determined by the MSCA and communicated to the ERCA in the Certificate Signing Request for that certificate. The CHR of a Test equipment certificate is determined by the component personaliser. The Digital Tachograph Laboratory shall keep track of the profile associated with each certificate.

As shown in Table 18, only the operations 2, 3, 4, 6, 7, 8, 9, 10, 11 of the Mutual Authentication protocol are tested during interoperability tests. They are specifically tested only according to the combinations of keys and certificates profiles summarised in Table 23: Distribution of ECC domain parameters over test certificates. In general, all possible test combinations have to be evaluated during functional tests.

10.2.1.1 Generating Interoperability Test Keys and Certificates

Keys and certificates for interoperability testing will be generated and distributed in the same way as the keys and certificates for production (see Annex IC and the ERCA Certificate Policy [4]), to the maximum extent possible and with the exceptions listed in this section and in section 10.2.1.5. At the ERCA level a Test ERCA system is available that is explicitly devoted to manage Interoperability Test keys and certificates. Similarly, Test MSCA systems shall be used at the MSCA level to manage test keys and certificates.

ERCA level

For the Test ERCA system, the following applies:

1. The system shall be capable of generating ECC key pairs using either the three Brainpool standardised domain parameters or the three NIST standardised domain parameters specified in Appendix 11, so as to test the three possible key lengths in the Smart Tachograph system. One set of domain parameters will be chosen, either the Brainpool or the NIST one, and it will be used for all interoperability test material.
2. The system shall be capable of creating self-signed ERCA root certificates as specified in Appendix 11.
3. The system shall be capable of processing Certificate Signing Requests (CSRs) and Key Distribution Requests (KDR)s from Test MSCAs. The format of these CSRs and KDRs shall be as specified in the Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy, [4].
4. Before signing a certificate, the system shall carry out the checks listed in [4], i.e. the same checks as done in production.
5. For each key certification operation, the system shall record the information listed in [4], i.e. the same information as recorded in production.
6. Before distributing a symmetric key, the system shall carry out the checks listed in [4], i.e. the same checks as done in production.
7. For each key distribution operation, the system shall record the information listed in [4], i.e. the same information as recorded in production.
8. The resulting signed certificates and Key Distribution Messages (KDMs) shall comply with the format specified in [4].
9. MSCAs may send CSRs and KDRs by e-mail to jrc-iot@ec.europa.eu. Resulting signed certificates and KDMs will be returned to the originating e-mail address.

MSCA level

Regarding the Test system of MSCAs, the following applies for the interaction with the Test ERCA:

1. The MSCA Test system shall be capable of generating ECC key pairs using either the three Brainpool standardised domain parameters or the three NIST standardised domain parameters specified in Appendix 11, at the choice of the MSCA.
2. The MSCA Test system shall be capable of generating CSRs in accordance with [4], using the value '54 4B' ("TK") in the additionalInfo element of the CHR field[6].
3. The CSRs must contain the identifier of the European root private key to be used for signing the respective certificate.
4. The MSCA Test system shall be capable of generating KDRs in accordance with [4], using the value '54 4B' ("TK") in the additionalInfo element of the Key Identifier field.
5. The KDRs must indicate the type and version of the requested test key.

The following applies for the interaction of an MSCA Test system with the component personalisers:

6. The MSCA Test system shall be capable of processing Certificate Signing Requests (CSRs) and Key Distribution Requests (KDR)s from component personalisers. The format of these CSRs and KDRs shall be specified by the MSCA in its Certificate Policy and Symmetric Key Infrastructure Policy.
7. Before signing a certificate, the MSCA Test system shall carry out same checks as done in production.
8. For each key certification operation, the MSCA Test system shall record the same information as recorded in production.
9. Before distributing a symmetric key, the MSCA Test system shall carry out the same checks as done in production.
10. For each key distribution operation, the MSCA Test system shall record the same information as recorded in production.
11. The resulting signed certificates and Key Distribution Messages (KDMs) shall comply with the format specified by the MSCA in its Certificate Policy and Symmetric Key Infrastructure Policy.
12. The manner in which test CSRs and test KDRs will be communicated to the MSCA, and the resulting signed test certificates and KDMs will be communicated to the component personaliser, shall be determined by the MSCA.
13. The MSCA shall make the test ERCA root certificates and its own MSCA certificates available to the component personalisers.

[6] In particular, the MSCA Test system must set the Certificate Effective Date and the Certificate Expiry Date in a CSR in the normal way, using the correct validity period for an MSCA_Card or MSCA_VU-EGF certificate. The DTLab needs this information to keep track of the type of MSCA certificate requested. However, in the returned MSCA certificate, the DTLab will set the Certificate Effective Date to 01-01-2004 and the Certificate Expiry Date to 01-01-2100, regardless of the values used in the CSR.

Component personaliser level

The following applies for the systems of component personalisers:

1. The personaliser's Test system shall be capable of generating ECC key pairs using either the three Brainpool standardised domain parameters or the three NIST standardised domain parameters specified in Appendix 11, at the choice of the personaliser.
2. The personaliser's Test system shall be capable of generating CSRs and processing the resulting signed certificates in accordance with the Certificate Policy and Symmetric Key Infrastructure Policy of the respective MSCA.
3. The personaliser's Test system shall be capable of generating KDRs and processing the resulting KDMs in accordance with the Certificate Policy and Symmetric Key Infrastructure Policy of the respective MSCA.

The component personaliser shall install the test keys and certificates received from the respective MSCA, along with the relevant ERCA and MSCA certificates, in the equipment provided to the Digital Tachograph Laboratory, in accordance with the requirements in section 6.3, 6.4, 6.5 or 6.6, as applicable.

10.2.1.2 Test Keys at the ERCA level

For the Interoperability Test ERCA:

- Three European root keys and certificates shall be present (EUR_01, EUR_02, EUR_03), one for each possible key length listed in Table 21: Cipher suites defined for the Smart Tachograph system
- The ERCA shall choose to use either the Brainpool or the NIST curves. The selected curves will be used for all interoperability test material. The three Interoperability Test ERCA root certificates are published on the Digital Tachograph Laboratory website.
- Three DSRC master keys shall be present. The length of these keys shall correspond to the three European root keys, in accordance with Appendix 11. The keys shall be indicated by version numbers '01', '02' and '03', respectively.
- Three sets of motion sensor-related master keys (K_M, $K_{M\text{-}WC}$, $K_{M\text{-}VU}$) shall be present. The length of these keys shall correspond to the three European root keys, in accordance with Appendix 11. The keys shall be indicated by version numbers '01', '02' and '03', respectively.
- The Test ERCA has to self-generate such material according to Section 10.2.1.1.

10.2.1.3 Test Keys at the MSCA level

For the Test MSCA_VU-EGF:

- Three test MSCA_VU-EGF certificates shall be present (MSCA_VU-EGF_01, MSCA_VU-EGF_02, MSCA_VU-EGF_03), one for each possible key length listed in Table 21: Cipher suites defined for the Smart Tachograph system
- Each MSCA shall choose to use either the Brainpool or the NIST curves.
- All three versions of the DSRC master key shall be present.
- All three versions of K_M shall be present.
- All three versions of $K_{M\text{-}VU}$ shall be present.

- In order to generate such material the Test MSCA has to interact with the Test ERCA according to Section 10.2.1.1.

For the Test MSCA_Card:

- Three test MSCA_Card certificates shall be present (MSCA_ Card_01, MSCA_ Card_02, MSCA_ Card_03), one for each possible key length listed in Table 21: Cipher suites defined for the Smart Tachograph system
- Each MSCA shall choose to use either the Brainpool or the NIST curves.
- All three versions of the DSRC master key shall be present.
- All three versions of $K_{M\text{-}WC}$ shall be present.
- In order to generate such material the Test MSCA has to interact with the Test ERCA according to Section 10.2.1.1.

10.2.1.4 Test Keys at the Equipment level

- Each Vehicle Unit supplied to the Digital Tachograph Laboratory by a component personaliser shall contain the keys and certificates specified in section 6.3. The key length used for a VU_MA or a VU_Sign certificate shall correspond to the key length of the MSCA_VU-EGF certificate used to sign that certificate.
- Each motion sensor supplied to the Digital Tachograph Laboratory by a component personaliser shall contain the keys and certificates specified in section 6.4.
- Each EGF supplied to the Digital Tachograph Laboratory by a component personaliser shall contain the keys and certificates specified in section 6.5. The key length used for a EGF_MA certificate shall correspond to the key length of the MSCA_VU-EGF certificate used to sign that certificate.
- Each tachograph card supplied to the Digital Tachograph Laboratory component personaliser shall contain the keys and certificates specified in section 6.6. The key length used for a Card_MA or a Card_Sign certificate shall correspond to the key length of the MSCA_Card certificate used to sign that certificate.
- In order to obtain such material, by default a component personaliser shall interact with the respective Test MSCA according to Section 10.2.1.1. Only if this Test MSCA is not yet available, the component personaliser may interact directly with the Digital Tachograph Laboratory as described in Section 10.2.1.5.
- The Test MSCA signing a particular Test equipment certificate, or providing symmetric keys and encrypted data for motion sensors, shall be the same MSCA that would sign that equipment certificate and would provide symmetric keys and related material in production.

10.2.1.5 Special Provisions for the Initial Distribution of Test Keys

Section 10.2.1.1 above stated that keys and certificates for interoperability testing will by default be generated and distributed in the same way as the keys and certificates for production. MSCAs and component personalisers are encouraged to start developing Interoperability Test systems for the generation and exchange of interoperability test cryptographic material as soon as possible. Because these test systems will be (almost) identical to the Production system, using these systems for generating and distributing interoperability test certificates and test keys also offers a way to do early testing of the Production systems.

A possible drawback of this principle is that it makes the Interoperability Test dependent on the timely presence of the Interoperability Test systems of the MSCAs and component personalisers. In particular, a component personaliser may not be able to begin the interoperability test because its MSCA is not offering interoperability test services yet. To prevent this problem, the Digital Tachograph Laboratory offers the possibility to generate and distribute Interoperability Test keys and certificates directly to component personalisers. To make use of this possibility, a component personaliser must send a request to the Digital Tachograph Laboratory, stating

- the reason for which the default method of test key generation and distribution cannot be used in this case,
- for each tachograph card, VU, motion sensor or EGF to be personalised separately, the necessary data, as specified in Appendix A.1.

Note that the Digital Tachograph Laboratory will offer this possibility only temporarily. Once an MSCA has successfully implemented its second-generation Production system, it also has to have a working Interoperability Test system and has to offer its component personalisers the possibility to obtain Test keys and certificates through that system. The Digital Tachograph Laboratory will not sign test certificates or distribute test symmetric keys to component personalisers whose MSCA is already capable of providing these services.

10.2.2 Identification of Public Keys

Smart tachograph Generation-2 certificate contents are defined in Annex IC Appendix 11 CSM_136 and summarised in Table 24: Smart Tachograph certificate format:

Field	Tag	Length (bytes)	ASN.1 data type (see Appendix 1 of Regulation (EU) 2016/799 [2])
ECC Certificate	'7F 21'	var	
ECC Certificate Body	'7F 4E'	var	
Certificate Profile Identifier	'5F 29'	'01'	`INTEGER(0..255)`
Certificate Authority Reference	'42'	'08'	`KeyIdentifier`
Certificate Holder Authorisation	'5F 4C'	'07'	`CertificateHolder Authorisation`
Public Key	'7F 49'	var	
Domain Parameters	'06'	var	`OBJECT IDENTIFIER`
Public Point	'86'	var	`OCTET STRING`
Certificate Holder Reference	'5F 20'	'08'	`KeyIdentifier`
Certificate Effective Date	'5F 25'	'04'	`TimeReal`
Certificate Expiration Date	'5F 24'	'04'	`TimeReal`
ECC Certificate Signature	'5F 37'	var	`OCTET STRING`

Table 24: Smart Tachograph certificate format

The format of a `KeyIdentifier` (CHR) appropriate for Member State certificates permits the identification of the Member State (data type `NationNumeric` and `NationAlpha`, see definitions in Annex IC Appendix 1).

The format of the CHR appropriate for equipment certificates identifies the equipment manufacturer (data type `ManufacturerCode`, see definition in Annex IC Appendix 1). The assignment of manufacturer codes is the responsibility of the Digital Tachograph Laboratory.

The Certificate Holder Authorisation permits the identification of the equipment type. For VUs, driver cards and workshop cards it also permits to distinguish between certificates for mutual authentication and for signing.

The possible values for the Domain Parameters field have been specified in section 10.2.1.

10.2.3 Validity Period Assignment

All Test certificates (at the level of the ERCA, the MSCAs and the equipment) will have a validity period starting at 01-01-2004 and ending at 01-01-2100. The effective date is chosen to allow interoperability testing against Gen-1 equipment already existing in the DT Laboratory, whose EOV may be dated in the past. The expiry date is chosen such that problems related to expired certificates will be avoided in the future. Finally, the effective date of all certificates must be the same to avoid problems with the test cards' internal time, which may be set forward inadvertently if this is not the case.

11 Legislation

The text of the COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 (Annex IC) chapter 8 – *Type Approval of Recording Equipment and Tachograph Cards* is reproduced here for reference purposes.

8.1 General points
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.

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.

(425) Recording equipment shall be submitted for approval complete with any integrated additional devices.

(426) Type approval of recording equipment and of tachograph cards shall include security related tests, functional tests and interoperability tests. Positive results to each of these tests are stated by an appropriate certificate.

(427) Member States type approval authorities will not grant a type approval certificate as long as they do not hold:
— a security certificate,
— a functional certificate,
— and an interoperability certificate
for the recording equipment or the tachograph card, subject of the request for type approval.

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

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

(430) Type approval of software modifications aimed to upgrade a previously type approved recording equipment may not be refused if such modifications only apply to functions not specified in this Annex. Software upgrade of a recording equipment may exclude the introduction of new character sets, if not technically feasible.

8.2 Security certificate

(431) The security certificate is delivered in accordance with the provisions of Appendix 10 of this Annex. Recording equipment components to be certified are vehicle unit, motion sensor, external GNSS facility and tachograph cards.

(432) In the exceptional circumstance that the security certification authorities refuse to certify new equipment on the ground of obsolescence of the security mechanisms, type approval shall continue to be granted only in these specific and exceptional circumstances, and when no alternative solution, compliant with the Regulation, exists.

(433) In this circumstance the Member State concerned shall, without delay, inform the European Commission, which shall, within twelve calendar months of the grant of the type approval, launch a procedure to ensure that the level of security is restored to its original levels.

8.3 Functional certificate

(434) Each candidate for type approval shall provide the Member State's type approval authority with all the material and documentation that the authority deems necessary.

(435) Manufacturers shall provide the relevant samples of type approval candidate products and associated documentation required by laboratories appointed to perform functional tests, and within one month of the request being made. Any costs resulting from this request shall be borne by the requesting entity. Laboratories shall treat all commercially sensitive information in confidence.

(436) A functional certificate shall be delivered to the manufacturer only after all functional tests specified in Appendix 9, at least, have been successfully passed.

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

(438) The functional certificate of any recording equipment component shall also indicate the type approval numbers of the other type approved compatible recording equipment components tested for its certification.

(439) The functional certificate of any recording equipment component shall also indicate the ISO or CEN standard against which the functional interface has been certified.

8.4 Interoperability certificate

(440) Interoperability tests are carried out by a single laboratory under the authority and responsibility of the European Commission.

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

(442) Requests will be officially registered only when the laboratory is in possession of:

— the entire set of material and documents necessary for such interoperability tests,

— the corresponding security certificate,

— the corresponding functional certificate.

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

(443) No interoperability tests shall be carried out by the laboratory, for recording equipment or tachograph cards that have not been granted a security certificate and a functional certificate, except in the exceptional circumstances described in Requirement 432.

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

(445) The interoperability tests shall be carried out, in accordance with the provisions of Appendix 9 of this Annex, with respectively all the types of recording equipment or tachograph cards:

— for which type approval is still valid or,

— for which type approval is pending and that have a valid interoperability certificate.

(446) The interoperability tests shall cover all generations of recording equipment or tachograph cards still in use.

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

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

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

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

8.5 Type-approval certificate

(451) The type approval authority of the Member State may deliver the type approval certificate as soon as it holds the three required certificates.

(452) The type approval certificate of any recording equipment component shall also indicate the type approval numbers of the other type approved interoperable recording equipment.

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

(454) The laboratory competent for interoperability tests shall run a public web site on which will be updated the list of recording equipment or tachograph cards models:

— for which a request for interoperability tests have been registered,

— having received an interoperability certificate (even provisional),

— having received a type approval certificate.

8.6 Exceptional procedure: first interoperability certificates for 2nd generation recording equipment and tachograph cards

(455) Until four months after a first couple of 2nd generation recording equipment and 2nd generation tachograph cards (driver, workshop, control and company cards) have been certified to be interoperable, any interoperability certificate delivered (including the first ones), regarding requests registered during this period, shall be considered provisional.

(456) If at the end of this period, all products concerned are mutually interoperable, all corresponding interoperability certificates shall become definitive.

(457) If during this period, interoperability faults are found, the laboratory in charge of interoperability tests shall identify the causes of the problems with the help of all manufacturers involved and shall invite them to realise the necessary modifications.

(458)If at the end of this period, interoperability problems still remain, the laboratory in charge of interoperability tests, with the collaboration of the manufacturers concerned and with the type approval authorities who delivered the corresponding functional certificates shall find out the causes of the interoperability faults and establish which modifications should be made by each of the manufacturers concerned. The search for technical solutions shall last for a maximum of two months, after which, if no common solution is found, the Commission, after having consulted the laboratory in charge of interoperability tests, shall decide which equipment(s) and cards get a definitive interoperability certificate and state the reasons why.

(459) Any request for interoperability tests, registered by the laboratory between the end of the four month period after the first provisional interoperability certificate has been delivered and the date of the decision by the Commission referred to in requirement 455, shall be postponed until the initial interoperability problems have been solved. Those requests are then processed in the chronological order of their registration.

References

Ref.	Title
[1]	Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014; Official Journal of the European Union L60
[2]	Commission Implementing Regulation (EU) 2016/799 of 18 March 2016; Official Journal of the European Union L 139
[3]	Commission Implementing Regulation (EU) 2018/502 of 28 February 2018; Official Journal of the European Union L 85
[4]	Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy, JRC technical report JRC110814, June 2018

List of abbreviations and definitions

AA	Administrative Arrangement
AETR	Accord Européen sur les Transports Routiers (European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport)
DTC	Smart tachograph Cards (procedures)
DTGNSS	Smart tachograph External GNSS (procedures)
DTLab	Digital Tachograph Laboratory
DTMS	Smart tachograph Motion Sensors (procedures)
DTVU	Smart tachograph Vehicle Units (procedures)
EU	European Union
VU	Vehicle Unit

List of tables

A.1 Format of requests for interoperability test keys and certificates for the second-generation Digital Tachograph from the DTLab

A.1.1 General

Section 10.2.1.5 specifies that under certain circumstances, component personalisers may obtain second-generation Digital Tachograph cryptographic material for the interoperability test directly from the Digital Tachograph Laboratory, rather than via their MSCA. This Appendix specifies the format of requests and responses to be used in this case.

A.1.2 Certificate Signing Requests

The Digital Tachograph Laboratory (DTLab) supports two methods to request an equipment certificate:

- The DTLab receives a request for generating test equipment certificates from a component personaliser by e-mail. If not existing yet, the DTLab first generates a suitable test MSCA key pair and signs the associated MSCA certificate with the proper Interoperability Test ERCA key. The DTLab then generates a test key pair for the equipment, creates the associated certificate and signs it using the private test key of the MSCA. The DTLab then returns the test equipment key pair and the equipment certificate to the requester. The DTLab also returns the MSCA certificate that can be used to verify the equipment certificate, while the Interoperability Test ERCA certificate can be found on the DTLab website.
- The second possibility is that the component personaliser sends the DTLab a Certificate Signing Request (CSR) by e-mail. The format of this request is almost identical to that of the requested certificate, but it is self-signed. See below for details. The DTLab inspects the CSR contents to determine the MSCA private key to be used for signing the certificate. If this MSCA key is not existing yet, the DTLab first generates a suitable test MSCA key pair and creates and signs the associated MSCA certificate with the proper Interoperability Test ERCA key whose certificate is published on the DTLab website. It then changes the test equipment certificate contents as appropriate and signs it using the MSCA private key. The DTLab then returns the test certificate to the requester.

Method 1

Using method 1, the component personaliser should send a request to jrc-iot@ec.europa.eu, specifying the following:

- The (nationality of the) Test MSCA to be used for signing the equipment certificate(s) and/or the CHR of the intended test MSCA certificate if it is known.
- The type of equipment (VU, driver card, workshop card, company card, control card, or EGF).
- For VUs, driver cards and workshop cards: whether a MA certificate or a Sign certificate is requested.
- For a VU: whether a VU serial number or a certificate request identifier must be used in the certificate (see Appendix 11 of Annex 1C [2]).
- The 4-byte serial number of the equipment[7], in hexadecimal format.
- The 1-byte manufacturer code.
- The domain parameters of the elliptic curve to be used to generate the equipment key pair.

[7] Or the 4-byte request serial number, in case a certificate request identifier must be used (VU only).

In case the DTLab notes an error or omission in the data provided by the personaliser, it will notify the personaliser by e-mail.

Otherwise, if the data is complete and correct, the Digital Tachograph Laboratory will generate an equipment key pair using the indicated curve. The public and private key will be put in a file complying with the PKCS#8 format specified in Appendix A.2. The DTLab will create a certificate for the public key and sign it using the correct private key of the indicated MSCA. If the test MSCA certificate does not exist yet, it will be generated. The certificate format complies with Appendix 11 to Annex IC, except that the Certificate Effective Date will be set to 1-1-2004 and the Certificate Expiry Date to 1-1-2100.

The DTLab will return to the component personaliser

- three copies of the PKCS#8 file: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .pkcs8 (hexadecimal) format.
- three copies of the equipment certificate: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .bin (hexadecimal) format.
- three copies of the MSCA certificate that can be used to verify the equipment certificate, in the same formats.
- three copies of the ERCA root certificate that can be used to verify the MSCA certificate, in the same formats.

Note: it is possible to request multiple equipment certificates in a single e-mail (e.g., three Interoperability Test VU certificates, having three different key lengths according to Section 6.3). However, the necessary data listed above shall be clearly specified for each requested certificate separately.

Method 2

Using method 2, the component personaliser should send an equipment Certificate Signing Request (CSR) to jrc-iot@ec.europa.eu. The format of the equipment CSR shall be identical to the certificate format specified in Appendix 11 to Annex IC, with the following exceptions:

- if the component personaliser knows the CHR of test MSCA certificate that should sign the equipment certificate, they shall set the CAR field of the CSR to the value of this CHR. If the CHR of the intended est MSCA certificate is not known, the nationNumeric and nationAlpha elements in the CAR shall indicate the nationality of the test MSCA that should sign the certificate and the additionalInfo element shall have the value "TK". The DTLab will ignore the value of other data elements in the CAR. If a test MSCA certificate for the intended nation is already present, the DTLab will use it to sign the equipment certificate. Otherwise, a test MSCA certificate will be generated on purpose.
- the component personaliser shall set the Certificate Effective Date to 1-1-2004 and the Certificate Expiry Date to 1-1-2100.
- the signature shall be generated using the equipment private key that corresponds to the public key in the equipment CSR itself.

The DTLab will verify that signature is correct, whether the additionalInfo field is equal to "TK", and whether all other elements of the CSR have correct and consistent values.

In case the DTLab notes an error or omission in the equipment CSR provided by the personaliser, it will notify the personaliser by e-mail.

Otherwise, if all is correct, the DTLab will note the nationality, key length and type (MSCA_VU or MSCA_Card) of the MSCA private key to be used for signing the equipment certificate. It will replace the CAR in the CSR with the CHR of this MSCA private key. Then, it will replace the signature with a signature over the new certificate contents, calculated using the MSCA private key.

The DTLab will return to the component personaliser:

- three copies of the equipment certificate: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .bin (hexadecimal) format.
- three copies of the MSCA certificate that can be used to verify the equipment certificate, in the same formats.
- three copies of the ERCA root certificate that can be used to verify the MSCA certificate, in the same formats.

Notes:

- For both Method 1 and Method 2, the component personaliser and the DTLab will keep the MSCA of the component personaliser in copy of all communications. In particular, the MSCA shall inform the DTLab of the type of ECC curve (Brainpool or NIST) to be used for generating the test MSCA keys and certificates.
- In principle the DTLab will generate maximum one MSCA_Card and one MSCA_VU Test certificate for every MSCA, for each possible key length. This means that after their initial request to the DTLab, component personalisers using Method 2 should use the CHR of the existing MSCA certificate as the CAR in any subsequent certificate signing request. In case a component personaliser uses Method 1, the DTLab should use the existing MSCA certificate as the CAR in any subsequent equipment certificate generated.
- Even if test MSCA certificates have been generated by the Interoperability Test ERCA system in response to equipment manufacturer requests, once the Interoperability Test MSCA system of a nation has been implemented, the respective MSCA can ask for the generation of new test MSCA certificates according to the provisions of Section 10.2.

A.1.3 Key Distribution Requests

A.1.3.1 Master Keys

For requesting a test K_{M_WC}, the workshop card part of the Motion Sensor Master Key, a card issuer shall send an e-mail to jrc-iot@ec.europa.eu, specifying the length of the requested key.

Likewise, for requesting a test K_{M_VU}, the VU part of the Motion Sensor Master Key, a VU manufacturer shall send an e-mail to jrc-iot@ec.europa.eu, specifying the length of the requested key.

The DTLab will return the requested key in plain text. For each key, three copies will be returned: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .bin (hexadecimal) format.

Note: it is possible to request multiple keys (having different lengths) in a single e-mail.

A.1.3.2 VU-specific DSRC keys

For requesting a set of test VU-specific DSRC keys for a VU (as specified in Appendix 11), a VU manufacturer shall send an e-mail to jrc-iot@ec.europa.eu, specifying

- the 8-byte hexadecimal value of the extended serial number or certificate request identifier of the VU in question.
- the length of the test DSRC Master Key to be used to derive the VU-specific keys.

The DTLab will verify that the extended serial number is correctly formatted.

If all is correct, the DTLab will derive the ENC key and the MAC key for this VU using the Test DSRC Master Key of the specified length. It will return these keys in plain text. For each key, three copies will be returned: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .bin (hexadecimal) format.

Note: it is possible to request multiple keys (for different VUs) in a single e-mail. However, the required length and the VU extended serial number should be clearly specified for every VU separately.

A.1.3.3 Encrypted Motion Sensor Pairing Key and Serial Number

For requesting a test encrypted Motion Sensor Pairing Key and a test encrypted serial number for a motion sensor, as specified in Appendix 11, a motion sensor manufacturer shall send an e-mail to jrc-iot@ec.europa.eu, specifying

- the length of the test Motion Sensor Master Key (and therefore also the length of the corresponding Identification Key) to be used for encryption.
- the hexadecimal value of the extended serial number of the motion sensor in question.
- the hexadecimal value of the Pairing Key of the motion sensor in question.

The DTLab will verify that the extended serial number is correctly formatted. Moreover, the DTLab will verify that the length of the Pairing Key is consistent with the specified length of the Motion Sensor Master Key.

If all is correct, the DTLab will encrypt the Pairing Key with the Test Motion Sensor Master Key of the correct length. Next, it will encrypt the motion sensor serial number with the motion sensor test Identification Key (K_{ID}). Test K_{ID} is calculated as Test K_M XOR CV, where CV is the constant vector specified in Appendix 11 to Annex IC.

The DTLab will return three copies of both encryptions: one in .txt (UTF-8) format, one in .pem (Base64) format and one in .bin (hexadecimal) format.

Note: it is possible to request multiple encryptions (for different motion sensors) in a single e-mail. However, the necessary data listed above should be clearly specified for each motion sensor separately.

A.2 Format of PKCS#8 files

Format of .pkcs8 files containing an equipment private and public key for interoperability testing, as returned by the DLT to the component personaliser in case method 1 described in Appendix A1.2 is used. Format is compliant with RFC 5958. All values hexadecimal.

30	**L**	SEQUENCE SIZE (1) OF OneAsymmetricKey; see RFC 5958. Both of the optional elements attributes and publicKey in this data type are omitted									
		02	**01**	**00**	Version; the value is set to '00' to indicate that the format of OneAssymmetricKey is equal to that of PrivateKeyInfo as specified in RFC 5280						
		30	**L**	PrivateKeyAlgorithmIdentifier							
				06	**07**	**2A 86 48 CE 3D 02 01**	PUBLIC-KEY: Algorithm identifier for elliptic curve is given in RFC 5912				
				06	**L**	**V**	PrivateKeyAlgorithms: see data type ECParameters in RFC 5912. The CHOICE made here is to use a namedCurve; the value is the DER-encoded OID of the relevant curve.				
		04	**L**	OCTET STRING containing private key; see RFC 5958							
				30	**L**	ECPrivateKey; see RFC 5915. Both of the optional elements parameters and publicKey in this data type are present.					
						02	**01**	**01**	version; the value represents ecPrivkeyVer1.		
						04	**L**	**V**	OCTET STRING containing the value of the private key		
						A0	**L**		parameters		
								06	**L**	**V**	ECParameters; the CHOICE made here is to use a namedCurve; the value is the DER-encoded OID of the relevant curve.
						A1	**L**	publicKey			
								03	**L**	**V**	BITSTRING containing the value of the public key. Note that the first byte '00' indicates zero empty bits, as per the definition of the ASN.1 BITSTRING data type. The second byte '04' indicates the uncompressed encoding, as per TR 03111.

JRC112773