European Commission

JRC TECHNICAL REPORTS

Smart Tachograph

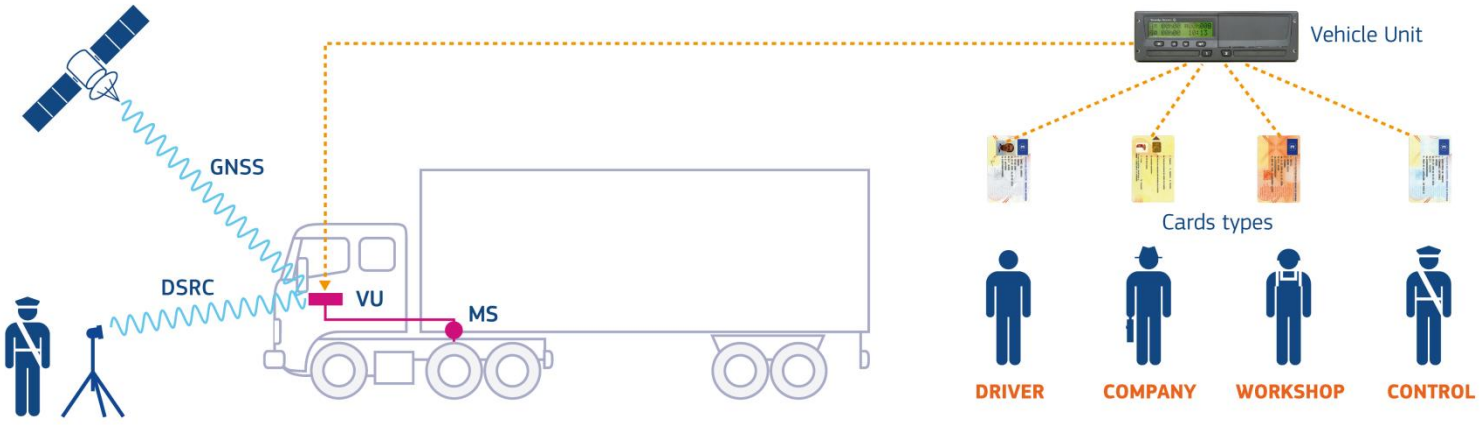
Cryptographic keys and digital certificates sample set

David Bakker (UL)

Luigi Sportiello (JRC)

Version 1.2

April 2017



Joint Research Centre

EUR 28475 EN

Contact information
Email: erca@jrc.ec.europa.eu

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

JRC105740

EUR 28475 EN

PDF ISBN 978-92-79-65787-0 ISSN 1831-9424 doi:10.2760/716503

Luxembourg (Luxembourg): Publications Office of the European Union, 2017.

How to cite this report: Bakker D., Sportiello L., Smart Tachograph: Cryptographic keys and digital certificates sample set, EUR 28475 EN, doi:10.2760/716503.

Contents

Abstract

In order to aid manufacturers, component personalisers, certification authorities and other Digital Tachograph stakeholders with the development and testing of equipment and systems complying with the Generation-2 Smart Tachograph specifications, a comprehensive set of Generation-2 sample cryptographic keys and digital certificates has been developed.

This document serves to detail the contents of this sample set and the values chosen for individual fields in the certificates. It also explains which kind of tests can be done using the cryptographic material in the set, as well as identifying some tests that cannot be done with this set.

1 Introduction

The digital tachograph system (Generation-1 Digital Tachograph) has been introduced by Council Regulation 3821/85 as amended by Council Regulation 2135/98 [1] and Commission Regulation 1360/2002 [2]. Regulation (EU) No 165/2014 [3] and its Commission Implementing Regulation (EU) 2016/799 [4] call for the introduction of a Generation-2 Smart Tachograph.

Annex 1C (Requirements for construction, testing, installation, and inspection) to [4] includes the technical specifications of the Smart Tachograph system. Detailed technical information is contained in a series of sixteen appendices to Annex 1C. Appendix 11 (Common Security Mechanisms) describes all details of the cryptographic security mechanism used to protect the data stored and transmitted in the Smart Tachograph system.

1.1 Scope of this document

Security mechanisms have been defined to secure the exchange and storage of data by the Smart Tachograph equipment, namely Vehicle Units, Tachograph Cards, Motion Sensors and External GNSS Facilities. Such mechanisms are mainly based on cryptographic solutions. Specifically, a cryptographic infrastructure has been defined, with symmetric keys, asymmetric keys and digital certificates stored in the Smart Tachograph equipment, allowing the execution of cryptographic algorithms and protocols. Section 2.1 below gives an overview of the cryptographic infrastructure of the Smart Tachograph. In order to support Member State Certification Authorities (MSCAs), manufacturers, component personalisers and other stakeholders with the development and testing of equipment and systems complying with these new specifications, a comprehensive set of Generation-2 sample keys and certificates has been developed.

This document serves to detail the contents of this sample set and the values chosen for individual fields in the certificates. It also explains which kind of tests can be done using the cryptographic material in the set, as well as identifying some tests that cannot be done with this set.

Please note that most of the Generation-2 equipment must also contain Generation-1 cryptographic keys and digital certificates, in order to be able to communicate to Generation-1 equipment. However, for these keys and certificates stakeholders may adapt cryptographic test material developed or made available in the past. The sample set described in this document contains only Generation-2 keys and certificates.

1.2 Intended audience

This document accompanies the sample set of Generation-2 keys and certificates. It is intended for stakeholders involved in the development of devices and systems for the Smart Tachograph system. Readers of this document should be familiar with the contents of Annex 1C, and especially with Appendix 11 to that Annex.

1.3 Disclaimer

This sample set has to be only seen as a support to the development and testing processes of digital tachograph stakeholders. In the event of any conflict between the contents of the sample set and the Implementing Regulation 2016/799 [4] and its Annexes and Appendices, the latter shall prevail. Each stakeholder remains fully responsible for making sure that their equipment complies with all requirements in [4].

2 Smart Tachograph security mechanisms

Figure 1 shows an overview of the Smart Tachograph system.

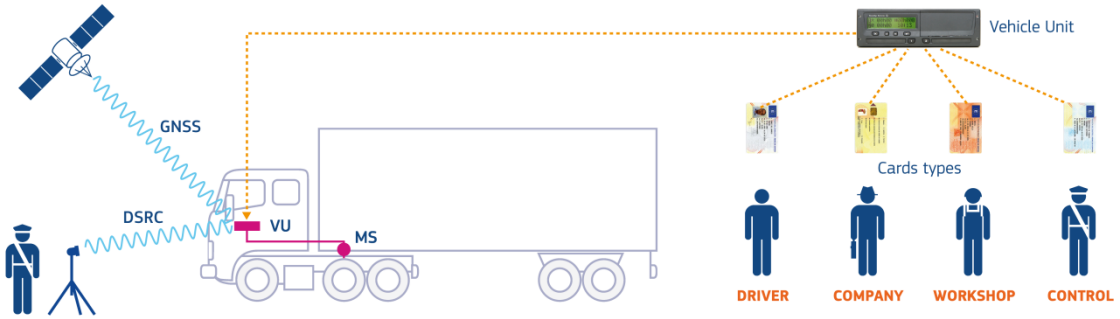


Figure 1 Overview of the Smart Tachograph system

The vehicle unit (VU) is the central component of the system. Every vehicle is equipped with a vehicle unit whose main task is to log driving activities.

In order to do so, each vehicle unit is securely paired to a motion sensor (MS), which is connected to the gearbox of the vehicle and provides the vehicle unit with a signal that represents the vehicle's speed. During pairing, which is done once by a workshop, the VU and the motion sensor mutually authenticate each other. After this, part of the communication between a VU and a motion sensor is authenticated and encrypted.

Users of a vehicle unit are equipped with a tachograph card (TC). There are four types of cards, corresponding to the four roles of Driver, Control Officer, Workshop or Company. Upon insertion of a card in a VU, the card and the VU mutually authenticate each other. Subsequently, communication between them is authenticated and in some cases encrypted. Moreover, once the VU is authenticated to the card, it is allowed to write data to some of the data structures on the card. In addition, the exact working mode of a VU is determined by the card(s) that is/are inserted into its card slots.

The vehicle unit is also able to periodically log the vehicle's position and check the plausibility of the motion sensor's signal by means of position determination based on a Global Navigation Satellite System (GNSS). The GNSS receiver that is necessary to do so is either contained in the VU itself, or in an External GNSS Facility (EGF). In case an EGF is used, the vehicle is securely coupled once to the VU by a workshop. During coupling, the VU and EGF authenticate each other. Afterwards, communication between them is authenticated.

The data stored on either a vehicle unit or a card must be downloaded by a control officer during a check or by the responsible company. Although the communication interfaces used for downloading data from a card or from a VU are rather different, the security requirements on both interfaces are equal: the integrity, authenticity and non-repudiation of the downloaded data must be protected by means of a digital signature created by the VU or the card.

Finally, the Smart Tachograph system also contains Remote Early Detection Communication Readers (REDCRs). These are readers that are operated by a control officer and are positioned along the roadside or on officers' vehicles. They are capable of

interrogating a Remote Communication Facility (RCF) in a passing vehicle over a DSRC link, without having to stop the vehicle. The VU periodically stores relevant data, in particular driving and control data, in the RCF. Such a system allows for a frequent verification of the vehicle status through remote interrogations. The data communicated over the DSRC link is encrypted and authenticated by the VU before it is sent to the RCF.

2.1 Smart Tachograph cryptographic infrastructure

In order to fulfil the security requirements for each of the interactions outlined above, the vehicle unit, tachograph cards, motion sensor and EGF all contain a number of cryptographic elements, namely public/private key pairs, digital certificates and/or symmetric keys. They comply with Appendix 11 of Annex 1C, which also gives a full specification of the protocols adopted to secure the interaction of the different system components.

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

A number of pre-defined key lengths and hash sizes have been specified and combined together to form cipher suites, which assure a consistent level of security for all interactions of the Smart Tachograph components. The cipher suites are summarized in Table 1. All system components mentioned above 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 1 Cipher suites defined for the Smart Tachograph system

For Elliptic Curve Cryptography there is the need to choose domain parameters. Appendix 11 of Annex 1C allows two sets of standardized 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 1 has been selected. The complete set is shown in Table 2.

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

Table 2 Allowed standardized domain parameters for ECC

A cryptographic infrastructure has been designed for the generation and deployment of the cryptographic elements in the Smart Tachograph system. It is made of three layers, a European level, a member state level and a system component level. Such an infrastructure acts both as Public Key Infrastructure (PKI) and as symmetric keys distribution infrastructure.

2.1.1 Asymmetric keys and Public Key Infrastructure

The ECC key pairs are part of a Public Key Infrastructure (PKI), as shown in Figure 2. This Public Key Infrastructure (PKI) consists of three levels. From top to bottom, these are:

- the European level, managed by the European Root Certificate Authority (ERCA).
- the Member State level, managed by the Member State Certificate Authority (MSCA) of every member state involved in the digital tachograph system.
- The equipment level, managed by the manufacturers or personalizers of vehicle units, tachograph cards and EGFs.

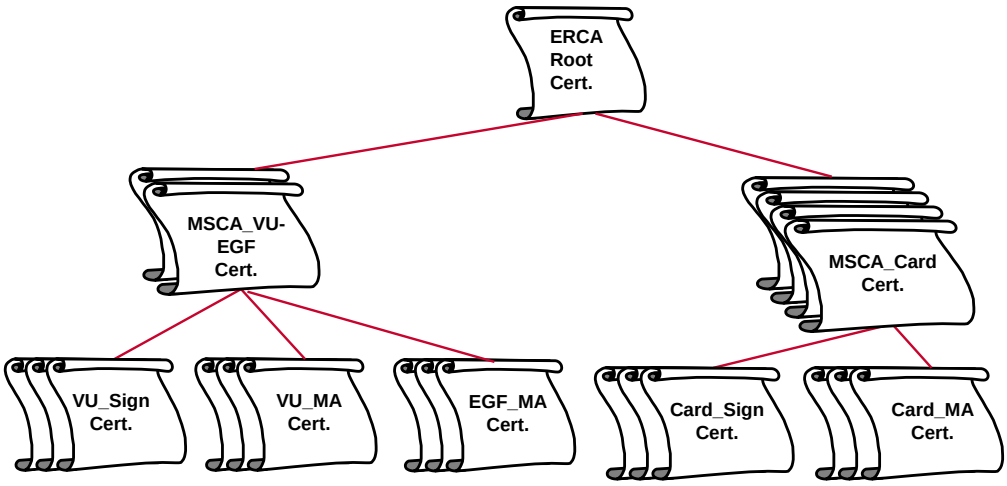


Figure 2 Smart Tachograph PKI

On the European level, the ERCA creates a single ECC key pair that serves as the root key pair of the entire PKI. The ERCA also creates a self-signed root certificate containing the root public key. ERCA certificates have a validity period of 34 years and 3 months. The ERCA root key pair and certificate are renewed over time (see next section). The ERCA uses the corresponding private key to sign MSCA certificates. The public MSCA keys to be signed are sent to the ERCA by the MSCAs.

On the Member State level, each MSCA that needs to issue certificates for VUs or EGFs creates a key pair, which is indicated in Appendix 11 as MSCA_VU-EGF. Then it requests the ERCA to sign a certificate for the respective public key. Similarly, each MSCA that needs to issue certificates for tachograph cards creates an MSCA_Card key pair and asks the ERCA to sign the corresponding certificate. MSCA_VU-EGF certificates are valid for 17 years and 3 months. MSCA_Card certificates have a validity period of 7 years and 1 month. The MSCA uses the corresponding private keys to sign equipment certificates.

On the equipment level, the manufacturer or personaliser of each VU, card or EGF[1] creates at least an equipment key pair for mutual authentication. The component will use this key pair to authenticate itself to other equipment it will interoperate with during its lifetime. In addition, for a VU, a workshop card or a driver card, the manufacturer or personaliser also creates a key pair for signing. These components will use their signing private key to sign data that is downloaded from them. Other component types are not required to support data downloads and hence do not need a signing key pair. All generated public keys are sent to the competent MSCA for the generation of the respective certificate. The validity period of equipment certificates is as follows:

- VU_Sign 15 years and 3 months
- VU_MA 15 years and 3 months
- Driver Card_Sign: 5 years and 1 month
- Workshop Card_Sign: 1 year and 1 month
- Driver Card_MA: 5 years
- Company Card_MA: 5 years
- Control Card_MA: 2 years
- Workshop Card_MA: 1 year
- EGF_MA 15 years

All certificates issued within the Smart Tachograph system are so-called card-verifiable certificates. Their format is equal for all types of certificates and is show in the table below:

Field	Tag	Length (bytes)	ASN.1 data type (see Appendix 1 of Regulation (EU) 2016/799 [4])
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 3 Smart Tachograph certificate format

[1] Note that motion sensors do not contain asymmetric keys or certificates.

2.1.2 Symmetric keys

Concerning symmetric keys in the Smart Tachograph system, there are two kinds of keys managed in the cryptographic infrastructure:

- Keys for protecting the communication between a VU and a Motion Sensor:
  - Motion Sensor Master Keys. These are constituted from a Workshop Card Master Key part and a VU Master Key part.
  - Identification Keys, which are derived from the Motion Sensor Master Keys and a constant vector.
- Keys for protecting the communication over a DSRC link between a VU and a Remote Early Detection Communication Reader:
  - DSRC Master Keys
  - VU-specific DSRC keys for encryption and authentication, derived from a DSRC Master Key

The motion sensor keys are used to secure the link between VU and Motion Sensor. The DSRC keys are used to secure the data uploaded on the Remote Communication Facility.

The Motion Sensor Master Key, along with its constituting parts, and the DSRC Master Key are generated by the ERCA. Every time the ERCA replaces the ERCA root key pair, it also replaces the Master Keys (see next section). The Master Keys are provided by the ERCA to the MSCAs. A MSCA can use the Motion Sensor Master Keys to generate specific cryptographic material to be installed in a Motion Sensor. A MSCA can also provide the Workshop Card Master Key part to be installed in Workshop cards, or can provide the VU Master Key part to be installed in VUs according to Appendix 11 of Annex 1C. A MSCA can use the DSRC Master Keys to generate the VU-specific DSRC keys for a VU. A MSCA can also provide the DSRC Master Keys to be installed in Control and Workshop card according to Appendix 11 of Annex 1C. Each generation of these Master Keys will be in use by Smart Tachograph component for 34 years.

2.2 ERCA keys replacement and link certificates

Appendix 11 of Annex 1C describes a mechanism that ERCA can use to replace the root key pair and respective certificate, along with the associated master keys. The appendix also specifies that such a replacement shall take place every 17 years.

An important advantage of this key replacement is that it gives ERCA a chance to review whether the security level of the root key pair and associated master keys is still sufficient. If this is not the case, ERCA can decide to switch to longer key lengths.

Whenever ERCA creates a new root key pair, the following actions take place:

- In order to ensure interaction between equipment issued under different generations of the root key, ERCA will issue a so-called link certificate. A link certificate contains the new ERCA public key and is signed with the previous ERCA private key. By verifying the link certificate, equipment issued under the previous ERCA key pair is able to trust the new ERCA public key and so it is allowed to interact with equipment issued under the new ERCA public key. See Appendix 11 of Annex 1C for more details.
- ERCA also generates a new Motion Sensor Master Key, and relative parts, and a new DSRC Master Key. For the concerned equipment all master keys, and related materials, that are valid at the time of its issuance have to be installed in its memory. This ensures the interaction between equipment linked to different master key generation. See Appendix 11 of Annex 1C for more details.

2.3 Goal of the sample set

All stakeholders should develop and implement the security mechanisms relevant to them and should be able to test their implementation. The sample set of keys and certificates was developed with this need in mind. In particular, the sample set allows:

- Testing the use of the AES, SHA-2 and ECC algorithms, using all specified key lengths and standardized domain parameters.
- Testing the use of all types of key pairs / certificates (i.e. on ERCA, MSCA and Equipment level) and all types of symmetric keys (i.e. DSRC and Motion Sensor keys) defined in Appendix 11 of Annex 1C.
- Testing of the correct implementation of the link certificate mechanism specified in Appendix 11.
- Testing of the mechanisms to manage the replacement of the DSRC Master Key and Motion Sensor Master Key with new ones.
- Testing of the correct handling of certificate validity periods.

More details are given in chapter 6.

3 Contents of the sample set

This chapter describes the contents of the sample set, i.e. the keys and certificates that are present. The chapter also discusses the reasoning behind the selection of these keys and certificates and the relation between them.

Section 3.1 describes the asymmetric key pairs and certificates present in the sample set in more detail. Section 3.2 describes the symmetric keys and related encrypted data.

3.1 Asymmetric key pairs and certificates

The overall logic behind the asymmetric cryptographic material in the sample set is the following:

1. Three generations of ERCA root certificates have been defined, with an increasing key size. Two link certificates linking these certificates have been provided.
2. Two countries have been defined, indicated as UTO (for Utopia) and ARC (for Arcadia). For both countries, there is an MSCA responsible for issuing card certificates (MSCA_Card) and an MSCA for issuing VU and EGF certificates (MSCA_VU-EGF).
3. On the equipment level, a VU is issued under every MSCA_VU-EGF certificate and a full set of tachograph cards is issued under every MSCA_Card certificate. Also, an EGF is issued under every MSCA_VU-EGF certificate. This implies that the sample set contains certificates for VUs, EGFs and sets of cards for both Utopia and Arcadia.

Figure 3 below shows the certificates that are present in the sample set. Notes to the figure:

- Different generations of the root certificate are indicated by a number in brackets. E.g. ERCA (1) is the first generation of ERCA root certificate; ERCA (2) is the second generation, etc.
- Other certificates are indicated by two numbers in brackets, the first one indicating the root certificate generation under which they are issued, the second one the sequence number of the certificate itself. E.g. MSCA_Card (1-1) is the first MSCA_Card certificate issued under ERCA (1); MSCA_Card (2-1) is the first MSCA_Card certificate issued under ERCA (2); Card_MA(2-1) is the first Card certificate for mutual authentication that is issued under ERCA (2), etc.

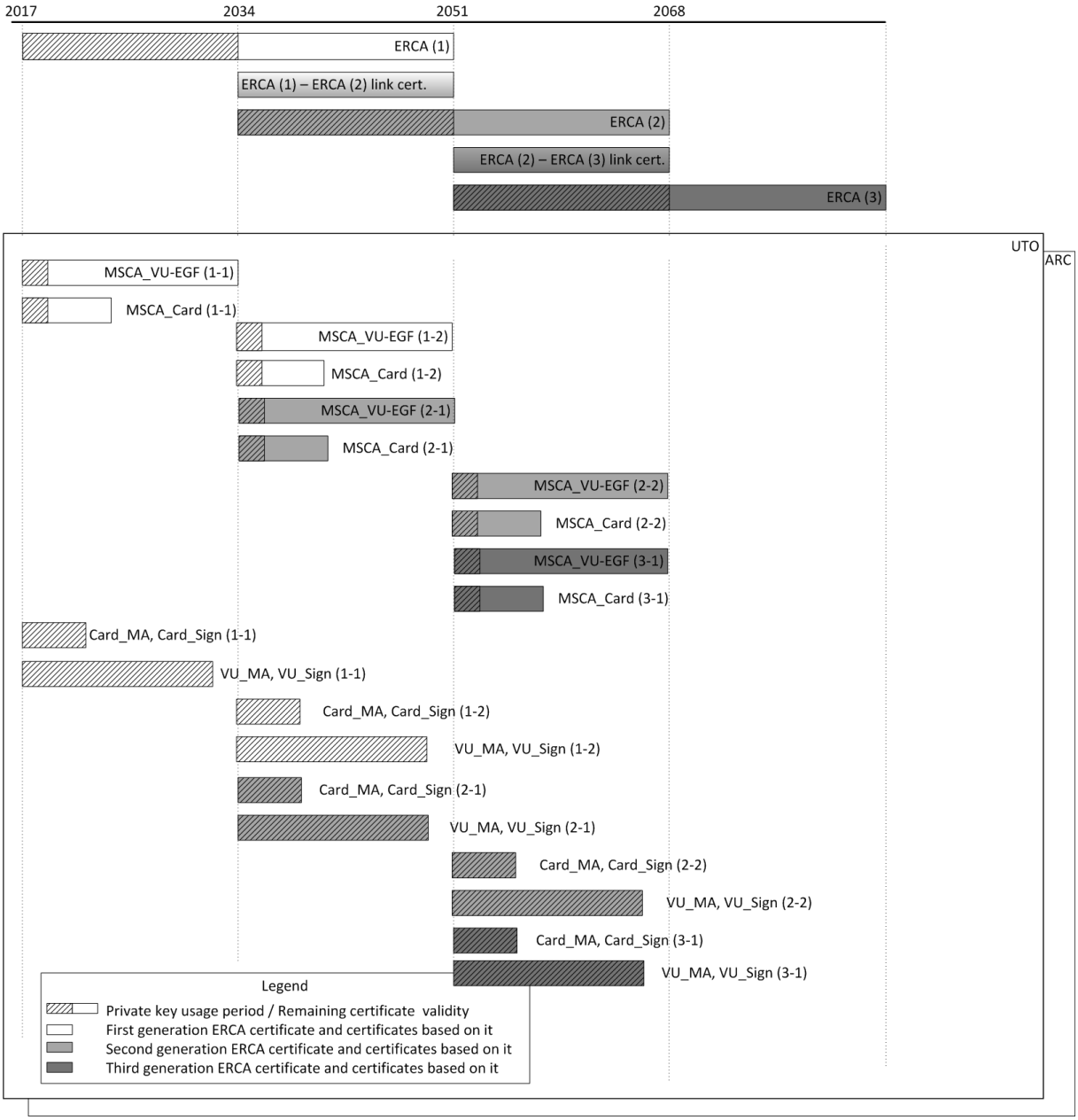


Figure 3 Asymmetric keys and certificates in the sample set

The following assumptions have also been made:

1. The set contains a number of European root key pairs and certificates, as described in section 9.1.2 of Appendix 11. It has been decided that at the ERCA level the root keys are based only on Brainpool curves. This means that three root certificates are present, differing in the ECC domain parameters used and in the validity period, as follows:

ERCA(1)	ERCA(2)	ERCA(3)
BrainpoolP256r1	BrainpoolP384r1	BrainpoolP512r1

Note: The Certificate Effective Date (CEfD) of the ERCA(1) is January 1st, 2017, 00:00:00. The Certificate Effective Date of ERCA(2) starts 17 years later. Similarly, the CEfD of the ERCA(3) is 17 years after the ERCA(2) CEfD.

2. The set also contains the two link certificates between these three root keys.

3. For the MSCA and equipment levels, the set is based on the following assumptions:
   - MSCAs are free to use either Brainpool or NIST curves. For the Utopia MSCA it has been decided to adopt Brainpool curves. On the other hand, for the Arcadia MSCA, NIST curves are used.
   - Component personalizers and manufacturers must use either Brainpool or NIST, based on the choice made by 'their' MSCA.

4. Therefore, under each of the three ERCA certificates in bullet 1, the sample set contains:
   - Two key pairs and certificates necessary for a MSCA_VU-EGF in Utopia[2]. These certificates use the Brainpool curve of the length given by the relevant ERCA root certificate. These certificates have country code UTO (for Utopia). One of these MSCA_VU-EGF certificates has a Certificate Effective Date very close to the beginning of the private key usage period of the corresponding root certificate. The CEfD of the other MSCA_VU-EGF certificate is very close to the end of that key usage period.
   - Two key pairs and certificates necessary for a MSCA_Card in Utopia[3], using the same Brainpool curve as above. The Certificate Effective Dates of these certificates will be distributed in the same way as above.
   - Two key pairs and certificates necessary for a MSCA_VU-EGF in Arcadia[4], using the NIST curve of the length given by the relevant ERCA root certificate. The certificates will have country code ARC. The Certificate Effective Dates of these certificates will be distributed in the same way as Utopia certificates.
   - Two key pairs and certificates necessary for a MSCA_Card in Arcadia[5], also using the NIST curve. The Certificate Effective Dates of these certificates will be distributed in the same way as Utopia certificates.

UTO MSCA_Card(1)	UTO MSCA_Card(2)	UTO MSCA_Card(3)
BrainpoolP256r1	BrainpoolP384r1	BrainpoolP512r1

[2] The third ERCA generation is an exception; for this generation only one MSCA_VU-EGF certificate is generated, close to the beginning of the ERCA private key usage period.
[3] The third ERCA generation is an exception; for this generation only one MSCA_Card certificate is generated, close to the beginning of the ERCA private key usage period.
[4] The third ERCA generation is an exception; for this generation only one MSCA_VU-EGF certificate is generated, close to the beginning of the ERCA private key usage period.
[5] The third ERCA generation is an exception; for this generation only one MSCA_Card certificate is generated, close to the beginning of the ERCA private key usage period.

UTO MSCA_VU-EGF(1)	UTO MSCA_VU-EGF(2)	UTO MSCA_VU-EGF(3)
BrainpoolP256r1	BrainpoolP384r1	BrainpoolP512r1

ARC MSCA_Card(1)	ARC MSCA_Card(2)	ARC MSCA_Card(3)
NIST P-256	NIST P-384	NIST P-521

ARC MSCA_VU-EGF(1)	ARC MSCA_VU-EGF(2)	ARC MSCA_VU-EGF(3)
NIST P-256	NIST P-384	NIST P-521

This will allow testing card-VU and EGF-VU interaction for the same type of curve and between different types of curve, according to the above-mentioned assumptions on the domain parameters used in the components.

5. Under each MSCA_VU-EGF certificate, the set contains the keys and certificates needed by one VU. These are a VU_MA and a VU_Sign key pair plus certificate, as described in section 9.1.4 of Appendix 11. The Certificate Effective Dates of these certificates is close to the beginning of the usage period of the MSCA_VU-EGF private key used to sign it.

   So in total the set contains the VU_MA and VU_Sign certificates for 10 VUs.

6. Under each MSCA_Card certificate, the sample set contains all keys and certificates needed for a complete set of tachograph cards. These are the following key pairs and certificates, as described in section 9.1.5 of Appendix 11:
   - Driver Card_MA
   - Driver Card_Sign
   - Control Card_MA
   - Workshop Card_MA
   - Workshop Card_Sign
   - Company Card_MA

This means the set contains the keys and certificates for 10 sets of cards. The Certificate Effective Dates of these certificates are set close to the beginning of the usage period of the MSCA_Card private key.

7. Under each MSCA_VU-EGF certificate, the set contains the keys and certificates needed by one External GNSS Facility. This is a EGF_MA key pair plus certificate, as described in section 9.1.6 of Appendix 11. The Certificate Effective Date of these certificates is close to the beginning of the usage period of the MSCA_VU-EGF private key used to sign it.

So in total the set contains the EGF_MA certificate for 10 EGFs.

8. All of the abovementioned key pairs are valid ECC key pairs according to the requirements in Appendix 11.

9. All of the abovementioned certificates are valid, 'happy flow' certificates. This means that they comply with all requirements in Appendix 11 of Annex 1C regarding the certificate format.

3.2 Symmetric keys

10. The sample set contains three complete sets of ERCA motion sensor-related keys, as described in section 9.2.1 of Appendix 11:
    - Motion Sensor Master Key – VU part
    - Motion Sensor Master Key – Workshop part
    - Motion Sensor Master Key
    - Identification Key

These sets correspond to the first, second and third generation of the ERCA root certificate and are featured by a key length of 128 bits, 192 bits and 256 bits respectively.

11. Next to that, the sample set contains the following data for four Motion Sensors (see below for details):
    - One to three Pairing Key(s) (see CSM_117 in Appendix 11);
    - The encryption of the Pairing Key(s) with all valid generations of the Motion Sensor Master Key (as described in CSM_116 in Appendix 11);
    - The serial number;
    - The encryption of the serial number with all valid generations of the Identification Key (see CSM_116 in Appendix 11).

The 'production date' of these four Motions Sensors (MS) is chosen as follows (see Figure 4)[6]:

- MS_1 is issued at the beginning of the validity period of the ERCA(1) certificate. This MS has one Pairing Key of 128 bits long. This Pairing Key is additionally present in encrypted form, using the first-generation (128-bits) Motion Sensor Master Key. The serial number is present in plaintext form as well as encrypted with the 128-bits Motion Sensor Master Key.
- MS_2 is issued at the beginning of the validity period of the ERCA(2) certificate. This MS has two Pairing Keys, one 128 bits, the other 192 bits. These Pairing Keys are additionally present in encrypted form, using the first-generation (128-bits) and second-generation (192-bits) Motion Sensor Master Key, respectively. The serial number is present in plaintext form as well as encrypted twice, once using both of these Motion Sensor Master Keys.
- MS_3 issued at the end of the private key usage period of the ERCA(2) certificate. This MS has three Pairing Keys, of 128 bits, 192 bits and 256 bits length. These Pairing Keys are additionally present in encrypted form, using the first, second and third generation Motion Sensor Master Key, respectively. The serial number is present in plaintext form as well as encrypted thrice, once using each of these Motion Sensor Master Keys.
- MS_4 issued at the beginning of the validity period of the ERCA(3) certificate. This MS has two Pairing Keys, one 192 bits, the other 256 bits. These Pairing Keys are additionally present in encrypted form, using the second-generation (192-bits) and third-generation (256-bits) Motion Sensor Master Key,

[6] Note that these production dates are not directly mentioned in the cryptographic material. They just influence the number of Pairing Keys and encrypted serial numbers stored in the motion sensor.

respectively. The serial number is present in plaintext form as well as encrypted twice, once using both of these Motion Sensor Master Keys.

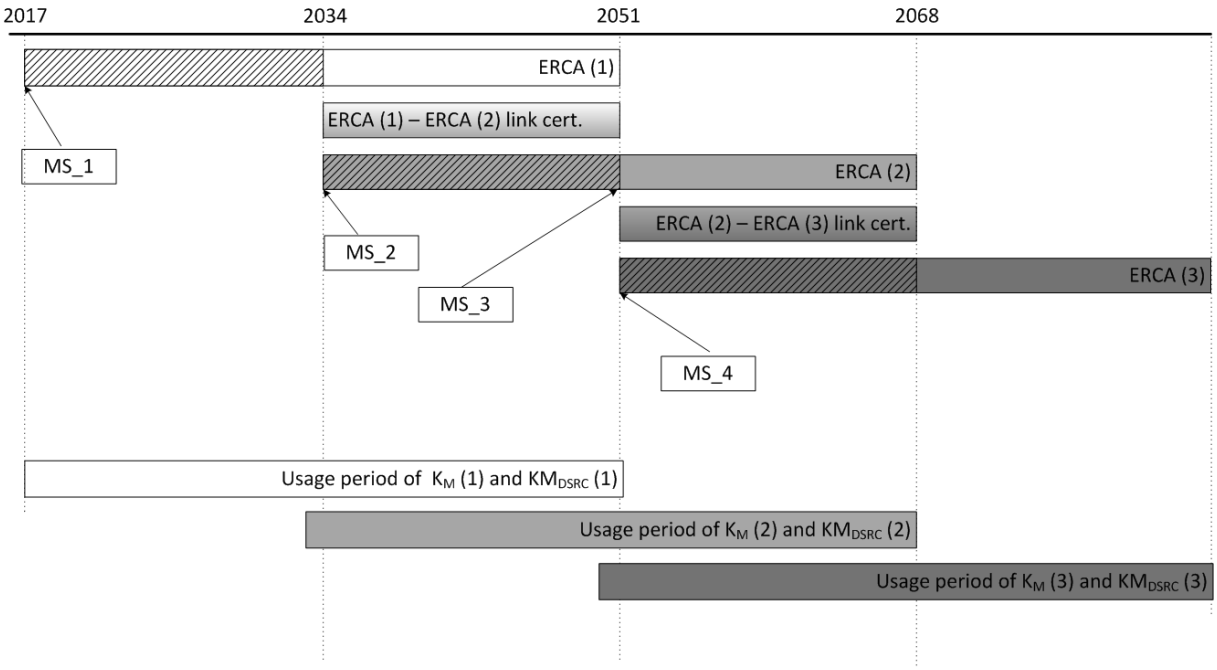


Figure 4 'Production dates' of Motion Sensors contained in the sample set. Motion Sensor Master Key and DSRC Master Key usage periods.

12. The sample set contains three DSRC Master Keys as described in section 9.2.2 of Appendix 11, with a length of 128 bits, 192 bits and 256 bits respectively, for each of the key generations defined in Appendix 11. This is depicted in Figure 4.

13. Next to that, for each of the VUs for which the set contains VU_MA and VU_Sign key pairs and certificates (see section 3.1), the sample set also contains the VU-specific keys K_VU_{DSRC}_ENC and K_VU_{DSRC}_MAC, as specified in section 9.2.2 of Appendix 11. For each VU, the correct DSRC Master Key has been used (following from the Certificate Effective Date of that VU). As diversification data, the serial number of the VU is used, which is equal to the CHR in this VU's MA or Sign certificate.

4 Data element values for certificates

This chapter describes how the values for all fields in all certificates are set in detail.

Section 4.1 describes the values used for ERCA root certificates and ERCA link certificates.

Section 4.2 describes the values used for MSCA certificates.

Section 4.3 describes the values used for VU, EGF and card certificates.

4.1 ERCA (link) certificates

Field	Value
Certificate Profile Identifier	'00'
Certificate Authority Reference	See for CHR below, except for keySerialNumber: for the first link certificate the keySerialNumber is '01', for the second link certificate it is '02'.
Certificate Holder Authorisation	
• tachographApplicationID	'FF 53 4D 52 44 54' (per Appendix 1)
• equipmentType	13 (decimal) (per Appendix 1)
Domain Parameters	OID of the Brainpool curve with the correct key length, see section 2.1 and Appendix 11
Certificate Holder Reference	
• nationNumeric	'FD'
• nationAlpha	"EC "
• keySerialNumber	For root certificates: Use '01' for the first certificate, '02' for the second certificate, etc. For link certificates, Use '02' for the first certificate, '03' for the second certificate.
• additionalInfo	'FF FF'
• caIdentifier	'01'
Certificate Effective Date (CEfD)	January 1st, 2017, 00:00:00 for the first certificate; the CEfD of the other generations follow then automatically.
Certificate Expiry Date (CExD)	Follows from CEfD and the validity period of the certificate type specified in Appendix 11.

4.2 MSCA certificates

Field	Value
Certificate Profile Identifier	'00'
Certificate Authority Reference	See for CHR of ERCA above.
Certificate Holder Authorisation	
• tachographApplicationID	'FF 53 4D 52 44 54' (per Appendix 1)
• equipmentType	14 (decimal) (per Appendix 1) Note: there is no difference for MSCA_VU-EGF and MSCA_Card certificates.
Domain Parameters	For country UTO: OID of the Brainpool curve with the correct key length, see section 2.1 and Appendix 11 For country ARC: OID of the NIST curve with the correct key length
Certificate Holder Reference	
• nationNumeric	For country UTO: 'FB For country ARC: 'FC' (Values not currently in use)
• nationAlpha	"UTO" for Utopia "ARC" for Arcadia
• keySerialNumber	Per MSCA, use 1 for the first certificate, 2 for the second certificate, etc.
• additionalInfo	'FF FF'
• caIdentifier	'01'
Certificate Effective Date (CEfD)	For both UTO and ARC and for both MSCA_Card and MSCA_VU-EGF certificates: • For the first certificate (1-1), equal to CEfD of the first ERCA certificate. • For the second certificate (1-2), equal to the end of the private key usage period of the first ERCA certificate, minus one second. • For the third certificate (2-1), equal to the CEfD of the second ERCA certificate. • Etc.
Certificate Expiry Date (CExD)	Follows from CEfD and the validity period of the certificate type specified in Appendix 11. Note that this period is different for MSCA_VU-

	EGF and MSCA_Card certificates.

4.3 Equipment certificates

Field	Value
Certificate Profile Identifier	'00'
Certificate Authority Reference	See for CHR of MSCA above.
Certificate Holder Authorization	
• tachographApplicationID	'FF 53 4D 52 44 54' (per Appendix 1)
• equipmentType	Per Appendix 1, all values decimal. Driver Card (for MA): 1 Workshop Card (for MA): 2 Control Card: 3 Company Card: 4 Vehicle Unit (for MA): 6 External GNSS Facility: 8 Driver Card (for signing): 17 Workshop Card (for signing): 18 Vehicle Unit (for signing): 19
Domain Parameters	For equipment issued under country UTO, OID of the Brainpool curve with the correct key length, see section 2.1 and Appendix 11. For equipment issued under country ARC, OID of the NIST curve with the correct key length.
Certificate Holder Reference	
• serialNumber	Sequential numbering per type of equipment. Note that the same serialNumber is used for the Signing and MA certificate of the same piece of equipment.
• monthYear	Consistent with Certificate Effective Date
• type	Per Appendix 1, all values decimal. Driver Card 1 Workshop Card 2 Control Card: 3 Company Card: 4 Vehicle Unit 6 External GNSS Facility: 8

	Note that for signing certificates, this value is different from equipmentType in the Certificate Holder Authorization.
• manufacturerCode	'FF' (Value not currently used)
Certificate Effective Date (CEfD)	Equal to CEfD of signing MSCA certificate.
Certificate Expiry Date (CExD)	Follows from CEfD and the validity period of the certificate type specified in Appendix 11.

5 Key and certificate file formats

5.1 Asymmetric keys and certificates

14. Asymmetric private keys are present in the sample set in plaintext PKCS #8 format, according to RFC 5958 [5] and related. This format is explained in more detail in Appendix 2.

15. Public key certificates are present in the set in the plaintext format specified in Appendix 11.

5.2 Symmetric keys

16. The sample set contains all symmetric keys in plaintext format.

5.3 File names

17. Each private key, each certificate and each symmetric key is stored in a separate file. Key identification (type, validity period) is done by means of the file name for each key file. The naming convention is the same as the convention described in section 3, except that a prefix is added where appropriate for MSCA and equipment certificates to indicate the country (ARC or UTO). Note that keys and certificates are located in folders that help clarify their meaning.

Examples

Some example file names for asymmetric keys and certificates, which are located in the folder 'ECC keys and certificates' are given below:

Folder: ...\ERCA\

- ERCA (1).pkcs8 contains the private key of the first the ERCA root key pair. As explained above, this private key uses the Brainpool256r1 standardized domain parameters.
- ERCA (2).cert contains the certificate of the second root key pair. This certificate uses the Brainpool384r1 domain parameters.

Folder: …\ERCA\MSCA\ARC\

- ARC_MSCA_VU-EGF (1-1).cert contains the first MSCA_VU-EGF certificate issued under ERCA(1). This certificate uses the NIST P-256 domain parameters because the country is Arcadia. As explained above, this certificate is issued very close to the beginning of the private key usage period of the ERCA(1) root key pair.

Folder: …\ ERCA\MSCA\ARC\Equipment\TC\

- ARC_Workshop Card_Sign (2-2).cert contains the second Workshop Card_Sign certificate issued under ERCA(2). This certificate is issued very close to the end of the private key usage period of the ERCA(2) certificate. This certificate uses the NIST P-384 domain parameters.

Some example file names for asymmetric keys and certificates, which are located in the folder 'AES keys' are given below:

Folder: …\DSRC keys\ERCA-MSCA\

- DSRCMK-1.bin contains the first-generation DSRC Master Key. This key has a length of 128 bits.

Folder …\DSRC keys\ERCA-MSCA\UTO\Equipment\

- UTO_VU (1-1)_DSRCK_ENC.bin contains the $K\_VU_{DSRC}\_ENC$ belonging to the VU(1-1) for Utopia. This key has been derived from DSRCMK-1 by diversifying with the serial number of this VU, which is equal to the CHR in this VU's MA or Sign certificate. (This certificate can be found in the folder …\ECC keys and certificates\ERCA\MSCA\UTO\Equipment\VU\)

Folder …\Motion sensor keys and encrypted data\ERCA-MSCA\

- MSMK-3.bin contains the third-generation Motion Sensor Master Key, which has a length of 256 bits. This key has been created by XOR-ing the key in MSMK-3-VU.bin and the one in MSMK-3-WS.bin. The Identification Key that is derived from this Motion Sensor Master Key can be found in the file MSIK-3.bin.

Folder …\Motion sensor keys and encrypted data\ERCA-MSCA\Equipment\

- MS-2-PK-1.bin contains the first-generation Pairing Key for motions sensor MS-2. This is a 128-bits keys allowing the motion sensor to be paired with a first-generation VU. Similarly, MS-2-PK-2 is the second-generation Pairing Key for this motion sensor.
- MS-2-PK-ENC-2.bin contains the encryption of this second-generation Pairing Key with the second-generation Motion Sensor Master Key (which itself can be found in the file MSMK-2.bin.)
- MS-2-SN.bin contains the serial number of this motion sensor.
- MS-2-SN-ENC-1.bin contains the encryption of this serial number with the first-generation Identification Key. Similarly, MS-2-SN-ENC-2.bin contains the encryption of the same serial number with the second-generation Identification Key.

6 Testing possibilities

6.1 Testing possibilities with the sample set

These certificates and the associated key pairs allow extensive testing of the security mechanisms specified in Appendix 11:

- Testing the correctness of the implementation of the AES, SHA-2 and ECC algorithms, using all specified key lengths and standardized domain parameters.
- Verification of a card certificate chain by a VU, including the possible use of a link certificate and the verification of the temporal validity of all certificates in the chain.
- Verification of a VU certificate chain by a tachograph card, including the possible use of a link certificate and the verification of the temporal validity of all certificates in the chain.
- The VU authentication mechanism, described in section 10.3 of Appendix 11.
- Chip Authentication and Session Key Agreement according to section 10.4 of Appendix 11.
- The Secure Messaging protocol between a VU and a card.
- The VU and EGF coupling mechanism.
- VU and EGF normal operation, including the use of Secure Messaging.
- Signing of downloaded data by a VU, including doing so in the first three months after the normal 15-year life period of the VU. See also CSM_78 and CSM_91 in Appendix 11.
- Signing of downloaded data by a driver card or workshop card, including doing so in the first month after the normal life period of the card. See also CSM_89 in Appendix 11.

In addition, the symmetric key material in the sample set allows testing of

- The interaction between a VU and a motion sensor (with the support of a workshop card) during pairing and their secure communication, as specified in chapter 12 of the Appendix 11, including the use of different key generations.
- The correct protection of the remote early detection communication link. This is described in chapter 13 of Appendix 11.

Please note that this list is informative only.

6.2 Other tests

There are a few situations that cannot be tested with the current sample set. Examples include:

- Using link certificates where the 'old' cipher suite has the same strength as the new one, or where the link certificate moves directly from the weakest to the strongest suite.
- Using a VU issued for instance under ERCA generation 2 and letting it interact with a card issued under ERCA(1), in case the VU is in fact issued earlier than the card. (So the VU, which uses 384-bits security, is actually older than the card, which uses 256-bits security.) This situation will occur towards the end of the private key usage period of the last MSCA key pairs issued under ERCA(1). Because this is somewhat unusual intuitively, badly implemented cards or VUs may not handle this situation correctly.
- The possible update of the card's current time as described in CSM_167. In theory it would be possible to test this with the provided set, e.g. by inserting a Card (1-2) in a VU (2-1). The card's current time should then be updated from 31-12-2033 23:59:59 to 01-01-2034 00:00:00. However, the problem may be

how to check that this update occurred. Maybe other certificates should be designed with validity dates suitable to test this behaviour.

Other tests may be envisioned as well. While such tests cannot be executed using the provided sample set, stakeholders may still carry out such tests if they choose to generate additional sample certificates and key pairs.

References

Ref.	Title
[1]	Council Regulation (EC) No 2135/98 of 24th September 1998; Official Journal of the European Communities L274
[2]	Commission Regulation (EC) No 1360/2002 of 13th June 2002; Official Journal of the European Communities L207
[3]	Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014; Official Journal of the European Union L60
[4]	Commission Implementing Regulation (EU) 2016/799 of 18 March 2016; Official Journal of the European Union L 139
[5]	RFC 5958 (Asymmetric Key Packages), S. Turner, August 2010
[6]	RFC 5912 (New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)), P. Hoffman et al., June 2010
[7]	RFC 5915 (Elliptic Curve Private Key Structure), S. Turner et al., June 2010
[8]	Technical Guideline TR-03111 (Elliptic Curve Cryptography) v2.0, BSI, 2012-06-28

List of abbreviations and definitions

AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
EGF	External GNSS Facility
ERCA	European Root Certificate Authority
GNSS	Global Navigation Satellite System
MA	Mutual Authentication
MS	Motion Sensor
MSCA	Member State Certificate Authority
PKI	Public Key Infrastructure
RCF	Remote Communication Facility
REDCR	Remote Early Detection Communication Reader
SHA-2	Secure Hash Algorithm 2
TC	Tachograph Card
VU	Vehicle Unit

List of figures

Appendix 1 Cryptographic elements per component

This Appendix describes all of the asymmetric keys, certificates and symmetric keys that are contained in each instance of the four main components of the Smart Tachograph system at issuance.

Appendix 1.1 Cryptographic elements installed in a Vehicle Unit

Asymmetric keys and certificates

Description	Purpose	Type	Source
VU private key and public key certificate for Mutual Authentication	Used by the VU to perform VU authentication towards tachograph cards and external GNSS facilities	ECC	Private key generated by VU or VU manufacturer. Certificate created and signed by MSCA
VU private key and public key certificate for signing	Used by the VU to sign downloaded data files	ECC	Private key generated by VU or VU manufacturer. Certificate created and signed by MSCA
ERCA root public key(s) and certificate(s)[7]	Used by the VU for the verification of MSCA certificates issued under the corresponding ERCA root certificate.	ECC	Generated by ERCA; inserted in VU by manufacturer at the end of the manufacturing phase or obtained from card or EGF during lifetime
Certificate of MSCA responsible for signing the VU_MA and VU_Sign certificates	Used by a card, EGF or dedicated equipment to obtain and verify the MSCA_VU-EGF public key they will subsequently use to verify the VU_MA or VU_Sign certificate		Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase

Table 4: Overview of VU asymmetric keys and certificates

Symmetric keys

Description	Purpose	Type	Source
Motion Sensor Master Key – VU part	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU.	AES	Generated by ERCA; inserted by VU manufacturer at the end of the manufacturing phase.
VU-specific DSRC keys for authenticity and confidentiality	Two separate keys used to ensure the authenticity confidentiality of data sent over a DSRC link between a RCF and a REDCR	AES	Derived by MSCA based on DSRC Master Key and VU serial number; inserted by VU manufacturer at the end of the manufacturing phase

Table 5: Overview of VU symmetric keys

[7] Note: Because of the regular replacement of the ERCA root key a VU may contain more than one ERCA certificates and Link certificates.

Appendix 1.2 Cryptographic elements installed in a Motion Sensor

Asymmetric keys and certificates

A motion sensor does not contain any asymmetric keys or certificates.

Symmetric keys

Description	Purpose	Type	Source
Motion sensor pairing key	Used by a VU for encrypting the motion sensor session key when sending it to the motion sensor during pairing.	AES	Generated by the motion sensor manufacturer; stored in motion sensor at the end of the manufacturing phase

Table 6: Overview of Motion Sensor symmetric keys

Apart from this key, a motion sensor contains the value of the pairing key encrypted under the motion sensor master key. It also contains the value of its serial number encrypted under the identification key[8].

Appendix 1.3 Cryptographic elements installed in a Tachograph Card

Asymmetric keys and certificates

Description	Purpose	Type	Source
Card private key and public key certificate for Mutual Authentication and session key agreement	Used by the card to perform card authentication towards VUs and perform session key agreement	ECC	Generated by card or card manufacturer/personaliser at the end of the manufacturing phase
Card private key and public key certificate for signing	Used by the card to sign downloaded data files.	ECC	Generated by card or card manufacturer/personaliser at the end of the manufacturing phase. Driver cards and workshop cards only
Certificate of MSCA responsible for signing the Card_MA and/or Card_Sign certificates	Used by a VU or dedicated equipment to obtain and verify the MSCA_Card public key they will subsequently use to verify the Card_MA or Card_Sign certificate	ECC	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase
ERCA root public key(s) and certificate(s)	Used by the card for the verification of MSCA certificates issued under the corresponding ERCA root certificate.	ECC	Generated by ERCA; inserted in card by manufacturer at the end of the manufacturing phase or obtained from VU during lifetime

Table 7: Overview of TC asymmetric keys and certificates

[8] Note: Because the motion sensor master key and all associated keys are regularly replaced, up to three different encryptions of the pairing key and the serial number (based on consecutive generations of the motion sensor master key) may be present in a motion sensor.

Symmetric keys

Description	Purpose	Type	Source
Motion sensor master key – workshop card part[9]	Allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU	AES	Generated by ERCA; inserted in card by card manufacturer Workshop cards only
DSRC Master Key[10]	Master key to derive keys to protect confidentiality and authenticity of data sent from a VU to a control authority over a DSRC channel	AES	Generated by ERCA; inserted in card by card manufacturer Control and workshop cards only

Table 8: Overview of TC symmetric keys

Appendix 1.4 Cryptographic elements installed in an EGF

Asymmetric keys and certificates

Description	Purpose	Type	Source
EGF private key and public key certificate for Mutual Authentication	Used by the EGF to perform EGF authentication towards VUs	ECC	Private key generated by EGF or EGF manufacturer at the end of the manufacturing phase Certificate created and signed by MSCA
Certificate of MSCA responsible for signing the EGF_MA certificate	Used by a VU to obtain and verify the MSCA_VU-EGF public key it will subsequently use to verify the EGF_MA certificate	ECC	Created and signed by ERCA based on MSCA input; inserted by manufacturer at the end of the manufacturing phase
ERCA root public key(s) and certificate(s)	Used by the EGF for the verification of MSCA certificates issued under the corresponding ERCA root certificate.	ECC	Generated by ERCA; inserted in EGF by manufacturer at the end of the manufacturing phase or obtained from VU during lifetime

Table 9: Overview of EGF asymmetric keys and certificates

Symmetric keys

At issuance, an EGF does not contain any symmetric keys.

[9] Note: Because of the regular replacement of the ERCA root key and all associated keys, a workshop card may in fact contain up to three of these keys.

[10] Note: Because of the regular replacement of the ERCA root key and all associated keys, a control or workshop card may in fact contain up to three of these keys

Appendix 2 Format of .pkcs8 files

Format of .pkcs8 files in the sample set, according to RFC 5958 [5]. All values hexadecimal.

30	**L**	SEQUENCE SIZE (1) OF OneAsymmetricKey; see RFC 5958 [5]. 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 [6]				
				06	**L**	**V**	PrivateKeyAlgorithms: see data type ECParameters in RFC 5912 [6]. 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 [5]							
				30	**L**	ECPrivateKey; see RFC 5915 [7]. 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 [8]

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

KJ-NA-28475-EN-N

JRC Mission

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

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/716503

ISBN 978-92-79-65787-0