European Commission

JRC TECHNICAL REPORTS

Smart Tachograph

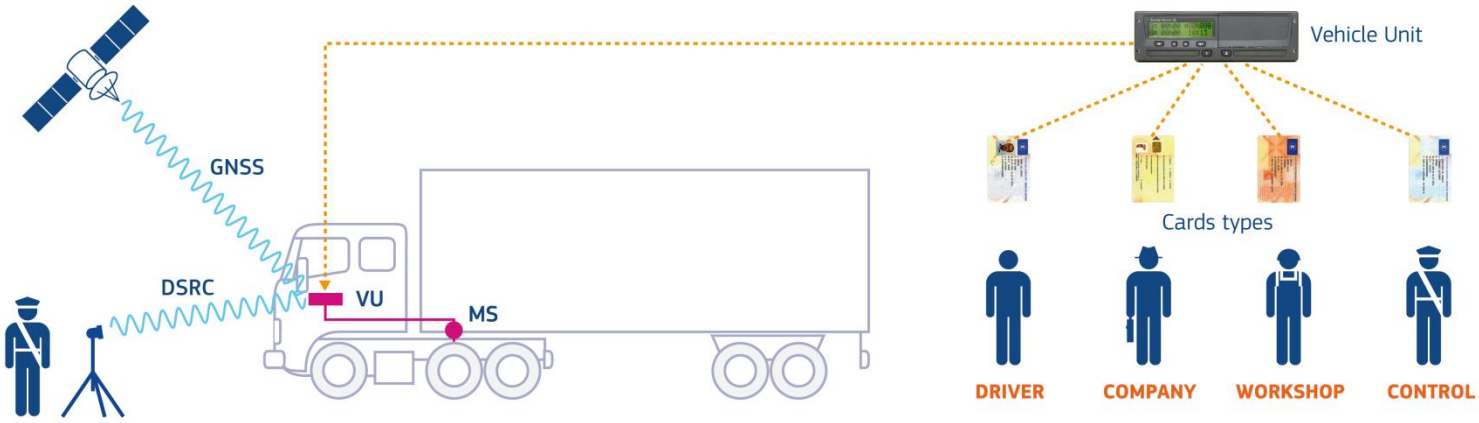
Certificate signing requests, key distribution requests and key distribution messages sample set

Version 1.0

February 2018

David Bakker (UL)

Luigi Sportiello (JRC)



Joint Research Centre

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

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

JRC110932

Ispra: European Commission, 2018

How to cite this report: Bakker D., Sportiello L.; Smart Tachograph: Certificate signing requests, key distribution requests and key distribution messages sample set.

Contents

1 Introduction

The digital tachograph system (Generation-1 Digital Tachograph) was originally 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 Digital Tachograph system, called the 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 mechanisms used to protect the data stored and transmitted in the Smart Tachograph system.

The cryptographic keys and certificates used in combination with these security mechanisms must be distributed securely between the different parties in the Smart Tachograph ecosystem. In particular, some of the keys and of the certificates have to be exchanged between an appointed European Authority (the ERCA) and appointed Member State Authorities (the MSCAs). The key and certificate distribution mechanisms and messages used between the ERCA and the MSCAs are specified in full in the ERCA Certificate Policy (CP) [10]. The CP includes a full specification of the format of Certificate Signing Requests (CSR) which MSCAs may send to the ERCA in order to obtain a signed certificate for a MSCA public key. The ERCA CP also describes the format of Key Distribution Requests (KDR) that MSCAs may use to request a symmetric master key from the ERCA, and the format of Key Distribution Messages (KDM) that the ERCA will use to securely distribute a key to an MSCA in response to a KDR.

1.1 Scope of this document

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; see [9].

In order to help MSCAs with the development and testing of their systems for creating CSRs and KDRs and processing KDMs, this cryptographic keys and digital certificates sample set [9] is complemented with CSRs, KDRs and KDMs samples. These messages are created in such a way that the values of the keys and certificates embedded in them are fully consistent with the ERCA and MSCAs cryptographic keys and digital certificates in the sample set. Basically the CSRs, KDRs and KDMs samples represent the distribution messages for the ERCA and MSCAs keys and certificates that are in the sample set.

The current document serves to detail the contents of the CSRs, KDRs and KDMs samples. It must be read in conjunction with the description of the cryptographic keys and digital certificates sample set, see [9].

1.2 Intended audience

This document is intended for MSCA employees and contractors involved in the development of MSCA systems that will generate or process the certificate signing requests, key distribution requests and key distribution messages which the MSCA will use to communicate with the ERCA.

Readers of this document should be familiar with Appendix 11 to Annex 1C [4] and with the ERCA Certificate Policy [10].

Readers of this document should also be familiar with the contents of the cryptographic keys and digital certificates sample set [9].

1.3 Disclaimer

The CSRs, KDRs and KDMs samples have to be seen only as a support to the development and testing processes of the MSCAs. In the event of any conflict between the contents of the samples and the ERCA Certificate Policy, the latter shall prevail. Each MSCA remains fully responsible for making sure that their systems comply with all requirements in the ERCA Certificate Policy [10] and the Commission Implementing Regulation (EU) 2016/799 [4].

2 CSR, KDR and KDM formats

For an overview of the Smart Tachograph system and it security mechanisms, please refer to Chapter 2 of [9]. For an explanation of the mechanisms used for distributing keys and certificates between the ERCA and the MSCAs, please refer to chapter 4 of [10]. For the convenience of the reader, this section summarizes the formats of the CSRs, KDRs and KDMs specified in [10].

2.1 Certificate Signing Request format

The format of the Certificate Signing Requests sent by the MSCAs to the ERCA in order to obtain a signed MSCA certificate for an MSCA public key is show in the table below:

Data Object	Presence	Tag
Authentication	c	'67'
ECC (CV) Certificate	m	'7F 21'
Certificate Body	m	'7F 4E'
Certificate Profile Identifier	m	'5F 29'
Certification Authority Reference	m	'42'
Certificate Holder Authorisation	m	'5F 4C'
Public Key	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'
Certificate Holder Reference	m	'5F 20'
Certificate Effective Date	m	'5F 25'
Certificate Expiry Date	m	'5F 24'
Inner Signature	m	'5F 37'
Certification Authority Reference of Outer Signature Signatory	c	'42'
Outer Signature	c	'5F 37'

Table 1 Certificate Signing Request format

As specified in section 4.1.1 of the ERCA Certificate Policy, the Inner Signature is self-signed, i.e., it is created using the private key belonging to the public key in the certificate body.

Table 1 shows that the presence of the Authentication tag and length, the Certification Authority Reference of Outer Signature Signatory object and the Outer Signature object is conditional. In fact, these fields are only present in case the CSR is not the first CSR originating from a certain MSCA. For all subsequent CSRs, the Outer Signature is created by one of the currently valid MSCA certificates of the same type. For all details of CSR contents and formatting, please refer the ERCA Certificate Policy [10].

2.2 Key Distribution Request format

The format of the Key Distribution Requests sent by the MSCAs to the ERCA in order to obtain a symmetric master key is show in the table below:

Data object	Presence	Tag
Key Distribution Request	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorisation	m	'83'
Key Identifier	m	'84'
Public Key (for ECDH key agreement)	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'

Table 2 Key Distribution Request format

The Message Recipient Authorisation encodes the type and version of the requested symmetric key.

When an MSCA creates a KDR, it must generate an ephemeral ECDH key pair for key agreement. The public key of this key pair is put it the KDR as shown in Table 2; the private key is kept in the HSM of the MSCA. See next section for a summary of the key agreement process.

The Key Identifier in the KDR is a unique 8-byte octet string identifying the MSCA ephemeral public key for key agreement.

For all details of KDR contents and formatting, please refer to section 4.2.1 of the ERCA Certificate Policy [10].

2.3 Key Distribution Message format

The format of a Key Distribution Message sent by the ERCA to an MSCA in response to a Key Distribution Request is show in the table below:

Data object	Presence	Tag
Key Distribution Message	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorisation	m	'83'
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	m	'84'
Public Point of the ERCA for ECDH key agreement	m	'86'
Encrypted symmetric key	m	'87'
MAC	m	'88'

Table 3 Key Distribution Message format

The Message Recipient Authorisation encodes the type and version of the distributed symmetric key. It is copied from the related KDR; see previous section.

The Key Identifier in the KDM is copied by the ERCA from the related Key Distribution Request, see previous section. When the MSCA receives the KDM, it uses the Key Identifier to identify the private key that it must use to perform key agreement.

When the ERCA creates a Key Distribution Message, it generates an ephemeral ECDH key pair for key agreement, using the standardized domain parameters indicated in the KDR from the MSCA. It includes the Public Point in the KDM; see Table 3. Next, it performs ECDH key agreement using its ephemeral private key and the ephemeral public key in the KDR. Key agreement results in two AES keys: one key K_{ENC} for encryption and one key K_{MAC} for authentication.

The ERCA uses K_{ENC} to encrypt the requested symmetric key. It then puts the encrypted symmetric key in the KDM as shown in Table 3. Next, the ERCA uses K_{MAC} to calculate a MAC over the encrypted key, the Message Recipient Authorisation and the Key Identifier. The MAC is put in the KDM.

When the Key Distribution Message arrives at the MSCA, the MSCA uses the Key Identifier to identify the private key in its HSM that it must use for key agreement. The MSCA uses this private key, together with the ERCA public point in the KDM, to arrive at the same AES keys that the ERCA derived. The MSCA uses these keys to verify the MAC in the KDM and decrypt the encrypted symmetric key.

For all details of KDM contents and formatting, please refer to section 4.2.4 of the ERCA Certificate Policy [10].

3 Contents and values of CSR, KDR and KDM samples

3.1 Overview

This chapter describes the CSR, KDR and KDM sample messages. It describes the folder structure containing these sample messages, the logic behind the presence of these messages, and the contents of these messages.

At the top level of the sample set two folders are present, called 'CSRs' and 'KDRs and KDMs'. These folders are in correspondence to the two top folders of the set of cryptographic keys and digital certificates samples [9], namely 'ECC keys and certificates' and 'AES keys'.

Section 3.2 describes the CSRs present in the sample set.

Section 3.3 describes the KDRs and KDMs.

3.2 Certificate Signing Requests

3.2.1 CSRs present

The logic behind the presence of the CSRs is as follows: for every MSCA certificate present in the folder 'ECC keys and certificates' of the set of cryptographic keys and digital certificates samples, there is a corresponding CSR in the folder 'CSRs'. Please note that no CSRs are present for the ERCA certificates, since such certificates will not be requested by means of a CSR. Neither are any CSRs present for the equipment certificates, since the format of the CSRs used to request such certificates is MSCA-specific and out of scope for this document.

3.2.2 CSR file naming

The name of each CSR in the sample set is consistent with the name of the corresponding certificate; please refer to [9] for more information on the naming system for the certificates.

For example, the MSCA for Arcadia may have used ARC_MSCA_Card (1-1)_CSR to request the ERCA to sign certificate ARC_MSCA_Card (1-1). This means that the Certificate Body object in the CSR (see section 2.1) is identical to the Certificate Body in the corresponding certificate.

3.2.3 Data element values for CSRs

Apart from the Certification Authority Reference of Outer Signature Signatory field, the Outer Signature and the Inner Signature, the value of all data elements in a CSR in the sample is equal to the corresponding data element value in the corresponding certificate. Please refer to chapter 4 in [9].

Regarding the Certification Authority Reference of Outer Signature Signatory field: the value of this field in a CSR is equal to the value of the Certificate Holder Reference field in the certificate that must be used to verify the outer signature, if present. The outer signature is created by the previous MSCA private key of the same type (MSCA_VU-EGF or MSCA_Card). For example:

- The outer signature of ARC_MSCA_Card (1-2)_CSR can be verified using the public key in certificate ARC_MSCA_Card (1-1).
- The outer signature of ARC_MSCA_Card (2-1)_CSR can be verified using the public key in certificate ARC_MSCA_Card (1-2).
- The outer signature of UTO_MSCA_VU-EGF (3-1)_CSR can be verified using the public key in certificate UTO_MSCA_VU-EGF (2-2).

Note that the outer signature (including the Certification Authority Reference of Outer Signature Signatory field and the Authentication tag and length) is absent for all CSRs whose name ends with …(1-1)_CSR, because these certificates are the first ones for the particular MSCA (UTO or ARC) and MSCA type (MSCA_VU-EGF or MSCA_Card).

3.3 Key Distribution Requests and Messages

3.3.1 KDRs and KDMs present

The logic behind the presence of the KDRs and KDMs in the sample set is summarized here. According to section 4.2.1 of the ERCA Certificate Policy, there are four master keys that must be distributed from the ERCA to the MSCAs, namely

- the motion sensor master key (MSMK),
- the motion sensor master key - workshop part (MSMK-WC),
- the motion sensor master key - VU part (MSMK-VU),
- the DSRC master key (DSRCMK).

These keys are present in the folder 'AES keys' of the set of cryptographic keys and digital certificates samples. Each of them has to be distributed to the MSCAs of Arcadia and Utopia. The KDRs, KDMs and associated data corresponding to these distributions are in the folder 'KDRs and KDMs'.

Note that no KDR – KDM pairs are present for the VU-specific DSRC keys in the sample set. Neither are there KDR – KDM pairs for the distribution of the encrypted motion sensor serial number and Pairing Key. This is because the format of these KDRs and KDMs is MSCA-specific and out of scope for this document.

3.3.2 KDR and KDM file naming and folder contents

In the folder 'KDRs and KDMs', a separate folder is present for each master key to be distributed to Arcadia and Utopia, with the name of the folder reflecting the name of the master key. In each folder the KDR, its associated KDM and also additional key material is present. For example, the folder for the distribution of the DSRCMK-1 master key to the UTO MSCA contains the following files (in alphabetic order):

- DSRCMK-1_UTO_erca_ephemeral_private_key.pkcs8
- DSRCMK-1_UTO_KDM.bin
- DSRCMK-1_UTO_KDR.bin
- DSRCMK-1_UTO_Kenc.bin
- DSRCMK-1_UTO_Kmac.bin
- DSRCMK-1_UTO_msca_ephemeral_private_key.pkcs8

The contents of these files are described below:

- DSRCMK-1_UTO_KDR.bin contains the key distribution request sent by the UTO MSCA to the ERCA to receive the DSRCMK-1 key.
- DSRCMK-1_UTO_KDM.bin contains the associated KDM, sent by the ERCA to the UTO MSCA.

- DSRCMK-1_UTO_msca_ephemeral_private_key.pkcs8 contains the plain-text value of the ephemeral ECDH private key for key agreement generated by the UTO MSCA in the course of creating the KDR – see section 4.2.3 of the ERCA CP, ref. [10]. The structure of this file complies with Appendix 1 in this document.
- DSRCMK-1_UTO_erca_ephemeral_private_key.pkcs8 contains the plain-text value of the ephemeral ECDH private key for key agreement generated by the ERCA in the course of creating the KDM.
- DSRCMK-1_UTO_Kenc.bin and DSRCMK-1_UTO_Kmac.bin contain the plain-text values of K_{ENC} and K_{MAC}, respectively. These keys are used to protect the confidentiality, authenticity and integrity of the distributed key. As described in section 4.2.3 of the ERCA CP, these keys are derived from the value of the ephemeral key pairs of the ERCA and of the MSCA used in the KDR-KDM exchange.

Similarly for other master keys: the associated folder will contain the same files but with the first part of all file names changed accordingly

3.3.3 Data element values for KDRs in the sample set

Field	Value
Request Profile Identifier	'00'
Message Recipient Authorisation	
• The six most significant bytes of the Tachograph Application ID	'FF 53 4D 52 44 54'
• Key type	'07' for motion sensor master key (file name contains "MSMK-x") '27' for motion sensor master key workshop part (file name contains "MSMK-WC-x") '67' for motion sensor master key VU part (file name contains "MSMK-VU-x") '09' for DSRC master key (file name contains "DSRCMK-x")
• version number of the requested master key	'01', '02' or '03', as indicated in file name
Key Identifier	
• NationNumeric	For country UTO: 'FB For country ARC: 'FC'
• NationAlpha	"UTO" for Utopia "ARC" for Arcadia
• keySerialNumber	Per MSCA, use 1 for the first KDR (= first ephemeral key), 2 for the second one, etc.

• additionalInfo	'4B 52' ("KR")
• CA identifier	'01'
Public Key (for ECDH key agreement)	
• Standardised Domain Parameters OID	For country UTO: OID of the Brainpool curve with the correct key length, see Appendix 11 For country ARC: OID of the NIST curve with the correct key length, see Appendix 11
• Public Point	Random value of the correct length

3.3.4 Data element values for KDMs in the sample set

Field	Value
Request Profile Identifier	'00'
Message Recipient Authorisation	Equal to the Message Recipient Authorisation field in the corresponding KDR, see previous section
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	Equal to the Key Identifier field in the corresponding KDR, see previous section
Public Point of the ERCA for ECDH key agreement	Random value of length equal to the length of the Public Point in the corresponding KDR, see previous section
Encrypted symmetric key	The symmetric key requested in the corresponding KDR, encrypted with K_{ENC} as specified in the ERCA Certificate Policy
MAC	The MAC, calculated using K_{MAC} as specified in the ERCA Certificate Policy

4 Testing possibilities with the CSRs and KDRs

The CSRs and KDRs allow extensive testing of the mechanisms specified in chapter 4 of the ERCA Certificate Policy:

- An MSCA can verify that its system is capable of generating the correct CSR for all MSCA certificates in the sample set, including the outer signature (if present). The CSRs generated by its system should be fully equal to the CSRs in the sample set.
- An MSCA can verify that its system is capable of generating the correct KDR for all symmetric master keys in the sample set. The KDRs generated by its system should be fully equal to the KDRs in the sample set, provided they use the MSCA ephemeral key pair provided in the folder of each KDR / KDM (see section 3.3.2).
- An MSCA can verify that its system is capable of successfully processing the KDMs in the sample set. Processing a KDM should lead to the import of the relevant master key in (the HSM connected to) its system. Successful processing of a KDM is dependent on the use of the private MSCA ephemeral key provided in the folder of each KDR / KDM (see section 3.3.2).

Please note that this list is informative only.

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
[9]	Smart Tachograph - Cryptographic keys and digital certificates sample set, version 1.2, April 2017
[10]	ERCA Certificate Policy, version 1.0, MM 2018

List of abbreviations and definitions

AES	Advanced Encryption Standard
CSR	Certificate Signing Request
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman (key agreement protocol)
EGF	External GNSS Facility
ERCA	European Root Certificate Authority
GNSS	Global Navigation Satellite System
KDM	Key Distribution Message
KDR	Key Distribution Request
MA	Mutual Authentication
MS	Motion Sensor
MSCA	Member State Certificate Authority
PKI	Public Key Infrastructure
SHA-2	Secure Hash Algorithm 2
TC	Tachograph Card
VU	Vehicle Unit

Appendix 1 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]

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