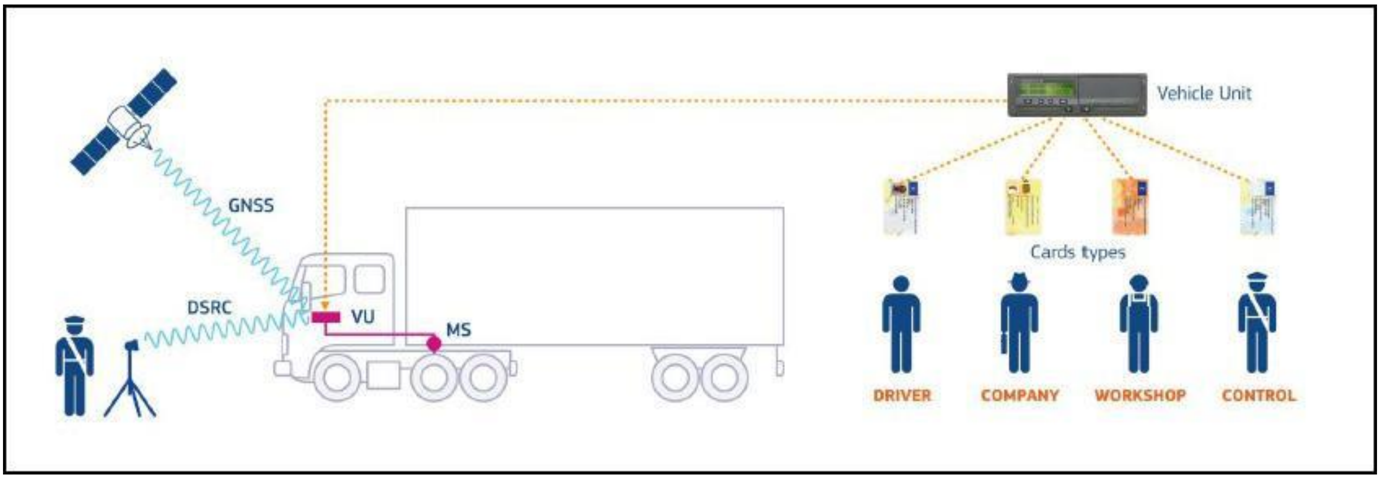
AUTOTRANSPORTA DIREKCIJA

Latvian

Smart Tachograph

Member State Authority Certificate Policy (LV-MSA-CP)



Version 1.1

March 25, 2019

Contents

1 Introduction

1.1 Overview

The second-generation Digital Tachograph system, called Smart Tachograph, has been introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council.

Annex IC of Commission Implementing Regulation (EU) 2016/799 lays down the technical requirements for the construction, testing, installation, operation and repair of Smart Tachographs and their components. Appendix 11 (Common Security Mechanisms) of Annex IC specifies the security mechanisms ensuring:

- Mutual authentication between different components of the tachograph system.

- Confidentiality, integrity, authenticity and/or non-repudiation of data transferred between different components of the tachograph system or downloaded to external storage media.

Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realize this for the second-generation tachograph system.

A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic system relies on master keys that must be delivered to the relevant actors. An infrastructure consisting of three layers has been set up. At the European level, the European Root Certification Authority (ERCA) is responsible for the generation and management of root public-private key pairs, with the respective certificates, and symmetric master keys. The ERCA issues certificates to Member State Certification Authorities (MSCAs) and distributes symmetric master keys to the MSCAs. The MSCAs are responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment.

This document forms the Certificate Policy (CP) for the PKI of the Latvian Certification Authority (LV-CA). It lays down the policy at MSCA level for key generation, key management and certificate signing for the Smart Tachograph system, based on the ERCA Certificate Policy. For the LV-CA to issue certificates and/or symmetric keys to component personalizers, they shall comply with requirements also laid down in this document.

This document follows the framework for CPs described in RFC 3647 [4].

How the LV-CA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the LV-CA Certification Practice Statement (CPS)for the Smart Tachograph system.

Digital Tachograph (first generation system) and Smart Tachograph (second generation system) are two different systems that must be run in parallel and independently. For this reason, separate MSA policies have to be maintained to avoid problems when in the future the time comes to discontinue the Digital Tachograph and its corresponding ERCA (Gen 1). For this reason, the “Latvian MSA Policy for the Digital Tachograph System” will stay in place in addition to this LV-MSA-CP.

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119[5].

1.2 Document Name and Identification

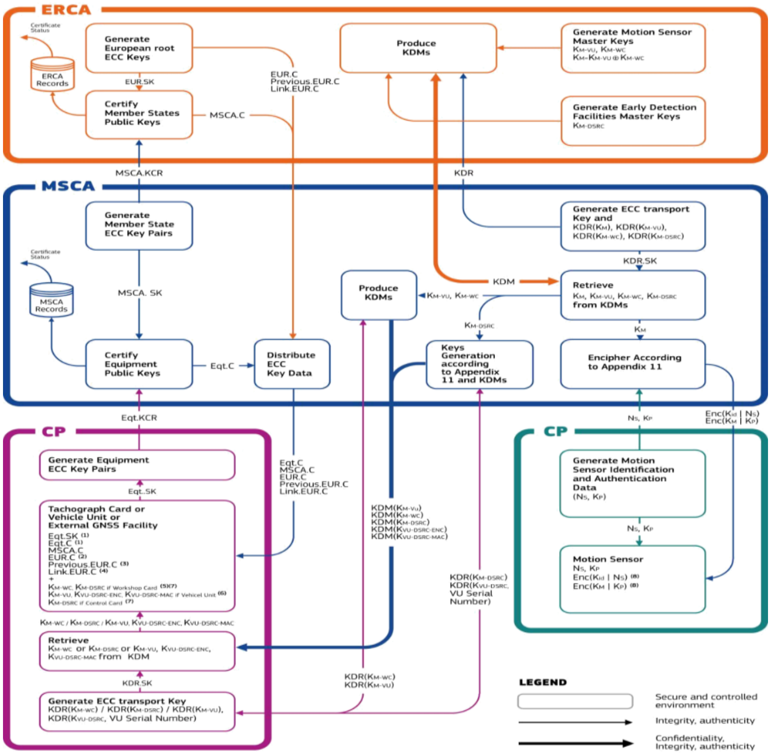
This document is named “Latvian Smart Tachograph Member State Authority Certificate Policy” (LV-MSA-CP). This Certificate Policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the certificates used in the Smart Tachograph system do not contain a reference to this policy. The current version can be found at the beginning and the end of this document.

Requirements regarding vehicle unit and motion sensor manufacturers are currently not covered by this policy. This policy must be respectively amended if the need arises.

Version 1.1 of this policy was endorsed by the ERCA (see section 1.5.1) on March 26, 2019.

1.3 PKI Participants

The participants in the Smart Tachograph PKI and in the Symmetric Key Infrastructure are described here and represented in Figure 1. Figure 1 also represents the exchanges between the participants, namely ERCA, MSCAs and component personalizers (CPs).


ERCA
Certificate Status
ERCA Records
Generate European root ECC Keys
EUR.SK
Certify Member States Public Keys
MSCA.C
EUR.C
Previous.EUR.C
Link.EUR.C
Produce KDMs
Generate Motion Sensor Master Keys
K_{M-VU}, K_{M-WC}
K_M=K_{M-VU} ⊕ K_{M-WC}
Generate Early Detection Facilities Master Keys
K_{M-DSRC}
MSCA.KCR
KDR
MSCA
Generate Member State ECC Key Pairs
Certificate Status
MSCA Records
MSCA. SK
Certify Equipment Public Keys
Eqt.C
Distribute ECC Key Data
Produce KDMs
K_{M-VU}, K_{M-WC}
Generate ECC transport Key and
KDR(K_M), KDR(K_{M-VU}),
KDR(K_{M-WC}), KDR(K_{M-DSRC})
KDR.SK
KDM
Retrieve
K_M, K_{M-VU}, K_{M-WC}, K_{M-DSRC}
from KDMs
K_{M-DSRC}
K_M
Keys Generation according to Appendix 11 and KDMs
Encipher According to Appendix 11
Eqt.KCR
N_S, K_P
Enc(K_{id} | N_S)
Enc(K_M | K_P)
CP
Generate Equipment ECC Key Pairs
Eqt..SK
Tachograph Card or Vehicle Unit or External GNSS Facility
Eqt.SK (1)
Eqt.C (1)
MSCA.C
EUR.C (2)
Previous.EUR.C (3)
Link.EUR.C (4)
+
K_{M-WC}, K_{M-DSRC} if Workshop Card (5)(7)
K_{M-VU}, $K_{VU-DSRC-ENC}$, $K_{VU-DSRC-MAC}$ if Vehicel Unit (6)
K_{M-DSRC} if Control Card (7)
K_{M-WC} / K_{M-DSRC} / K_{M-VU}, $K_{VU-DSRC-ENC}$, $K_{VU-DSRC-MAC}$
Retrieve
K_{M-WC} or K_{M-DSRC} or K_{M-VU}, $K_{VU-DSRC-ENC}$,
$K_{VU-DSRC-MAC}$ from KDM
KDR.SK
Generate ECC transport Key
KDR(K_{M-WC}) / KDR(K_{M-DSRC}) / KDR(K_{M-VU}),
KDR($K_{VU-DSRC}$, VU Serial Number)
Eqt.C
MSCA.C
EUR.C
Previous.EUR.C
Link.EUR.C
KDM(K_{M-Vu})
KDM(K_{M-WC})
KDM(K_{M-DSRC})
KDM($K_{VU-DSRC-ENC}$)
KDM($K_{VU-DSRC-MAC}$)
KDR(K_{M-DSRC})
KDR($K_{VU-DSRC}$,
VU Serial Number)
KDR(K_{M-WC})
KDR(K_{M-VU})
CP
Generate Motion Sensor Identification and Authentication Data
(N_S, K_P)
N_S, K_P
Motion Sensor
N_S, K_P
Enc(K_{id} | N_S) (8)
Enc(K_M | K_P) (8)
LEGEND
Secure and controlled environment
Integrity, authenticity
Confidentiality, Integrity, authenticity

NOTES
1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All K_{M-WC} keys associated to K_{M-VU} keys currently in circulation have to be inserted.
6. The K_{M-VU} key associated to the EUR certificate of note 2.
7. All K_{M-DSRC} keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Figure 1 Smart Tachograph PKI and Symmetric Key Infrastructure

For more information on the symmetric and asymmetric keys mentioned in this section, refer to Appendix 11 Part B.

1.3.1 Certification Authorities

1.3.1.1 European Root Certification Authority (ERCA)

The ERCA is the root Certification Authority (CA) that creates and assigns public key certificates in the PKI. It operates the following component services: Registration service, certificate generation service, dissemination service.

The ERCA generates PKI root key pairs and respective certificates, along with link certificates to create a chain of trust between different root certificates.

The ERCA is also the entity generating, managing and distributing on request the symmetric master keys, i.e. the Motion Sensor Master Key–VU part (K_{M-VU}), the Motion Sensor Master Key-Workshop Card part (K_{M-WC}) and the DSRC Master Key (K_{M-DSRC}).

1.3.1.2 Certification Authority of the Republic of Latvia (LV-CA)

The LV-CA operates as sub-CA under the ERCA. It creates and assigns public key certificates for equipment. For this, it operates a registration service, certificate generation service and dissemination service. The LV-CA receives the certificate requests from the LV-CP and disseminates the certificates to these parties. There are two types of LV-CA key pair(s) and corresponding LV-CA certificate(s) for the issuance of card certificates, called MSCA_Card key pair. The LV-CA may request both types of MSCA certificates from the ERCA, because of its responsibility regarding the issuance of card certificates. The LV-CA also requests symmetric master keys from the ERCA and distributes K_{M-WC} and K_{M-DSRC} to the LV-CP.

1.3.2 Registration Authorities

1.3.2.1 Card Issuing Authority for Tachograph Cards (LV-CIA)

CIA is responsible for:

- verifying whether all required documents were produced;
- verifying whether all prerequisites for the issuing of a tachograph card subject to the Regulation (EU) No 165/2014 of the European Parliament and of the Council, Annex IC of the Commission Implementing Regulation (EU) 2016/799, all other relevant legal provisions, the ERCA Policy and this LV-MSA-Policy are fulfilled;
- verifying the identity of a card applicant as well as whether a tachograph card was already issued to the applicant in another EU-member state;
- ensuring that the applications data is transmitted to the LV-CP properly according to the produced documents and to the requirements of this policy;
- informing all users about the requirements of this policy in an appropriate manner;
- ensuring that the PIN of the workshop card is handed over only to the intended bearer of the workshop card by using separate recipients for workshop card (workshop) and PIN (named technician);
- immediately informing the LV-MSA and the LV-CA or one of its authorized agencies about all security-relevant incidents.

1.3.2.2 LV-CA RA

The LV-CA ensures within its authority, that a proper registration of the LV-CP takes place before issuing of a certificate, distribution of symmetric keys or encrypting device data. The registration process is detailed in the CPS.

1.3.3 Subscribers

The only subscriber to the LV-CA public key certification service is the LV-CP. The LV-CP is responsible for the personalization of:

- Tachograph Cards: four different types of tachograph cards exist: driver cards, company cards, workshop cards and control cards.

This equipment contains cryptographic keys.

- The driver cards and workshop cards have two key pairs and corresponding certificates issued by an MSCA_Card, namely
  - a key pair and certificate for mutual authentication, called Card_MA;
  - a key pair and certificate for signing, called Card_Sign.

The workshop cards also contain K_{M-WC} and K_{M-DSRC} with key length of all possible VUs – with regard to the used cipher suites.

- The company and control cards have a key pair and corresponding certificate issued by an MSCA_Card for mutual authentication.

The control cards also contain K_{M-DSRC} with key length of all possible VUs – with regard to the used cipher suites.

The LV-CP is responsible for ensuring the card is provided with the appropriate keys and certificates.

1.3.3.4 Personalizer of Latvian Tachograph Cards (LV-CP)

- ensures generation of the two card key pairs, for mutual authentication and signing, for driver and workshop cards;
- performs the certificate application process with the LV-CA_Card for driver and workshop cards;
- performs the application for K_{M-WC} and K_{M-DSRC} (workshop cards only);
- ensures availability of keys and certificates in the card for mutual authentication and signing, MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only);
- ensures generation of the card key pairs for mutual authentication for company and control cards;
- performs the certificate application process with the LV-CA_Card for company and control cards;
- performs the application of K_{M-DSRC} (control cards only);
- ensures availability of keys and certificates in the card for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only).

1.3.4 Relying Parties

Parties relying on the LV-CA certification services are primarily the Latvian authorities tasked with enforcing the rules and regulations regarding driving times and rest periods, especially the State Police of Latvia.

The LV-CA certifications are used within the system to validate the authenticity of equipment certificates, which in turn are used to validate the authenticity of data downloaded from Vehicle Units and driver cards. Other directly relying parties are LV-CP, CIA's, drivers, companies and workshops.

1.4 Key and Certificate Usage

The LV-CA shall use its LV-CA private keys only for:

- Signing of equipment certificates, in accordance with Annex IC Appendix 11.
- Signing of certificate signing requests (see section 4.1.1)
- Issuing Certificate Revocation Lists, if such a method is used for providing certificate status in-formation.

The LV-CA shall use the symmetric master keys solely to derive VU-specific keys and encrypt motion-sensor related data as specified in Annex IC Appendix 11.

The LV-CA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to the LV-CP by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11.

The LV-CA_Card certificates shall be used to verify card certificates issued by the LV-CA_Card.

The Card_MA certificates shall be used for mutual authentication and session key agreement between Card and VU.

The Card_Sign certificates shall be used to verify the authenticity and integrity of data downloaded from the card. The Card_Sign private key may only be used to sign data downloaded from the card. All valid versions of K_M shall be used by the LV-CA to encrypt MoS pairing keys K_P, and to derive all valid versions of the MoS identification key K_{ID}. All valid versions of K_{ID} shall be used by the LV-CA to encrypt MoS serial numbers. K_{M-WC} shall be provided to the LV-CP for their installation Workshop Cards.

K_{M-DSRC} shall be used by the LV-CA to derive VU specific keys to secure the DSRC communication. K_{M-DSRC} shall be used by control and workshop cards to derive the VU specific DSRC keys required to decipher and verify the authenticity and integrity of the VU's DSRC communication.

1.5 Policy Administration

1.5.1 ERCA

The European Commission service responsible for implementation of the certification policy at the European level and for the provision of key certification and key distribution services to the Member States is referred to as the European Root Certification Authority (ERCA).

The contact address of the ERCA is:

Head of the Cyber and Digital Citizens’ Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

The ERCA reviews this LV-MSA certificate policy, for conformity with the requirements defined in the ERCA certificate policy. The objective of the review process is to assure comparable levels of security in each Member State. The ERCA archives the policy review reports and the MSA certificate policies for reference purposes.

The ERCA provides key certification services to the MSCAs affiliated to an MSA only if the outcome of the MSA certificate policy review provides sufficient grounds to judge that the requirements in the ERCA Certificate policy will be met. Continuation of key certification service from the ERCA to an MSCA de-pends on timely receipt of the MSA audit reports (see section 8.1) demonstrating that the MSCA is continuing to fulfil its obligations as laid down in the approved MSA Certificate Policy.

1.5.2 Latvian Member State Authority (LV-MSA)

The LV-MSAs responsibilities are:

- Laying down and documenting an MSA certificate policy in conformance with all applicable requirements in the ERCA certificate policy and taking care of its approval by the ERCA. The LV-MSA makes an English version of the LV-MSA certificate policy available to the ERCA and takes care for publishing of it.
- Approving the CPS of the LV-CA and stating its compliance with this CP. This can be accomplished in conjunction with the compliance audits of the LV-CA (see chapter 8).
- Ensuring or arranging that the LV-MSA-CP is made available to all authorities involved.
- Ensuring that the LV-CA has the resources required to operate in conformity with this certificate policy.

The contact address of the LV-MSA is:

Road Transport Administration
Vaļņu Street 30
Riga, LV-1050, Latvia
Phone: (371) 67280485
Fax: (371) 67821107
e-mail: info@atd.lv

1.5.3 LV-CA/LV-CP

The LV-MSA appoints ”Trüb Baltic” AS to operate as LV-CA as well LV-CP in order to implement the Latvian certification policy, to provide key certification, key distribution and card personalization services on behalf of Latvia.

The contact address of the LV-CA/LV-CP is:

Trüb Baltic AS
Laki 5, 10621
Tallinn
Estonia
www.trueb.ee

The LV-CA documents its implementation of the LV-MSA certificate policy in a Certification Practice Statement (LV-CA CPS). The LV-CA CPS is the LV-CAs procedural document, which details how the LV-MSA certificate policy is enforced in day-to-day management. The document is developed and owned by the LV-CA. It shall be treated as restricted information. The LV-CA shall make the contents of its CPS available on a need-to-know basis only. The LV-CA CPS shall be managed, reviewed, and modified following document control procedures.

The LV-CA makes its CPS available to the LV-MSA. The LV-MSA is responsible to determine whether the LV-CA CPS complies with the LV-MSA certificate policy. Upon request, the LV-CA also makes a version of its CPS available to the ERCA.

The LV-CA maintains records of its operations as appropriate to demonstrate conformity with the LV-MSA certificate policy and shall make these records available to the LV-MSA and/or the ERCA on demand. Complaints from LV-CP (if it represents another entity) about the services provided by the LV-A shall be addressed to the LV-MSA (contact address see 1.5.2).

1.6 Definitions and Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CP	Card/Component Personalizer
CP	Certificate Policy
CPS	Certification Practice Statement
LV-CA	Latvian Member State Certification Authority
LV-CIA	Latvian Card Issuing Authority
LV-CP	Latvian Card Personalizer
LV-MSA	Latvian Member State Authority
LV-MSA-CP	Latvian Member State Authority Certificate Policy
DSRC	Dedicated Short Range Communications
CSR	Certificate Signing Request
EC	Elliptic Curve
EC	European Commission
ECC	Elliptic Curve Cryptography

EGF	External GNSS Facility
EA	European Authority
ERCA	European Root Certification Authority
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISMS	Information Security Management System
ISSO	Information System Security Officer
JRC	Joint Research Centre
KDR	Key Distribution Request
K_{M}	Motion Sensor Master Key
K_{M-VU}	VU part of K_{M}
K_{M-WC}	WC part of K_{M}
K_{ID}	Motion Sensor Identification Key
K_{P}	Motion Sensor Pairing Key
K_{M-DSRC}	DSRC Master Key
LKM	Labeled Key Message
MA	Mutual Authentication
MoS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
NCP	Normalized Certificate Policy
PKI	Public Key Infrastructure
RFC	Request for Comment
RSA	Rivest, Shamir und Adleman
TC	Tachograph Card
VU	Vehicle Unit
WC	Workshop Card

Further definitions may be found in the documents referenced by this LV-MSA-CP certificate policy; see the section References towards the end of this document.

2. Publication and Repository Responsibilities

2.1 Repositories

- All equipment certificates issued by the LV-CA shall be maintained in the LV-CA database.

2.2 Publication of Certification Information

- The LV-MSA shall publish this Certification Policy on the website www.atd.lv
- The LV-CA Certification Practice Statement shall not be public but shall be communicated on request to the relevant parties.

2.3 Time or Frequency of Publication

- Information relating to changes in this policy shall be published according to the schedule defined by the change (amendment) procedures laid down in section 9.12 of this document.

2.4 Access Controls on Repositories

- All information available via the LV-MSA website shall have read-only access. The LV-CA shall designate staff having write or modify access to the information in the LV-CA CPS.
- All information published on the LV-MSA website shall be available via a secure Internet connection.

3 Identification and Authentication

This chapter describes how identification and authentication (I&A) shall take place for initial and re-key certificate requests and for symmetric key distribution requests between the LV-CA and the ERCA. I&A between the LV-CA and LV-CP is detailed in the LV-CA CPS.

3.1 Naming

3.1.1 Types of Names

3.1.1.1 Certificate Subject and Issuer

The Certification Authority Reference and Certificate Holder Reference identify the issuer and subject of a certificate. They shall be formed in the following way as described in Annex IC, Appendix 11, CSM_136/CSM_141and Appendix 1:

Entity:

- LV-CA

Identifier:

- Certification Authority Key Identifier (KID)

Construction:

- Nation numeric (‘20’ for Latvia)
- Nation alpha (’4c 56 20’, LV with to blanks, for Latvia)

- Key serial number
- Additional info
- CA identifier

Test key certificates, test certificate requests, test key distribution requests and test key distribution messages for the purpose of Interoperability Tests, shall contain the values '54 4B' ("TK") in the *additionalInfo* field.

3.1.1.2 Key Distribution Requests and Key Distribution Messages

Key Distribution Requests and Key Distribution Messages are identified by the key identifier of the ephemeral public key generated by each MSCA, see section 4.2.1. The key identifier value is determined according to section 3.1.1.1 with the following modifications:

- keySerialNumber: unique for each requesting entity
- additionalInfo: '4B 52' ("KR", for Key Request), unless it concerns a test KDR. In that case, '54 4B' ("TK", for Test Key) shall be used.

3.2 Initial Identity Validation

3.2.1 Method to prove Possession of Private Key

When submitting certificate signing requests (CSRs) to the ERCA, proof of possession of the corresponding private key via an internal signature, as specified in section 4.1.1, is necessary. The CSRs may also have an outer signature proving the authenticity of the message. The outer signature shall be produced by an already certified private key referenced in the CSR.

By verification (done manually together with the MSA/MSCA), if a hash calculated over the received CSR matches the hash over the CSR sent by the MSCA (as described in the ERCA CPS), additional prove of integrity, authenticity and initial trust is established.

3.2.2 Authentication of Organization Identity

The LV-CA shall define a procedure for the authentication of organization identities (e.g. equipment manufacturers) in its Certification Practice Statement.

3.2.3 Authentication of Individual Identity

The LV-CA shall define a procedure for the authentication of individual identities. The procedure is documented in the LV-CA's Certification Practice Statement.

3.2.4 Validation of Authority

The LV-CA shall define a procedure for the validation of authority in its Certification Practice Statement.

3.2.5 Criteria for Interoperation

The LV-CA shall not rely on any external certificate authority except the ERCA for the certificate signing and key distribution services it provides to the smart tachograph system.
If the LV-CA must rely on an external PKI for any other service or function, review and approval of the CP and/or CPS of the external certification service provider by the LV-MSA prior to applying for certification services, is required.

3.3 Identification and Authentication for Re-Key Requests

The Identification and Authentication procedures for re-key requests (see sections 4.1.8 and 4.2.9) shall be the same as those described in section 3.2.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests received by the ERCA from any source (see section 4.1.10) shall be validated by direct communication with the MSA responsible for the certificate-holding MSCA, through the contact point.
The LV-CA shall describe in its Certification Practice Statement how it will validate certification revocation requests for equipment certificates, if certificate revocation procedures are available.

4 Life-Cycle Operational Requirements for Certificates, symmetric Keys and Encryption Services

This chapter describes the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates, symmetric keys for cards and VUs and equipment data encryption services between the LV-CA and its LV-CP as well as for the application and distribution of MSCA certificates and symmetric master keys between the ERCA and the LV-CA.

4.1 LV-CA ERCA Public Key Certificate Application and Issuance

The following requirements are closely based on the respective chapter of the ERCA Gen. 2 certificate policy.

4.1.1 Certificate Signing Requests

Certificate signing requests can only be submitted by MSCAs recognized by their MSA via a compliance statement (see 1.5.2).

A CSR shall be in TLV-format. Table 1shows the CSR encoding, including all tags. For the lengths, the DER encoding rules specified in ISO/IEC 19790 shall be used. The values are specified in the remainder of this section.

Data Object	Req	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’
Standardized 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

m: mandatory
c: conditional

The **Authentication** data object shall only be present in case the Outer Signature data object is present.

The version of the profile is identified by the **Certificate Profile Identifier**. Version 1, specified in section 7.1, shall be identified by a value of ‘00’.

The **Certification Authority Reference** shall be used to inform the ERCA about the ERCA private key that the LV-CA expects to be used for signing the certificate. For Certification Authority Reference values see section 3.1. At any given time, the key identifier of the ERCA root key available for signing will be indicated on the ERCA website.

The **Certificate Holder Authorisation** shall be used to identify the type of certificate. It consists of the six most significant bytes of the Tachograph Application ID (‘FF 53 4D 52 44 54’), concatenated with the type of equipment for which the certificate is intended (Annex IC, Appendix 11, CSM_141). For MSCA certificates, the equipment type shall be set to ‘0E’ (14 decimal).

The **Public Key** nests two data objects:

- The **Domain Parameters** data object shall reference the standardized domain parameters to be used with the public key in the certificate. It shall contain one of the object identifiers specified in table 1 of Appendix 11, Annex IC.
- The **Public Point** data object shall contain the public point. Elliptic curve public points shall be converted to octet strings as specified in ISO/IEC 18033-2. The uncompressed encoding format shall be used (Annex IC, Appendix 11, CSM_143).

The **Certificate Holder Reference** is used to identify the public key contained in the request and in the resulting certificate. The Certificate Holder Reference shall be unique. It can be used to reference this public key in equipment-level certificates (Annex IC, Appendix 11, CSM_144). For Certificate Holder Reference values see section 3.1.

The **Certificate Effective Date** shall indicate the starting date and time of the validity period of the certificate. The **Certificate Expiration Date** shall indicate the end date and time of the validity period. Both data elements shall be of data type TimeReal, specified in Annex IC, Appendix 1. Note that the validity period defined by these two data elements shall be either 17 years and 3 months (for MSCA_VU-EGF certificates) or 7 years and 1 month (for MSCA_Card certificates).

The certificate body shall be self-signed via an **Inner Signature** that shall be verifiable with the public key contained in the certificate request. The signature shall be created over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116, using the hashing algorithm linked to the size of the public key in the CSR, as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

The **Certification Authority Reference of Outer Signature Signatory** shall indicate the MSCA and the respective key that placed the outer signature. It shall only be present in case an outer signature is present. For possible values, see section 3.1.

The **Outer Signature** shall be absent if the LV-CA applies for its initial certificate. The outer signature shall be required if the LV-CA applies for a successive certificate. In this case, the Certificate Signing Request shall be additionally signed via an outer signature by the LV-CA, using one of its current valid LV-CA private keys. The outer signature authenticates the request. Because the LV-CA is subscribed to receive both MSCA_Card and MSCA_VU-EGF certificates, the outer signature shall be placed using a private key linked to a certificate of the same type.
The Outer Signature shall be created over the encoded ECC (CV) Certificate (including the certificate's tag '7F 21' and its length) and the Certification Authority Reference of Outer Signature Signatory field (including the certificate's tag '42' and its length). The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116 using the hashing algorithm linked to the size of the LV-CA key used for signing, as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

The LV-CA shall calculate and store a hash over the complete CSR, using the hashing algorithm linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50. This hash will be used by the ERCA together with the MSA/MSCA to manually verify the authenticity of the CSR, see section 4.1.2.1.

4.1.2 Certificate Application Processing

4.1.2.1 Verification of CSR contents

The ERCA ensures that a CSR originating from any MSCA is complete, accurate, and duly authorized. The ERCA only signs an MSCA certificate if this is the case.

Checks for correctness, completeness and authorization are performed manually by the ERCA officers and/or in an automated way by the ERCA registration service. If the request is correct and complete, the ERCA officers authorize the signing of an MSCA certificate. For each CSR it receives, the ERCA verifies that

- the transport media is readable; i.e. not damaged or corrupted;
- the CSR format complies with Table 2;
- the request is duly authorized. If an outer signature is in place, the ERCA verifies the correctness of this signature. In any case, the ERCA contacts the MSCA as described in the ERCA CPS and verifies that a hash calculated over the received CSR matches the hash over the CSR sent by the MSCA;
- the MSCA is entitled to receive the requested type of certificate;
- the Certification Authority Reference contained in the request indicates the ERCA root private key currently valid for signing MSCA certificates;
- the Certificate Holder Reference is unique. For MSCAs the Certificate Holder Reference is a Certification Authority Key Identifier (KID). The Key Serial Number in this KID shall differ between keys of the same MSCA, making the KID unique;

- the domain parameters specified in the request are listed in Table 1 of Annex IC, Appendix 11, and the strength of these parameters matches the strength of the ERCA root key indicated in the Certification Authority Reference;
- the public point in the request has not been certified by the ERCA previously and has not been used as an ephemeral key for symmetric key distribution previously (see section 4.2.3), even for interoperability test purposes;
- the public point in the request is on the curve indicated in the request;
- the inner signature can be verified using the public point and the domain parameters indicated in the request. This proves that the MSCA is in possession of the private key associated with the public key;
- the outer signature is present if the request is not for the initial MSCA_VU-EGF or MSCA_Card certificate of the MSCA;
- If present, the outer signature can be verified using the public point and the domain parameters in the MSCA certificate referenced in the Certification Authority Reference of Outer Signature Signatory field. Moreover, the private key usage period of this key has not expired yet.

If any of these checks fails, the ERCA rejects the CSR. The ERCA communicates the rationale for any request rejection to the MSCA and the responsible MSA.

4.1.2.2 Certificate generation, distribution and administration

If all checks succeed, the ERCA proceeds to sign the certificate as described in section 4.1.3.

The following information is recorded in the ERCA database for each certificate signing request received:

- the complete CSR originating from the MSCA;
- the complete resulting public key certificate, if any;
- the standardized domain parameters OID and the public point of the certified public key;
- the certificate effective data and certificate expiration date;
- the Certificate Holder Reference (for identification of the public key);
- the hash over the binary certificate data, if any. The hash length shall be linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50;
- the hash over the binary CSR data, see section 4.1.1;
- the certificate status “Valid” if the certificate is issued or “Rejected” in case the CSR is rejected;
- a timestamp.

The MSCA certificate(s) are written to transport media in accordance with the requirements in section 4.1.4, for return to the MSCA. Every certificate copy written on transport media is verified afterwards using the ERCA public key. The ERCA also writes a copy of the ERCA public key certificate that can be used to verify the MSCA certificate(s) to the transport media.

After successful distribution of a new MSCA certificate, the ERCA updates the certificate status information in the ERCA repository. No other notification action is performed.

The ERCA retains the transport media with the CSR and archives it in their controlled premises.

The ERCA aims to complete public key certification operations within one working day. The time required for the ERCA to supply a MSCA public key certificate or distribute a symmetric key shall be determined solely by the time required for correct execution of the ERCA procedures. A turnaround time of one month is guaranteed. When requesting a certificate, MSCAs shall take into account this maximum turnaround time.

4.1.3 Certificates

The format of the MSCA public key certificates can be found in section 7.1.

The ERCA creates the signature over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in ISO/IEC 10116, using the hashing algorithm linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

4.1.4 Exchange of Requests and Responses

For transportation of certificate signing requests and certificates, CD-R media should be used:

- The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA accepts and dispatches CSRs and certificates as e-mail attachments.

The LV-CA shall write three copies of each certificate signing request to the transport medium for transport to the ERCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.
The ERCA writes three copies of each certificate to the transport medium for return to the LV-CA. These copies are in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.
Each certificate signing request and certificate shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS. Another paper copy of the data shall be held by the ERCA or the LV-CA, respectively.
For both CSRs and certificates, the transport media and the printouts are handed over between an ERCA employee and the LV-CAs courier in the ERCA controlled area.

4.1.5 Certificate Acceptance

The courier signs for receipt of the LV-CA certificate at the ERCA premises.
Upon reception of the certificate at the LV-CA premises, the LV-CA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the certificate complies with Table 5 in section 7.1;
- all certificate field values match the values requested in the CSR;
- the certificate signature can be verified using the ERCA public root key indicated in the CAR field.

If any of these checks fail, the LV-CA shall abort the process and contact the ERCA. Certificate rejection is managed according to the certificate revocation procedure (see section 4.1.10).

4.1.6 Key Pair and Certificate Usage

The LV-CA shall use any key pair and the corresponding certificate in accordance to section 6.2.

4.1.7 Certificate Renewal

Certificate renewal, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.1.8 Certificate Re-key

Certificate re-key means the signing of a new LV-CA certificate, in replacement of an existing certificate.
Certificate re-key shall take place either:

- When the LV-CA is nearing the end of the usage period of (one of) its private key(s). In this case, re-key shall be done in a timely manner to ensure that the LV-CA can continue operations after the end of this period;
- Following certificate revocation.

Certificate application, processing, issuance, acceptance and publication are the same as for the initial key pair. The LV-CA shall immediately distribute the necessary keys and certificates to the LV-CP as further described in the LV-CA CPS.

The MSCA key pair(s) may be changed regularly. The ERCA shall not impose any limits on the number of MSCA certificates that it will sign. MSCAs shall be allowed to request multiple MSCA certificates of the same type, if justified for its activity, with overlapping validity periods.

4.1.9 Certificate Modification

Certificate modification is not allowed.

4.1.10 Certificate Revocation and Suspension

4.1.10.1 Circumstances for certificate revocation

LV-CA certificates shall be revoked in the following circumstances:

- rejection on receipt of a newly issued certificate (see section 4.1.5);
- compromise or suspected compromise of a LV-CA private key;
- loss of a LV-CA private key;
- LV-CA termination;
- LV-MSA or LV-CA failure to meet obligations under the Regulation and the ERCA certificate policy.

4.1.10.2 Who can request revocation

The ERCA considers revocation requests originating from the following entities as authoritative:

- the European Authority;
- all MSAs;
- all recognized MSCAs;

The European Authority is authorized to request revocation of any MSCA certificate.

An MSA is authorized to request revocation for certificates issued to the MSCAs listed in its MSA certificate policy.

An MSCA is authorized to request revocation for certificates issued to itself.

The ERCA shall reject revocation requests originating from any other entity.

4.1.10.3 Procedure for revocation request

The certificate revocation procedure is described in the LV-CA CPS.

4.1.10.4 Revocation request grace period

The grace period for certificate revocation is five working days from the start of the circumstances for revocation, within which a subscriber shall make a revocation request.

4.1.10.5 Time within which ERCA shall process the revocation request

The ERCA processes correct, complete and authorized revocation requests within three working days of receipt.

4.1.10.6 Revocation checking requirements for relying parties

Relying parties shall be responsible for checking the certificate status information published in the ERCA repository.

4.1.10.7 Certificate status issuance frequency

The status of ERCA and MSCA public key certificates are retrievable online from https://dtc.jrc.ec.europa.eu/. The ERCA maintains the integrity of the certificate revocation status information.
Certificate status information published in the ERCA repository shall be updated on the first working day of each week.

4.1.10.8 Maximum latency for CRLs

Not applicable.

4.1.10.9 On-line revocation / status checking availability

The revocation / status information published in the ERCA repository is only guaranteed to be available during normal working hours.

4.1.10.10 On-line revocation / status checking requirements

No stipulation.

4.1.10.11 Other forms of revocation advertisements available

None.

4.1.10.12 Special requirements concerning key compromise

Key compromise is a security incident that shall be processed.

If the LV-CA keys (MSCA_Card.SK) is compromised or suspected to be compromised, the LV-CA shall report the incident to the ERCA and to the LV-MSA.

The follow-up investigation is led by the LV-MSA and all potential actions shall be taken by the LV-MSA to reduce the risk of misuse of a compromised key and the outcome shall be reported to ERCA.

4.1.10.13 Certificate suspension

Certificate suspension is not allowed.

4.1.11 Certificate Status Service

The availability of the website mentioned in section 4.1.10.7 is guaranteed during normal working hours. A list of MSCA certificate status information is also downloadable from this website in a common file format (e.g. .csv, Excel).

4.1.12 End of Subscription

Subscription for the ERCA's certificate signing services ends when the LV-MSA decides for LV-CA termination. Such a change is notified to the ERCA by the LV-MSA as a change to the LV-MSA certificate policy. In the case of subscription ending, the decision to submit a certificate revocation request for any valid LV-CA certificates, or to allow all LV-CA certificates to expire, is in the responsibility of the LV-MSA.

4.1.13 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that LV-CA root private keys will never be exported to or stored in any system apart from the LV-CA production and fallback systems.

4.2 Symmetric Master Key Application and Distribution between the ERCA and the LV-CA

The following requirements are closely based on the respective chapter of the ERCA Gen. 2 certificate policy.

4.2.1 Key Distribution Requests

Key distribution requests can only be submitted by MSCAs recognized by their MSA via a compliance statement (see 1.5.2).

A KDR shall be in TLV-format. Table 2 shows the KDR encoding, including all tags. For the length, the DER encoding rules specified in ISO/IEC 19790 shall be used. The values are specified in the remainder of this section.

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

Table 2 Key distribution request format

The version of the profile is identified by the **Request Profile Identifier**. Version 1, specified in Table 2, shall be identified by a value of '00'.

The **Message Recipient Authorisation** shall be used to identify the symmetric key that is requested. It consists of the concatenation of

- the six most significant bytes of the Tachograph Application ID (‘FF 53 4D 52 44 54’),
- the type of key that is requested (see below, 1 byte),
- the version number of the requested master key (1 byte).

The following values shall be used to indicate the type of key requested:

- ‘07’: K_{M}, motion sensor master key
- ‘27’: $K_{M\text{-}WC}$, motion sensor master key workshop part
- ‘67’: $K_{M\text{-}VU}$, motion sensor master key VU part
- ‘09’: $K_{M\text{-}DSRC}$, DSRC master key

The **Key Identifier** is a unique 8-byte octet string identifying the public key presented in the KDR for ECDH key exchange, see section 4.2.3. Its value is determined according to section 3.1.1.2. Since a MSCA shall use a different ephemeral key pair for every key distribution request, the LV-CA may use the key identifier to keep track of the ephemeral private key to be used for the decryption of a particular key distribution message, once it arrives at the LV-CA. For that reason, the ERCA copies the key identifier in the key distribution message, see Table 3

The **Public Key** nests two data elements:

- The data element Public Point shall contain the public point of the ephemeral LV-CA key pair to be used for key agreement. The LV-CA shall convert the public point to an octet string as specified in ISO/IEC 18033-2, using the uncompressed encoding format.
- The data element Domain Parameters shall contain the object identifier of the set of standardized domain parameters to be used in conjunction with the public point. For more information, see section 4.2.3.

The LV-CA shall calculate and store a hash over the complete KDR, using the hashing algorithm linked to the key size of the requested master key, as specified in Annex IC, Appendix 11, CSM_50. This hash will be used by the ERCA to verify the authenticity of the KDR, see section 4.2.2.1.

4.2.2 Master Key Application Processing

4.2.2.1 Verification of KDR contents

The ERCA ensures that a KDR originating from an MSCA is complete, accurate, and duly authorized. The ERCA only creates a key distribution messages if this is the case.

Checks for correctness, completeness and authorization are performed manually by the ERCA officers and/or in an automated way by the ERCA registration service. If the request is correct and complete the ERCA officers may authorize the generation of a key distribution message by the key distribution service. For each KDR it receives, the ERCA verifies that

- the transport media is readable; i.e. not damaged or corrupted;
- the KDR format complies with Table 2
- the request is duly authorized. The ERCA contacts the MSCA as described in the ERCA CPS and verifies that a hash calculated over the received KDR matches the hash over the KDR stored by the MSCA (see the end of section 4.2.1);
- the MSCA is entitled to receive the requested type of master keys:
  - MSCAs responsible for issuing tachograph cards shall be entitled to receive all valid versions of $K_{M\text{-}WC}$ with regard to used cipher suite and the DSRC master key $K_{M\text{-}DSRC}$;

- MSCAs responsible for issuing VUs shall be entitled to receive $K_{M\text{-}VU}$ and the DSRC master key $K_{M\text{-}DSRC}$;
- MSCAs responsible for issuing motion sensors shall be entitled to receive all valid versions of K_M with regard to used cipher suite;

Note that in case an MSCA has received both $K_{M\text{-}WC}$ and $K_{M\text{-}VU}$ of a valid cipher suite, it could generate the corresponding K_M by itself. However, MSCAs shall not do this, even if they need K_M for issuing motion sensors. An MSCA needing K_M shall request the ERCA to distribute this key.

- the requested master key type and version has not been requested by this MSCA before. If this is the case the ERCA investigates the reason why a request for redistribution is done;
- the MSCA ephemeral public key in the request has not been certified by the ERCA or used for key distribution previously, even for interoperability test purposes;
- the domain parameters specified in the request are listed in Table 1 of Annex IC, Appendix 11, and the strength of these parameters matches the length of the requested symmetric key (see section 4.2.3 step 2);
- the public point specified in the request is on the curve specified in the request.

If any of these checks fail, the ERCA rejects the KDR. The ERCA communicates the rationale for any request rejection to the MSCA and the MSA.

4.2.2.2 KDM generation, distribution and administration

If all checks succeed, the ERCA proceeds to prepare the key distribution message by determining the symmetric key requested by the MSCA and following the steps as described in section 4.2.3 (from step 2). The following information is recorded in the ERCA database for each key distribution request received:

- the complete KDR originating from the MSCA;
- the complete resulting key distribution message, if any;
- the standardized domain parameters OID, the ephemeral public point and the key identifier;
- the key type and version of the master key;
- the hash over the binary key distribution message data, if any. The hash length shall be linked to the key size of the signing authority, as specified in Annex IC, Appendix 11, CSM_50;
- the hash over the binary KDR data, see section 4.2.1;
- the status “Distributed” in case the key is distributed to the MSCA or “Rejected” in case the KDR is rejected;
- a timestamp.

The ERCA retains the transport media with the KDR and archives it in their controlled premises. Once the key distribution message has been generated, the ERCA sends it to the MSCA as specified in section 4.2.5.

The ERCA aims to complete key distribution operations within one working day. Turnaround time of one month is guaranteed. When requesting distribution of a key, MSCAs shall take into account this maximum turnaround time.

4.2.3 Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys distributed by the ERCA to MSCAs is protected via an Elliptic Curve Integrated Encryption Scheme (ECIES). This scheme allows for agreement between the ERCA and MSCA on encryption keys and MAC keys to be used to protect the master symmetric keys during distribution. The ECIES has been standardized in ISO/IEC 18033-2. The ECIES variant to be used for ERCA symmetric key distributions uses the following cryptographic algorithms, in accordance with Appendix 11 of Annex IC:

- Key derivation function: KDF2, as specified in ISO/IEC 18033-2;
- Message authentication code algorithm: AES algorithm in CMAC mode, as specified in NIST, Special Publication 800-38B;
- Symmetric encryption algorithm: AES in the Cipher Block Chaining (CBC) mode of operation, as defined in ISO/IEC 10116.

On a high level, the ECIES consists of the following steps. More details are given for each step below:

1. The MSCA generates a unique ephemeral ECC key pair for Diffie-Hellman key agreement and sends the public key to the ERCA in the Key Distribution Request, see Table 2
2. The ERCA similarly generates a unique ephemeral ECDH key pair and uses the Diffie-Hellman key agreement algorithm together with its own private key and the MSCA's ephemeral public key to derive a shared secret.
3. Using the key derivation function, the shared secret and additional information detailed below, the ERCA derives an encryption key and a MAC key.
4. The ERCA uses the encryption key to encrypt the symmetric key to be distributed.
5. The ERCA uses the MAC key to calculate a MAC over the encrypted key.

Step 1
For the generation of its ephemeral public key used for Diffie-Hellman key agreement, the MSCA shall choose one of the standardized domain parameters from Table 1 of Annex IC, Appendix 11. The strength of the chosen set of domain parameters shall match the length of the requested symmetric key, according to CSM_50 in Appendix 11. Ephemeral key pair generation shall take place in an HSM complying with the requirements in section 6.2. The ephemeral private key shall never leave the HSM. After generating the ephemeral key pair, the MSCA shall convert the public point to an octet string as specified in ISO/IEC 18033-2. The uncompressed encoding format shall be used. The MSCA shall include the OID of the chosen standardized domain parameters and the octet string representing the public point in the KDR, which is sent to the ERCA.

Step 2
The ERCA generates an ephemeral key pair, using the standardized domain parameters specified in the received KDR. The ERCA shall use the ECKA-DH algorithm as defined in ISO/IEC 18033-2 together with its own ephemeral private key and the MSCA's ephemeral public key to derive a shared point (K_x, K_y). The ERCA shall check that this point is not the infinity point. If it is, the ERCA shall generate a new ephemeral key pair and try again. Otherwise, the ERCA shall form the shared secret K by converting K_x to an octet string as specified in ISO/IEC 18033-2. Ephemeral key pair generation shall take place in an HSM complying with the requirements in section 6.2. The ephemeral private key shall never leave the HSM.

Step 3
For deriving the encryption key K_{ENC} and the MAC-ing key K_{MAC}, the ERCA uses the key derivation function KDF2(x, l) defined in ISO/IEC 18033-2. The octet string x shall be equal to the shared

secret K from the previous step. The hash function that is necessary to instantiate the KDF2 function shall be linked to the length of the symmetric key to be distributed, as described in Appendix 11 CSM_50. The output length l shall be equal to the output length of this hash function.

Given the output O of this key derivation function, the encryption and MAC-ing keys shall be formed as

- K_{ENC} = first L octets of O
- K_{MAC} = last L octets of O

where L is the required length of K_{ENC} and K_{MAC} in octets, in accordance to Appendix 11 CSM_50.

Step 4

If necessary (i.e. for a 192-bytes key), the ERCA pads the symmetric key to be distributed using padding method 2 defined in ISO/IEC 9797-1. Subsequently, the ERCA encrypts the padded key with AES in the Cipher Block Chaining (CBC) mode of operation, as defined in ISO/IEC 10116, using K_{ENC} with an inter-leave parameter m = 1 and an initialization vector SV consisting of binary zeros:

Encrypted symmetric key = AES-CBC (symmetric key + padding if necessary, K_{ENC})

Step 5

The ERCA concatenates the encrypted symmetric key with a string S, which is the concatenation of the values of the Message Recipient Authorization and the Key Identifier used in the key distribution message (see section 4.2.4)

S = Message Recipient Authorization || Key Identifier

Using K_{MAC}, the ERCA then computes a MAC over the concatenation of the Encrypted symmetric key and S, using the AES algorithm in CMAC mode, as specified in NIST Special Publication 800-38B. The length of the MAC shall be linked to the length of the AES session keys, as specified in Appendix 11 CSM_50.

MAC = AES-CMAC (Encrypted symmetric key || S, K_{MAC})

Any operations with the ephemeral private key, with the shared secret and with the derived keys K_{ENC} and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2.

The ERCA shall record the value of S and of the MAC. As described in section 4.2.6, the MSCAs will use these values to verify the authenticity of the key distribution message.

4.2.4 Key Distribution Messages

After performing the Master Key application processing (see section 4.2.2), the ERCA shall construct a key distribution message as shown in Table 3 For the lengths, the DER encoding rules specified in (ISO/IEC 8825-1 shall be used. The values are specified in the remainder of this section.

Data Object	**Req**	**Tag**
Key Distribution	m	‘A1’
Request Profile Identifier	m	‘5F 29’
Message Recipient Authorization	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 version of the profile is identified by the **Request Profile Identifier**. Version 1 specified in Table 3 shall be identified by a value of ‘00’.

The **Message Recipient Authorisation** shall be identical to the Message Recipient Authorisation data element in the KDR from the MSCA, see section 4.2.1.

The **Public Point** shall contain the public point of the ephemeral ERCA key pair used for key agreement, see section 4.2.3. The ERCA converts the public point to an octet string as specified in BSI Technical Guideline TR-03111 using the uncompressed encoding format.

The **Encrypted symmetric key** data element shall contain the output of step 4 in section 4.2.3.

The **MAC** data element shall contain the output of step 5 in section 4.2.3.

After successful generation of the key distribution message, the ERCA securely destroys its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.
The key distribution message is returned to the MSCA that issued the KDR.

4.2.5 Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages, CD-R should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).
Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA accepts and dispatches key distribution requests and key distribution messages as e-mail attachments.
The MSCA shall write three copies of each key distribution request to the transport medium for transport to the ERCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

The ERCA writes three copies of each key distribution message to the transport medium for return to the MSCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.

Each KDR and KDM shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS. Another paper copy of the data shall be held by the ERCA or the MSCA, respectively.
For both KDRs and KDMs, the transport media and the printouts shall be handed over between an ERCA employee and the MSCA courier in the JRC controlled area.

4.2.6 Master Key Acceptance

The courier signs for receipt of the key distribution message at the ERCA premises. Upon reception of the key distribution message at the MSCA premises, the MSCA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with Table 3
- the message is genuine. The MSCA shall do this by contacting the ERCA as described in the ERCA CPS and verifying that the MAC in the received KDM matches the MAC in the KDM sent by the ERCA;
- the master key type and version in the message matches the requested type and version;
- the public point specified in the message is on the curve specified by the key distribution request sent by the MSCA to the ERCA.

If any of these checks fail, the MSCA shall abort the process and contact the ERCA.

If all of these checks succeed, the MSCA shall

- use the ECKA-DH algorithm to derive a shared point (K_x, K_y), as described in step 3 in section
  4.2.3, using the MSCA's ephemeral private key indicated by the key identifier in the message and the ERCA's ephemeral public key. The MSCA shall verify that the shared point is not the infinity point; if it is, the MSCA shall abort the process and contact the ERCA. Else, the MSCA shall form the shared secret K by converting K_x to an octet string as specified in BSI Technical Guideline TR-03111;
- derive the keys K_{ENC} and K_{MAC} as described in step 4 in section 4.2.3;
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3. If this verification fails, the MSCA shall abort the process and contact the ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3. The MSCA shall verify that the padding of the decrypted key, if any, is correct. If this verification fails, the MSCA shall abort the process and contact the ERCA.

Any operations with the ephemeral private key, with the shared secret and with the derived keys K_{ENC} and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2. After successful recovery of the master key, or when the key distribution process is aborted and no KDM renewal (see section 4.2.8) is initiated, the MSCA shall securely destroy its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

4.2.7 Master Key Usage

The MSCA shall use any received master key in accordance to section 6.2.

4.2.8 KDM Renewal

KDM renewal means the issuance of a copy of an existing KDM to an MSCA without changing the ephemeral public key or any other information in the KDM.

KDM renewal may take place only if the original transport media received at the MSCA is damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the MSA and the ERCA. Subsequent to this report, the MSCA may send a KDM renewal request to the ERCA, referring to the original key distribution request. This procedure is described in the ERCA CPS.
The ERCA shall only accept KDM renewal request endorsed by the MSA which approved the MSCA. Note: In case the MSCA needs to send a request to re-distribute a master key that was already successfully distributed to the MSCA, it shall generate a new key distribution request, using a newly

generated ephemeral key pair. Such a request may lead the ERCA to initiate an investigation of the possibility of key compromise.

4.2.9 Master Key Re-key

In case the ERCA has generated a new version of a master key, as specified in Appendix 11 sections 9.2.1.2 and 9.2.2.2, the availability of a new key is published on the ERCA website, together with its version number and length.

To receive the new version, the LV-CA shall submit a new KDR. Requesting a new master key shall take place in a timely manner so that the key (or derived keys or encrypted data for motion sensors) can be placed in time in newly issued components.

Key application, processing, distribution and acceptance are the same as for the initial key. The LV-CP shall be informed immediately as further described in the LV-CA CPS.

4.2.10 Symmetric Key Compromise Notification

If an MSCA detects or is notified of the compromise or suspected compromise of a symmetric master key, the MSCA shall notify this to the ERCA and the MSA without unnecessary delay and at least within 8 hours of detection. In their notification, the MSCA shall indicate the circumstances under which the compromise occurred. Any follow-up investigation and potential action by the MSA and/or MSCA shall be performed as indicated in the MSA certificate policy. The outcome of the MSA investigation shall be reported to the ERCA.

If the ERCA detects or is notified of the compromise or suspected compromise of a symmetric master key, the ERCA shall notify the European Authority without unnecessary delay and at least within 8 hours of detection. The European Authority shall act accordingly. The ERCA shall handle the incident according to a defined security incident handling procedure.

4.2.11 Master Key Status Service

The status of symmetric master keys shall be retrievable online from https://dtc.jrc.ec.europa.eu/. The ERCA shall maintain the integrity of the status information.

Master key status information published in the ERCA repository shall be updated on the first working day of each week.
The availability of the website mentioned above shall be guaranteed during normal working hours.

4.2.12 End of Subscription

Subscription for the ERCA’s key distribution services ends when an MSA decides for MSCA termination.

Such a change is notified to the ERCA by the MSA as a change to the national policy.

In the case of subscription ending, the MSCA shall securely destroy all copies of any symmetric master key in its possession.

4.2.13 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that symmetric master keys shall not be exported to or stored in any system apart from the ERCA and MSCA production and fallback systems.

4.3 Tachograph Card Certificate Application and Issuance

More details on application and issuance of Tachograph card certificates are provided in the LV-CA documentation. These details will be provided to a registered LV-CP.

4.3.1 Certificate Application

The LV-CA only issues certificates if a proper certificate application is presented to the responsible authority and if all the requirements of regulation (EC) 165/2014 and of all other associated legal provisions and agreements have been adhered to at the time of applying.

For each tachograph card one unique ECC key pair, designated as Card_MA and used for mutual authentication, shall be generated. A second unique ECC key pair, designated as Card_Sign (used for signing of data), shall additionally be generated for each driver card and each workshop card. This task may be handled by the LV-CP, as described in Annex IC Appendix 11 (section 9.1.5). Whenever a card key pair is generated, the party generating the key shall send the public key to the LV-CA in order to obtain a corresponding card certificate signed by the LV-CA. The private key shall be used only by the tachograph card. Key certification requests that rely on transportation of private keys are not al-lowed.

4.3.2 Certificate Requests

Certificate requests are collected inside a request package. The packages are signed using the private key of a dedicated RA chip card as described in the LV-CA CPS.

Data Object	Length	Format	Data
certificateRequestID	8 Byte	CertificateRequestID	Request ID
cardNumber	16 Byte	CardNumber	Card number
equipmentType	1 Byte	INTEGER	Equipment type: - Driver card: ‘0x01‘ - Workshop card: ‘0x02‘ - Control card: ‘0x03‘ - Company cards: ‘0x04‘ - Driver card signature: ‘0x11‘ - Workshop Card Signature: ‘0x12‘
tachographApplicationID	6 Byte	OCTET STRING	Hard coded value: ‘FF 53 4D 52 44 54‘ („SMRDT“)
PK_DP	var	Object Identifier	Domain Parameter; references the standardized domain parameters to be used with the public key in the certificate. It shall contain one of the object identifiers specified in table 1 of Appendix 11, Annex IC

PK_PP	var	OCTET STRING	Public Point; Elliptic curve public points shall be converted to octet strings as specified in (BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, V.2.0). The uncompressed encoding format shall be used (Annex IC, Appendix11, CSM_143)
signature	var	OCTET STRING	ECC Certificate Request Signature; ECDSA Signature created over the certificate request data in plain format

Table 4 Tachograph Card Certificate Request Data .

The **signature** is created over all data objects (in the specified order) except “cardNumber”. The signature algorithm shall be ECDSA, as specified in FIPS PUB 186-4, using the hashing algorithm linked to the key size of the signing authority. The signature format shall be plain, as specified in BSI Technical Guideline TR-03111.

4.3.3 Certificate Issuance

The LV-CA shall ensure within its authority, that a proper registration with the responsible authorities takes place before issuing of a certificate to the LV-CP.

If key generation takes place outside the LV-CA, the LV-CA shall only issue a certificate to the LV-CP if proof is made by a pre-agreed procedure that they are in possession of the corresponding private key. At this time the private key should not leave the secured environment of key generation.

The LV-CA shall also ensure that a certificate request package originating from the LV-CP is complete, accurate, and duly authorized. The LV-CA shall only issue or sign a card certificate if this is the case.
Checks for correctness, completeness and authorization shall only be performed in an automated way by the LV-CA system as described in the LV-CA CPS. The key component for authorization hereby is the RA chip card.

According to Appendix 11 the validity period of a Card_MA certificate shall be as follows:

- For driver cards: 5 years
- For company cards: 5 years
- For control cards: 2 years
- For workshop cards: 1 year

The validity period of a Card_Sign certificate shall be as follows:

- For driver cards: 5 years and 1 month
- For workshop cards: 1 year and 1 month

The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate. It shall be the date of issuance of the certificate by the LV-CA.

The Card_MA and Card_Sign certificates of a given driver card or workshop card shall have the same Certificate Effective Date.

Usage time of Card_MA.SK and Card_Sign.SK shall be the same as the validity period of the corresponding certificate.

The format of the Card_MA and Card_Sign certificates can be found in section 7.2.

4.3.4 Certificate Acceptance

The LV-CP shall only accept the certificate if it matches the associated certificate request and if the certificate can be validated against the LV-CA's MSCA_Card certificate containing the MSCA_Card.PK.

4.3.5 Key Pair and Certificate Usage

- The LV-CP shall choose the strength of a card key pair equal to the strength of the MSCA key pair used to sign the corresponding card certificate.
- A tachograph card shall use its Card_MA key pair, consisting of private key Card_MA.SK and public key Card_MA.PK, exclusively to perform mutual authentication and session key agreement towards vehicle units, as specified in Annex IC, Appendix 11.
- A driver card or workshop card shall use the private key Card_Sign.SK of its Card_Sign key pair exclusively to sign downloaded data files, as specified in Appendix 11. The corresponding public key Card_Sign.PK shall be used exclusively to verify signatures created by the card.
- Key pairs, symmetric keys and pin numbers shall be generated and maintained in a trustworthy dedicated device which:
  - is certified to EAL 4 or higher in accordance with ISO/IEC 15408 using a suitable Protection Profile; or
  - meets the requirements identified in ISO/IEC 19790 level 3; or
  - meets the requirements identified in FIPS PUB 140-2 level 3.

The most common implementation of such a trustworthy dedicated device for use in a PKI system is a Hardware Security Module (HSM).

- Private key operations and symmetric key operations shall take place internally in the HSM where the keys used are stored.
- The private keys and symmetric keys shall only be used within a physically secure environment by personnel in trusted roles under at least dual control. Private keys and symmetric keys shall not be processed outside the HSM without adequate encryption. All events of private key usage and symmetric key usage shall be logged.
- The key pairs and corresponding certificates of a given tachograph card shall not be replaced or renewed once the card has been issued.
- When issued, tachograph cards shall contain the following cryptographic keys and certificates:
  - The Card_MA private key and corresponding certificate
  - For driver cards and workshop cards additionally: The Card_Sign private key and corresponding certificate
  - The MSCA_Card certificate containing the MSCA_Card.PK public key to be used for verification of the Card_MA certificate and Card_Sign certificate
  - The EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_Card certificate

  - The EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the MSCA_Card certificate, if existing
  - The link certificate linking these two EUR certificates, if existing
  - Symmetric master keys K_{M-WC} and K_{M-DSRC} for workshop cards
  - Symmetric master key K_{M-DSRC} for control cards
- In addition to the above-mentioned cryptographic keys and certificates, tachograph cards shall also contain the keys and certificates specified in Annex IC, Appendix 11, Part A, allowing these cards to interact with first-generation VUs.

4.3.6 Certificate Renewal

Certificate renewal, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.3.7 Certificate Re-key

Certificate re-key is not allowed. New tachograph cards shall be issued when a certificate has expired, and the usage period of the key pair has also expired.

4.3.8 Certificate Modification

Certificate modification is not allowed.

4.3.9 Certificate Revocation and Suspension

Revocation of Tachograph card certificates by the LV-CA is not intended and revocation requests shall not be accepted and processed by the LV-CA.

4.3.10 Certificate Status Services

Certificate status information for all issued Tachograph card certificates is maintained by the LV-CA. This information shall not be published, but will be made available to parties having a legitimate interest upon request.

4.3.11 End of Subscription

Subscription for the LV-CA’s certification service ends when the LV-CP decides for service termination. In this case all issued tachograph card certificates are allowed to expire. The LV-CP notifies service termination to the LV-MSA and the LV-CA. The LV-MSA informs the LV-CIA’s about service termination and subsequent card personalizers or card manufacturers.

4.3.12 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that the private keys Card_MA.SK and Card_Sign.SK shall not be exported to or stored in any place apart from the associated tachograph card.

5 Facility, Management, and operational Controls

5.1 Physical Controls

- The key and certificate generation services of the LV-CA and the corresponding services of LV-CP shall be housed in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorized access, damage, and interference. This area shall be monitored by guards and security alarms must be established.
- Power supply and air conditioning for the LV-CA systems must be appropriate and redundancy shall be established.
- LV-Cas and the LV-CP's systems and storage media used to store confidential information, such as hard disks, smart cards and HSMs, shall be protected against un-authorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Backup and installation media shall be stored in a separate location that is physically secured and protected against unauthorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Procedures for the disposal of waste shall be implemented to avoid unauthorized use, access, or disclosure of confidential data.
- An off-site facility for storage of LV-CA critical data and data needed for emergency recovery shall be implemented.

5.2 Procedural Controls

- Procedural controls shall be implemented by the LV-CA and the LV-CP to ensure secure operations. In particular separation of duties shall be enforced by implementing multiple-person control for critical tasks.
- Access to the LV-CA systems and the corresponding systems of the LV-CP shall be limited to individuals who are properly authorized and, on a need-to-know basis only. In particular, the following access control measures shall be in place:
  - Confidential data[13] shall be protected to safeguard data integrity and confidentiality when stored;
  - Confidential data shall be protected to safeguard data integrity and confidentiality when exchanged over unsecure networks;
  - Confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data, using a safe method acknowledged by the BSI.
  - The LV-CA systems and corresponding systems of the LV-CP shall ensure effective user administration and access management;
  - The LV-CA systems and corresponding systems of the LV-CP shall ensure that access to information and application system functions is restricted to authorized staff and provide sufficient computer security controls for the separation of trusted roles. Particularly, the use of system utility programs shall be restricted and tightly controlled. Access shall be restricted, only allowing access to resources as necessary for carrying out the role(s) allocated to a user;
  - LV-CA's and related LV-CP's personnel shall be identified and authenticated before using the LV-CA systems or the corresponding systems of the LV-CP. Related LV-CP's personnel shall provide a certificate of good conduct when registered with the LV-CA.
  - LV-CA's and LV-CP's personnel shall be accountable for their activities, which shall be logged in event logs as described in section 5.4;

- The LV-CA and LV-CP shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. They shall ensure that the ISMS policies address personnel training, clearances and roles. The ISMS implementation should conform to the requirements described in ISO 27001.

5.3 Personnel Controls

- The LV-CA responsibilities may be outsourced to a specialized company, or personnel from contractors may be hired to carry out the LV-CA responsibilities.
- All personnel involved with the LV-CA or related personnel of the LV-CP shall be properly trained and shall possess the expert knowledge, experience and qualifications necessary for the services offered and appropriate to the job function. This pertains to personnel employed directly, personnel from a specialized company to which tasks have been outsourced or personnel from contractors.
- Personnel training shall be managed according to a training plan described in the respective CPS or security concept.
- Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the CPS or security concept.
- Trusted roles, on which the security of the operation is dependent, shall be clearly identified in the respective CPS or security concept. These roles and the associated responsibilities shall be documented in a role concept or comparable document. This role concept shall be defined from the viewpoint of separation of duties and least privilege. No single person shall be authorized to simultaneously perform more than one of the trusted roles.

5.4 Audit Logging Procedures

All significant security events in the LV-CA software or related software of the LV-CP shall be automatically time-stamped and recorded in the system log files. This includes at least the following:

- Successful and failed attempts to create, update, remove or retrieve status information about accounts of personnel, or to set or revoke the privileges of an account;
- Successful and failed attempts to set or change an authentication method (e.g. password, biometric, cryptographic certificate) associated to a personal account;
- Successful and failed attempts to log-in and log-out on an account;
- Successful and failed attempts to change the software configuration;
- Software starts and stops;
- Software updates;
- System start-up and shut-down;
- Successful and failed attempts to add or remove an entity from the register of subscribers to which the LV-CA currently provides key certification services, or to change any details for any of the subscribers, or to retrieve information from the register;
- Successful and failed attempts to process a certificate signing request or a key distribution request;
- Successful and failed attempts to sign a certificate or generate a key distribution message;
- Successful and failed interactions with the database(s) containing data on (the status of) issued certificates, including connection attempts and read, write and update or removal operations;
- Successful and failed attempts to connect to or disconnect from an HSM.
- Successful and failed attempts to authenticate a user to an HSM.
- Successful and failed attempts to generate or destroy a key pair or a symmetric key inside an HSM;
- Successful and failed attempts to import or export a key to or from an HSM;

- Successful and failed attempts to change the life cycle state of any key pair or symmetric key;
- Successful and failed attempts to use a private key or symmetric key inside an HSM for any purpose.

In order to be able to investigate security incidents, where possible the system log shall include information allowing the identification of the person or account that has performed the system tasks.

The integrity of system event logs shall be maintained and shall be protected from unauthorized inspection, modification, deletion or destruction. System events logs shall be backed-up and stored internally.

5.5 Records Archival

- An overview of the events which shall be archived shall be described in internal procedures and shall be in accordance with relevant rules and regulations. The LV-CA and the LV-CP shall implement appropriate record archival procedures. Procedures shall be in place to ensure integrity, authenticity and confidentiality of the records.
- For all archived information, archival periods shall be indefinite.
- Measures shall be taken to assure that the record archive is stored in such a way that loss is reason-ably excluded.
- The events mentioned in section 5.4 shall be inspected periodically for integrity. These inspections shall take place at least annually.

5.6 Key Changeover

- LV-CA shall generate new LV-CA key pairs as needed. After LV-CA has generated a new key pair, it shall submit a certificate re-key request as described in the appropriate section of the ERCA policy and distribute the keys to the LV-CP as described in the re-keying sections in chapter 4 of this policy.
- The LV-CA shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in this certificate policy.

5.7 Compromise and Disaster Recovery

- The LV-CA and the LV-CP shall define security incident and compromise handling procedures in a Security Incident Handling Procedure manual, which shall be issued to administrators and auditors.
- The LV-CA and the LV-CP shall maintain a Business Continuity Plan detailing how they will maintain their services in the event of an incident that affects normal operations. On detection of an incident, operations shall be suspended until the level of compromise has been established. The LV-CA and the LV-CP shall furthermore assume that technological progress will render their IT systems obsolete over time. Measures to manage obsolescence shall be defined in the Business Continuity Plan.
- Back-up and recovery procedures for all relevant data shall be described in a Back-up and Recovery Plan.
- The following incidents are considered to be disasters:
  - compromise or theft of a private key (LV-CA_Card.SK,) and / or symmetric master key (K_{M-VU}, $K_{M-WC,}$ K_{M-DSRC});
  - loss of a private key (LV-CA_Card.SK,) and / or a symmetric master key (K_{M-VU}, K_{M-WC}, K_{M-DSRC});
  - IT hardware failure.

- In the event of compromise or theft of a LV-CA private key used to sign the public key certificates of tachograph cards (LV-CA_Card.SK), the LV-CA shall immediately inform the LV-MSA, the CIA, the affected LV-CP and the ERCA. All affected parties shall take appropriate measures within a reasonable time period.
- In the event of compromise or theft of one or more of the symmetric master keys stored by the LV-CA, EA and ERCA about the newly appointed (K_{M-VU}, $K_{M-WC,}$ $K_{M-DSRC)}$, the LV-CA shall immediately inform the LV-MSA, the ERCA and the affected LV-CP. All affected parties shall take appropriate measures within a reasonable period of time.
- There is effectively no recovery from a loss of the LV-CA private keys or of the symmetric master keys. Loss shall therefore be prevented by using multiple backup copies of the respective keys and master keys, subjected to periodic controls.
- Protection against IT hardware failures shall be provided by redundancy, i.e. availability of duplicate IT hardware.

5.8 Service Termination

- In the event of termination of LV-CA activity by the appointed organization, the LV-MSA shall notify the EA and the ERCA of this and optionally inform the EA and ERCA about the newly appointed LV-CA. The LV-MSA shall ensure that at least one LV-CA is operational at all times.
- In the event of service termination of the LV-CP, the LV-CA, LV-MSA and the CIA shall be informed of this and the LV-MSA optionally informs the EA and ERCA. The LV-MSA shall ensure that at least one LV-CP is operational at all times. The LV-MSA informs the CIA, EA and ERCA about the newly appointed LV-CP.

6 Technical Security Controls

6.1 Key pair generation and installation

- The LV-CA and the LV-CP shall generate private keys in accordance with Annex IC Appendix 11.
- Generation of key pairs and master keys shall be undertaken in a physically secured environment by personnel in trusted roles under at least dual person control. The key generation ceremony shall be documented.
- The LV-CA shall have available a Test LV-CA system for interoperability test purposes, according to the Regulation. The Test LV-CA system shall be a separate system and shall have its own LV-CA private keys and symmetric master keys. The Test LV-CA system shall be able to request the signing of test certificates and the distribution of symmetric test keys using the processes described in this document and the ERCA Policy. The Test LV-CA shall also be able to sign test equipment certificates on request of the LV-CP and to distribute symmetric test keys and encrypted data for motion sensors to the LV-CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

- The LV-CA and the LV-CP shall maintain the confidentiality, integrity, and availability of the private keys and the symmetric keys as described in this section.
- The private keys and symmetric keys shall be generated and used in a trustworthy dedicated device which:
  - is certified to EAL 4 or higher in accordance with ISO/IEC 15408 using a suitable Protection Profile; or
  - meets the requirements identified in ISO/IEC 19790 level 3; or
  - meets the requirements identified in FIPS PUB 140-2 level 3; or

- offers an equivalent level of security according to an equivalent national or internationally recognized evaluation criteria for IT security.
- The most common implementation of such a trustworthy dedicated device for use in a PKI system is a Hardware Security Module (HSM). Other implementations using different devices are possible as well, as long as the adopted devices satisfy one of the security requirements listed above. In addition, apart from these security requirements, this LV-MSA certificate policy contains various functional requirements for the trustworthy dedicated device used in the LV-CA system. Please note that in case a different device is used in place of an HSM, all such functional requirements have to be satisfied as well. The term “HSM” is used in this document as an abbreviation for the here mentioned requirements.
- Private key operations and symmetric key operations shall take place internally in the HSM where the keys used are stored.
- The LV-CA’s and the LV-CP ’s private keys and symmetric keys shall only be used within a physically secure environment by personnel in trusted roles under at least dual control. All events of private key usage and symmetric master key usage shall be logged.
- The LV-CA’s and the LV-CP’s private keys and the symmetric keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual per-son control in a physically secured environment.
- Back-up copies of the LV-CA’s and the LV-CP’s private keys and the symmetric keys shall be subject to the same level of security controls as the keys in use.
- One back-up copy of each LV-CA private key and of each master key shall be maintained off-site.
- Private key import and export shall only take place for backup and retrieval purposes.
- Symmetric key import and export is allowed for backup and retrieval. For the LV-CA, export of $K_{M-VU,}$ K_{M-DSRC} and K_{M-WC} in encrypted form is allowed in response to a valid key distribution request from the LV-CP by personnel in trusted roles under at least dual person control.
- At the end of the life cycle of a LV-CA private key or of a symmetric master key (as specified in the LV-CA CPS), all copies of the key shall be destroyed such that it cannot be retrieved.
- Private keys and symmetric keys shall be deactivated and destroyed if compromise is suspected. The keys shall be destroyed after the compromise has been investigated and the decision has been taken to deactivate the key.
- Destroying of private keys and master keys shall be done by using the function of the HSM for key destroying. Also, the back-up copies of compromised keys shall be destroyed.

6.3 Other Aspects of Key Pair Management

- The LV-CA public key certificates and hence the public keys shall be archived indefinitely.
- The validity periods of all LV-CA certificates shall comply with Annex IC Appendix 11.
- In accordance with Annex IC Appendix 11, the private key usage period of LV-CA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate. The LV-CA shall not use a private key after the private key usage period is over.

6.4 Activation Data

- The LV-CA private keys and/or symmetric master keys stored in an HSM shall be activated for use if all of the multiple persons controlling the key have authenticated themselves towards the HSM. Authentication shall take place by using proper means (e.g. passphrases, authentication tokens).
- The duration of an authentication session shall not be unlimited.
- For activation of the LV-CA software itself, user authentication shall take place using proper means (e.g. by a passphrase).

6.5 Computer Security Control

The LV-CA and the LV-CP shall specify and approve procedures and specific technical security measures for managing its computer systems. These procedures shall guarantee that the required security level is always met. The procedures and technical security measures shall be described in internal documentations and/or security concepts. Computer systems shall be arranged and managed conforming to these procedures, the procedures specified in the security concepts and best practice procedures for trust centers and for trustworthy computing.

6.6 Life Cycle Security Controls

- The LV-CA and the LV-CP shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built in-to their systems.
- A separation between Acceptance (or Pre-Production) and Production systems shall be maintained. Change procedures and security management procedures shall guarantee that the required security level is maintained in the Production system.
- Change control procedures shall be documented and used for releases, modifications and (emergency) software fixes for any operational software.

6.7 Network Security Controls

The LV-CA and the LV-CP shall devise and implement its net-work architecture in such a way that access from the internet to their internal network domain and from the internal network domain to the Certification Authority systems and related systems of the LV-CP can be effectively controlled.

6.8 Timestamping

The time and date of an event shall be included in every audit trail entry. The LV-CA CPS and the related documentation/ CP CPS shall describe how time is synchronized and verified.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile

All certificates shall have the profile specified in Annex IC, Appendix 11 and Appendix 1:

Data Object	Req	Field ID	Tag	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	m	C	‘7F 21’	var	
Certificate Body	m	B	‘7F 4E’	var	

Certificate Profile Identifier	m	CPI	‘5F 29’	‘01’	INTEGER (0…255)
Certification Authority Reference	m	CAR	‘42’	‘08’	KeyIdentifier
Certificate Holder Authorisation	m	CHA	‘5F 4C’	‘07’	Certificate Holder Authorisation
Public Key	m	PK	‘7F 49’	var	
Standardized Domain Parameters OID	m	DP	‘06’	var	OBJECT IDENTIFIER
Public Point	m	PP	‘86’	var	OCTET STRING
Certificate Holder Reference	m	CHR	‘5F 20’	‘08’	KeyIdentifier
Certificate Effective Date	m	CEfD	‘5F 25’	‘04’	TimeReal
Certificate Expiration Date	m	CExD	‘5F 24’	‘04’	TimeReal
ECC Certificate Signature	m	S	‘5F 37’	var	OCTET STRING

Table 5 Certificate profile

The algorithm is indicated via the Standardized Domain Parameters OID as specified in Table 1 of Appendix 11, Annex IC. The options are:

Name	**Object Identifier reference**	**Object identifier value**
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
BrainpoolP384r1	BrainpoolP384r1	1.3.36.3.3.2.8.1.1.11

Table 6 Allowed Standardized Domain Parameters OIDs

7.2 Certificate Format (Equipment Level)

Equipment level certificates for the smart tachograph system are ECC public key certificates according to ISO/IEC 7816-4 and 7816-8 with some special requirements:

- „card verifiable“ (CV):
  Certificates can be interpreted on the chip card during verification (VERIFY CERTIFICATE operation).

- „self descriptive“:
  For encoding of the ASN.1 data structures and data objects inside the certificates Distinguished Encoding Rules (DER) according to ISO 8825-1 shall be used. This results in the following TLV structure:
- Tag: The tag is encoded in one or two octets and indicates the content.
- Length: The length is encoded as an unsigned integer in one, two, or three octets, resulting in a maximum length of 65535 octets. The minimum number of octets shall be used.
- Value: The value is encoded in zero or more octets.

The issued equipment certificate has a variable length. The format of equipment certificates for tachograph cards (Card_MA.C and Card_Sign.C), is as follows:

Field	**Tag**	**Length**	**Value**	**Remarks**
C	‘7F 21’	var		ECC Certificate
B	‘7F 4E’	var		ECC Certificate Body
CPI	‘5F 29’	‘01’	‘00’	Certificate Profile Identifier
CAR	‘42’	‘08’	CertificationAuthorityKID	Certificate Authority Reference; public key for signature verification (corresponds with CHR in MSCA_Card.C and MSCA_VU-EGF.C)
nationNumeric		*1 Byte*	*‘20‘ for Latvia*	Numeric country code for Latvia: -32(‘0x20’)
nationAlpha		*3 Byte*	IA5String ’4c 56 20’ for Latvia	Alphabetic country code – IA5String with length 3 Bytes: ‚LV’ and one space for Latvia
keySerialNumber		*1 Byte*		*Serial number of key INTEGER (0…255)*
additionalInfo		*2 Byte*	- not used: ‘FF FF’ - for TC: ‘54 43‘ - for VU: ‘56 55‘	LV-CA-related additional information
caIdentifier		*1 Byte*	*‘01’*	*Identifier to differentiate between key identifiers of a CA – value: ‘0x01’*
CHA	‘5F 4C’	‘07’		Certificate Holder Authorization
tachographApplicationID		6 Byte	- *Tachograph card and VU: ‘FF 53 4D 52 44 54’* - *EGF: ‘FF 44 54 45 47 4D’*	6 leading Bytes of application identifier (AID) („SMRDT“) („DTEGM“)

equipmentType		1 Byte	’01’, ’02’, ’03’, 04’, ’06’, ’08’, ’11’, ’12’ or ’13’	With enrolled certificate corresponding equipment type: - Tachograph Cards: - driver card: ‘0x01‘ - workshop card: ‘0x02‘ - control card: ‘0x03‘ - company card: ‘0x04‘ - driver card signature: ‘0x11‘ - workshop card signature: ‘0x12‘ - vehicle unit: ‘0x06‘ - vehicle unit signature: ‘0x13‘ - ext. GNSS facility: ‘0x08‘
PK	‘7F 49’	var		Public Key
DP	‘06’	var	defined Object Identifier	Domain Parameter; Object ID for reference to the standardized Domain Parameters
PP	‘86’	var	OCTET STRING	Public Point (1); converted to octet strings (uncompressed format)
CHR	‘5F 20’	‘08’	ExtendedSerialNumber or CertificateRequestID	Certificate Holder Reference to the public key mentioned in the certificate
serialNumber		*4 Byte*	INTEGER (0..232-1)	Unique serial number of certificate request for mentioned manufacturer/personalizer and month or unique device serial number for mentioned manufacturer, device type, month and year.
monthYear		*2 Byte*	BCDString	Month and year of certificate request or manufacturing, BCD-encoded (2 digits for month, last two digits of the year)
type		*1 Byte*	EquipmentType (‘01’,‘02’, ‘03’, ‘04’, ‘06’,‘08’) or ‘FF’	Device type: - in case of ExtendedSerialNumber:

				EquipmentType: - driver card: ‘0x01’ - workshop card: ‘0x02’ - control card: ‘0x03’ - company card: ‘0x04’ - vehicle unit: ‘0x06’ - ext. GNSS facility: ‘0x08’ - in case of CertificateRequestID: ‘0xFF’
manufacturerCode		*1 Byte*		Numeric manufacturer code of type approved device
CEfD	‘5F 25’	‘04’	TimeReal	Certificate Effective Date Starting date and time of certificate validity (matches date of certificate generation)
CExD	‘5F 24’	‘04’	TimeReal	Certificate Expiration Date Ending date and time of certificate validity
S	‘5F 37’	var		ECC Certificate Signature (2) ECDSA signature over certificate body in plain format

Table 7 Smart Tachograph certificate format equipment level

Comment:

1. Public points on elliptic curves shall be converted to octet strings using the uncompressed encoding format as detailed in TR-03111. To encrypt a point on an elliptic curve, the validations mentioned in TR-03111 have to be performed.

   Uncompressed encoding P_U of point $P = (x_P, y_P)$:
   $P_U = C||X||Y$, with
   $C = 0x04$
   m: = FE2OS(x_P)
   n:= FE2OS(y_P)
   Decoding:
   P = (OS2FE(X),OS2FE(Y))
   Validation:

   Proof shall be made, that P is really a point of that elliptic curve:

   $$y_P^2 = x_P^3 + ax_P + b$$

2. The certificate signature is generated based on the encoded certificate body, including tag and length of the certificate body. According to DSS ECDSA shall be used as signature algorithm using the hash algorithm tied to the key size of the signing entity. The signature format is plain text as mentioned in TR-03111.

The signature (r, s), generated as DER encoded ECDSA signature value
0x30 b1 0x02 b2 (vr)0x02 b3 (vs)

shall be formatted as OCTET STRING R||S, i.e. as concatenation of octet strings R = I2OS(r,l) and S = I2OS(s, l) with $l = [\log_{256}n]$ with a resulting fixed length of 2l octets.

7.3 CRL Profile

No CRL shall be published.

7.4 OCSP Profile

No OCSP shall be used.

8. Compliance Audit and other Assessments

8.1 Frequency or Circumstances of Assessment

- A full and formal audit on the LV-CA operation and the operation of LV-CP shall be performed by order of the LV-MSA. The audit shall establish whether the requirements in this certificate policy and the ERCA policy are being maintained. The LV-MSA shall perform the first audit within 12 months of the start of the operations covered by the approved LV-MSA certificate policy.
- Before the start of the operations covered by the LV-MSA certificate policy, the LV-MSA shall carry out a pre-operational assessment to obtain evidence that the organization is able to operate in conformance to the requirements in the LV-MSA certificate policy.
- If an audit finds no evidence of non-conformity, the next audit shall be performed within a period of 12 to 24 months. If an audit finds evidence of non-conformity, a follow-up audit shall be per-formed within 12 months to verify that the non-conformities have been solved.
- In case of a severe security incident an extraordinary audit shall be performed within 6 months after detection of the incident. Severe incidents in this context are especially the loss of integrity or confidentiality of private and/or symmetric keys. This audit shall focus on the circumstances and follow-up measures with regard to the incident. The normal audit frequency as described in 8.1 is not affected by an extraordinary audit after a security incident.
- The LV-MSA shall report the results of the audits and provide the audit reports, in English, to the ERCA. The audit reports shall define any corrective actions, including an implementation schedule, required to fulfil the LV-MSA obligations.

8.2 Identity/Qualifications of Assessor

- The audit shall be performed by an independent auditor.
- Any person selected or proposed to perform a compliance audit of the LV-CA and LV-CP shall first be approved by the LV-MSA.
- The names of the auditors which will perform the audits shall be registered. Such auditors shall comply with the following requirements:
  - Ethical behavior - trustworthiness, uniformity and confidentiality regarding their relation-ship to the audited parties and when handling its information and data;
  - Fair presentation – findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit;

  - Professional approach – has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in in-formation technologies, PKI and the related technical norms and standards.
  - Good repute - a certificate of good conduct shall be provided to the LV-MSA.

- The auditor shall possess significant knowledge of, and preferably be accredited for:
  - Performance of information system security audits;
  - PKI and cryptographic technologies;
  - The operation of PKI software;
  - The relevant European Commission policies and regulations.

8.3 Assessor's Relationship to assessed Entity

The auditor shall be independent and not connected to the LV-CA and LV-CP.

8.4 Topics covered by Assessment

- The audit of the LV-CA and LV-CP shall cover compliance to the ERCA policy, the LV-MSA certificate policy, the LV-CA CPS and the LV-CP CPS or similar documents for Gen. 2 Smart Tachographs as well as associated procedures and techniques documented by the LV-CA or LV-CP.
- The subjects of the compliance audit shall be the implementation of the technical, procedural and personnel practices described in these documents. Some areas of focus for the audits shall be:
  - Identification and authentication;
  - Operational functions/services;
  - Physical, procedural and personnel security controls;
  - Technical security controls;
  - Security incident handling procedures.
- By assessment of the audit logs it shall be determined whether weaknesses are present in the security of LV-CA or LV-CP systems. Determined (possible) weaknesses shall be mitigated. The assessment and possible weaknesses shall be recorded.
- In case of an extraordinary audit triggered by a severe security incident the audit shall focus on processes and technical measures with regard to the security incident.

8.5 Actions taken as a Result of Deficiency

If deficiencies for non–conformity are discovered by the auditor, corrective actions shall be taken immediately by the LV-CA and LV-CP. After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.6 Communication of Results

- The independent auditor shall report the full results of the compliance audit in English language to the audited entity (LV-CA, LV-CP) and the LV-MSA. The LV-MSA shall send an audit report for the LV-CA covering the relevant results of the audit to the ERCA. This shall include at least the number of deviations found and the nature of each deviation. The audit report reception date shall be published on the ERCA website.
- If requested by the ERCA, the LV-MSA shall send the full results of the compliance audits of all re-quested entities to the ERCA.

9. Other Business and Legal Matters

9.1 Fees

Not applicable.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

Confidential data shall comprehend:

- Personal data (e.g. Cardholder data);
- Private keys;
- Symmetric master keys;
- Company or manufacturing data;
- Reasons for certificate revocation;
- Audit logs (unless access is required by law, regulations, or provisions of the CP or CPS);
- Detailed documentation regarding the PKI management;
- Audit reports by internal or external auditors.

Confidential information shall not be released, unless a legal obligation exists to do so.

9.4 Privacy of Personal Information

This data shall be treated according to the General Data Protection Regulation 2016/679.

9.5 Intellectual Property Rights

The LV-CA owns intellectual property rights of the LV-CA software.

9.6 Representations and Warranties

The LV-CA shall operate according to the ERCA CP, this CP and its own CPS.

9.7 Disclaimers of Warranties

The LV-CA disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorized source), and further disclaims any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

9.8 Limitations of Liability

The Republic of Latvia is not liable for any loss:

- of service due to war, natural disasters or other uncontrollable forces;
- incurred between the time certificate status changes and the next scheduled issuance of certificate status information;
- due to unauthorized use of certificates issued by the LV-CA, and use of certificates beyond the pre-scribed use defined by this Certificate Policy and the LV-CA CPS;
- caused by fraudulent or negligent use of certificates and/or certificate status information issued by the LV-CA.

The Republic of Latvia disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon:

- any certificate issued by the LV-CA, or its associated public/private key pair, used by a subscriber or relying party;
- any symmetric key distributed by the LV-CA, used by a subscriber or relying party;
- any encryption service provided by the LV-CA and used by a subscriber or relying party.

Issuance of certificates, symmetric keys and encryption services by the LV-CA does not make the Republic of Latvia or the LV-CA an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the Smart Tachograph key management system.

Subscribers and relying parties are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this key management system.

In addition, the LV-CA is not an intermediary to transactions between subscribers and relying parties. Claims against the LV-CA are limited to showing that it operated in a manner inconsistent with this certificate policy and the LV-CA CPS.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

This LV-MSA Certificate Policy is valid from the moment the LV-CA becomes operational. It shall be valid until further notice.

The validity of this CP ends when the LV-CA stops operating or when the LV-MSA announces this CP is no longer valid, e.g. because a new version of the CP becomes effective.

9.11 Individual Notices and Communications with Participants

Official notices and communications with participants in the Smart Tachograph key management system shall be in written form, and subject to the registration procedures for correspondence in force within the LV-MSA.

Notice of severance or merger may result in changes to the scope, management and/or operation of the LV-CA. In such an event, this LV-MSA certificate policy and the LV-CA CPS may require modification as well. Changes to these documents shall be made in a manner consistent with the administrative requirements stipulated in section 9.12 of this document.

9.12 Amendments

This CP is issued under responsibility of the LV-MSA. The LV-MSA may revise this CP if it deems this necessary.
The procedure for change propositions and approvals of this CP shall be as follows:

- Comments or requests for changes to the CP shall be directed to the LV-MSA. Such communication shall include a description of the comment or requested change, a rationale, and contact information for the person submitting the comments or requesting the change.
- The LV-CA shall accept, accept with modifications, or reject the comment or proposed change after completion of the comment period. LV-CA disposition of proposed changes are reviewed by the LV-MSA. Decisions with respect to the proposed changes are at the discretion of the LV-CA and the LV-MSA.
- A new version of this CP will be published on the website and distributed to the ERCA and to the LV-MSA.

Every change to this CP shall be accompanied by an increase in the version number of the document. The only changes that may be made to the CP and CPS with no change to the document version number are editorial or typographical corrections.
The LV-CA may change the contact information in section 1.5 with notification to the LV-MSA and the ERCA, but without change to the document version number. All other changes to the CP shall be made according to the amendment procedure outlined in this section.

9.13 Dispute Resolution Provisions

Any dispute related to key and certificate management between the LV-CA and an organization or individual outside of the LV-CA shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the LV-MSA.

9.14 Governing Law

Latvian and European regulations shall govern the enforceability, construction, interpretation, and validity of this LV-MSA Certificate Policy.

9.15 Compliance with Applicable Law

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 of the European Parliament and of the Council and with Commission Implementing Regulations (EU) 2016/799 and (EU) 2018/502. In case discrepancies exist between this document and the Regulation or Implementing Regulation, the latter shall prevail.

9.16 Miscellaneous Provisions

No stipulation

9.17 Other Provisions

No Stipulation

10 References

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, Official Journal of the European Union L 139, including ref. 3.

3. Commission Implementing Regulation (EU) 2018/502, amending Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 85

4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997

6. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0, Month year

7. Smart Tachograph - Equipment Interoperability Test Specification, JRC, version 1.0, Month year

8. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

9. ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition, 2006-05-01

10. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 – 2014

11. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15

12. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15

13. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001

14. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013

15. ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01

16. ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher. Third edition, 2006-02-01

17. National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005

18. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01

11 List of Figures

12 List of Tables