Smart Tachograph

Spanish Member State Authority Certificate Policy

Version 1.1

Version Control

Official Version 1.0	January 2019	Approved by the European Authority
Official Version 1.1	May 2020	Amendments according to the 2020 audit

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. The use of the digital tachograph is required by law in the European Union.

The Smart Tachograph is the second generation of the Digital Tachograph, a control device for recording drivers' activities, such as driving and rest periods in commercial vehicles.

Similar to the Digital Tachograph system (Gen-1), the Smart Tachograph system (Gen-2) is a three-layered hierarchic Public Key Infrastructure (PKI) system. A Root Certification Authority is established at the European level (European Root Certification Authority or ERCA) and is connected to the different Member State Certification Authorities (MSCAs) to create a consistent and secure system. The role of ERCA is to securely certify the public keys of the MSCAs to establish a trusted certification chain. Moreover, the ERCA also distributes a number of symmetric master keys to the MSCAs.

At the national level, the role of the MSCAs is to securely certify the public keys of Smart Tachograph equipment issued under their accountability: Vehicle Units (VU), Tachograph Cards (TC), Motion Sensors (MS) and/or External GNSS Facilities (EGF). Moreover, MSCAs are responsible for distributing master keys and/or cryptographic data derived from master keys to the component personalizers (CP) that are responsible for issuing this equipment.

At the equipment level, equipment personalizers are responsible for creating equipment key pairs and inserting equipment keys and certificates securely into their equipment. For some types of equipment, personalizers also insert symmetric keys into the equipment. Personalizers obtain these keys from the ERCA or from the MSCA.

To ensure compatibility with existing first-generation equipment, second-generation equipment shall be equipped both with first generation (TDES and RSA) keys and certificates as well as second-generation (AES and ECC) keys and certificates. This means that for the foreseeable future, tachograph cards will contain two applications, as specified in Appendix 2 to Annex 1C of EU 799/2016 [3].

For more details, the reader is referred to the Implementing Regulation (EU) 799/2016 [3], and especially to Appendix 11 of Annex 1C thereof. Note that this Regulation has been amended by Commission Implementing Regulation (EU) 502/2018. Every reference to EU 799/2016 [3] in this MSA certificate policy is supposed to include these amendments.

Part A of Appendix 11 defines the security mechanisms for the first-generation tachograph system (digital tachograph) based on RSA public-key cryptographic systems and Triple-DES based symmetric cryptographic systems.

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 systems rely on master keys that have to 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. 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 follows the framework for CPs described in RFC 3647 [4]. The Symmetric Key Infrastructure policy has been added to this document, preserving the lay-out of RFC 3647 [4]. How MSCA itself complies with this

Certificate and Symmetric Key Infrastructure Policy is described in the MSCA Certification Practice Statement (CPS).

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 “Smart Tachograph Spanish Member State Authority Certificate Policy“. 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.

1.2.1. Approval

Version 1.0 of this policy was endorsed by the European Root Certification Authority – ERCA (see section 1.3.1.1) on 29.01.2019**.**

1.2.2. Scope and applicability

This certificate policy is valid for the Smart Tachograph System only.

The smart cards and digital certificates issued by the Spanish MSCA are only for use within the Smart Tachograph system.

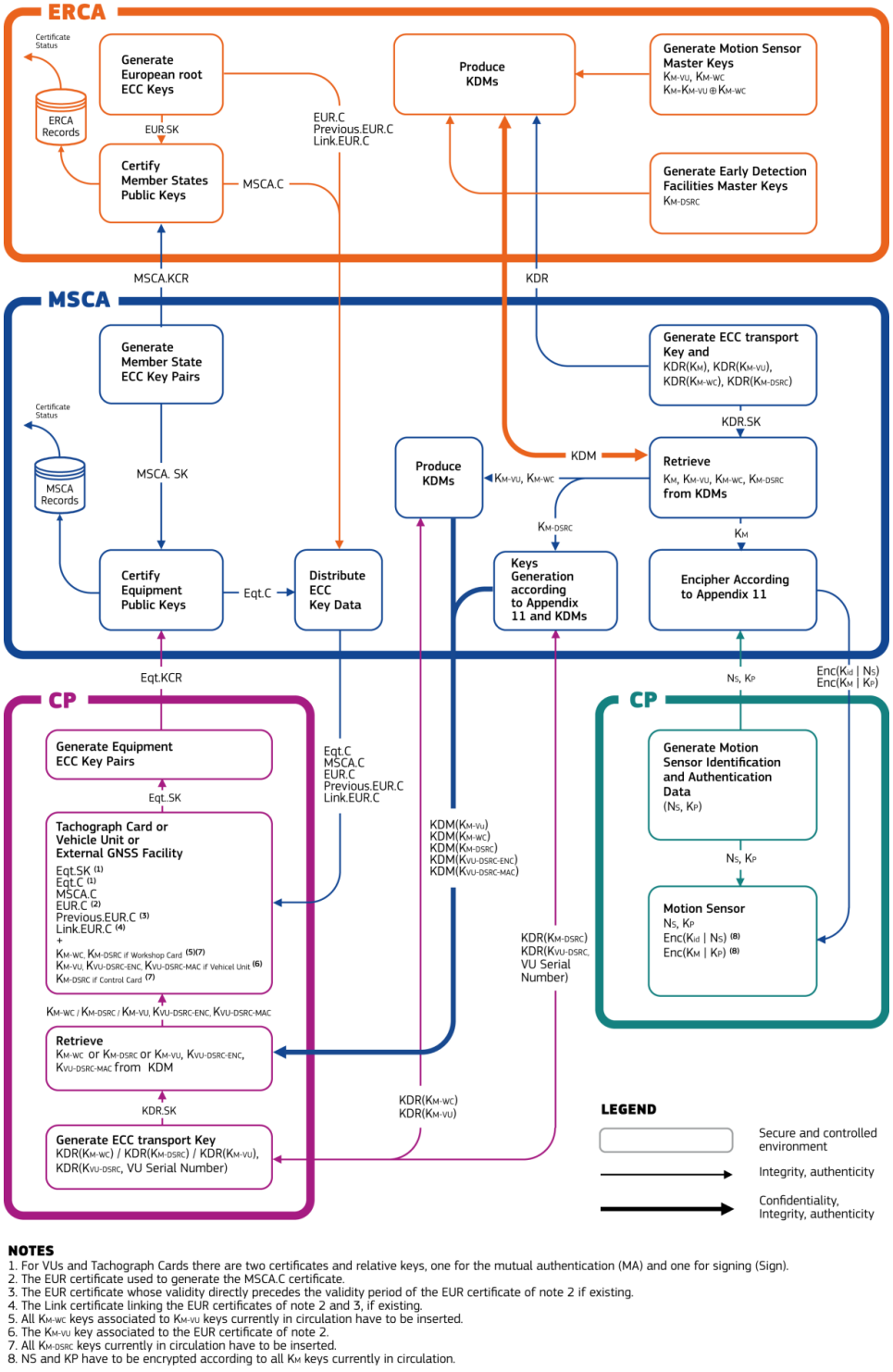
1.2.3. Document objective

The Certificate Policy for the MSA at the national level for the first generation of Digital Tachograph is “Spanish MSA policy (E-MSA)” version 1.3. It lays down the policy at national level for key generation, key management and certificate signing for the Digital Tachograph system (first-generation tachograph system).

The objective of this document is to form the Certificate Policy for the MSA at Spain level for elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems. It lays down the policy at Spain level for key generation, key management and certificate signing for the Smart Tachograph system.

1.3. Smart Tachograph PKI Participants

The participants in the Smart Tachograph PKI and in the Symmetric Key Infrastructure are described here and represented in Figure 2, it also represents the exchanges between the participants, namely ERCA, MSCAs and component personalizers (CPs).



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 $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ 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 Participants in the Smart Tachograph PKI and symmetric key infrastructure

1.3.1. Certification Authorities

1.3.1.1. European Root Certification Authority (ERCA)

ERCA is the root Certification Authority (CA) that signs public key MSCA certificates. It operates the following component services: registration service, certificate generation service, dissemination service.

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: the Motion Sensor Master Key–VU part ($K_{M\text{-}VU}$), the DSRC Master Key ($K_{M\text{-}DSRC}$) and the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC}$)

The ERCA Smart Tachograph European Root Certificate Policy and Symmetric Key [1] is available on the JRC website at:

https://dtc.jrc.ec.europa.eu/iot_doc/Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy v1.0.pdf

1.3.1.2. Spanish Member State Certificate Authority (E-MSCA)

The E-MSCA operates as sub-CA under the ERCA. It signs public key certificates for equipment. For this, it operates a registration service, certificate generation service and dissemination service. The E-MSCA receives the certificate requests from component personalizers and disseminates the certificates to these parties. There are two types of MSCA key pair(s) and corresponding MSCA certificate(s): one for the issuance of VU and EGF certificates, called MSCA_VU-EGF key pair; and one for the issuance of Card certificates, called MSCA_Card key pair. The E-MSCA shall request the MSCA_Card certificate from the ERCA, because of its responsibility regarding the issuance of Card certificates. The E-MSCA also requests symmetric master keys from the ERCA and distributes $K_{M\text{-}WC}$ and $K_{M\text{-}DSRC}$ to card personalizers.

1.3.2. Registration Authorities

The E-MSCA comprises only a certification authority. Functionality associated with a registration authority is performed by the Card Issuing Authority (CIA). The Spanish Card Issuing Authority (CIA), referred to hereinafter as E-CIA is appointed by the E-MSA.

The E-CIA shall operate in conformance with all applicable requirements in:

- this E-MSA certificate policy;
- the ERCA certificate policy for the Digital Tachograph;
- the ERCA certificate policy for the Smart Tachograph;
- the EU Regulation 799/2016 [3] in particular Annex 1C.

The E-CIA is responsible for

- verifying whether all required documents are correct;
- 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 E-MSA-Policy are fulfilled;
- verifying whether a tachograph card was already issued to the applicant in another member state of the Tachograph System;
- ensuring that the applications data is transmitted to the E-CP properly according to the required documents and to the requirements of this policy;
- informing all users about the requirements of this policy in an appropriate manner;

1.3.3. Subscribers

The subscribers to the E-MSCA certificate signing service is the E-CP responsible for the personalization of tachograph Cards

Four different types of tachograph cards exist: driver cards, company cards, workshop cards and control cards.

The following equipments contain 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 $K_{M\text{-}WC}$ and $K_{M\text{-}DSRC}$.
- 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 $K_{M\text{-}DSRC}$.

Component personalizers are responsible for ensuring the equipment are provided with the appropriate keys and certificates

1.3.3.1. Spanish Card Personalizer

For driver and workshop cards:

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

For company and control cards

- ensures generation of the card key pair for mutual authentication;
- performs the certificate application process with the MSCA_Card;
- performs the application of K_{DSRC} (control cards only);
- ensures availability in the card of keys and certificates for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only).

1.3.4. Relying parties

Parties relying on the public key certification services of the E-MSCA are primarily the national and international authorities (control bodies) tasked with enforcing the rules and regulations regarding driving times and rest periods. These parties use the certified public key in the Gen-1 Card certificate and the Gen-2 Card_Sign certificate on driver and workshop cards to validate the authenticity and integrity of data downloaded from such cards, by verifying the signature over these data.

1.4. Key and Certificate Usage

1.4.1. Appropriate Certificate Uses

The E-MSCA shall use its E-MSCA private keys only for:

- Signing of equipment certificates, in accordance with Appendix 11 of Annex 1C of EU Regulation 799/2016 [3].
- Signing of certificate signing requests
- Issuing Certificate Revocation Lists, if such a method is used for providing certificate status information.

The E-MSCA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to component personalizers by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Appendix 11 of Annex 1C of EU Regulation 799/2016 [3].

The E-MSCA_Card certificates shall be used to verify card certificates issued by the E-MSCA_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.

$K_{M\text{-}WC}$ shall be provided by E-MSCA to E-CP for their installation in Workshop Cards. $K_{M\text{-}WC}$ shall be used by the VU together with $K_{M\text{-}VU}$ to generate K_M during VU-MoS pairing.

K_{DSRC} shall be provided by E-MSCA to E-CP for their installation in 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

1.4.2. Prohibited Certificate Uses

All other uses of certificates issued by the E-MSCA are prohibited.

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 shall review the MSA certificate policies, including this E-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.

After approval by the ERCA the Member State Authority shall make its MSA certificate policy available to all stakeholders, including the MSCA(s) and equipment personalizers in its country.

The ERCA shall provide 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 this ERCA certificate policy will be met.

Continuation of key certification service from the ERCA to an MSCA shall depend 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. Spanish Member State Authority (E-MSA)

Responsible for this National MSA policy is the Spanish Member State Authority, **E-MSA,** that is responsible of:

- 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.
- Making an English version of this E-MSA CP available to the ERCA.
- Approving the E-MSCA CPS in compliance with this CP.
- Ensuring that the E-MSCA has the resources required to operate in conformity with this certificate policy.

The contact address of the **E-MSA** is:

Ministerio de Transportes, Movilidad y Agenda Urbana
Paseo de la Castellana, 67
28071 Madrid

The appointed authority in the Ministerio de Transportes, Movilidad y Agenda Urbana is the Dirección General de Transporte Terrestre (General Directorate of Terrestrial Transport), in charge of E-MSA policy and the execution of its tasks.

The Dirección General de Transporte Terrestre (General Directorate of Terrestrial Transport) is also in charge of the Card Issuing Authority for Tachograph Cards (E-CIA). It will keep in their own premises the system, hardware and software, to support this task.

1.5.3. Member State Certification Authority (MSCA)

The E-MSA appoints the **Fábrica Nacional de Moneda y Timbre Real Casa de la Moneda** as Spanish MSCA, **E-MSCA**. The E-MSCA is responsible for implementation of the E-MSA certificate policy and for the provision of key certification and key distribution services to the component personalizers in Spain.

The E-MSCA shall document its implementation of the E-MSA CP in an E-MSCA Certification Practice Statement. The E-MSCA shall make its Certification Practice Statement available to the E-MSA.

The E-MSA shall be responsible to determine whether the E-MSCA CPS complies with the E-MSA certificate policy.

The E-MSCA shall make its Certification Practices Statement available to its subscribers on a need-to-know basis. Upon request, the E-MSCA shall also make its Certification Practices Statement available to the ERCA.

The E-MSCA shall maintain record of its operations as appropriate to demonstrate conformity with the E-MSA CP, and shall make these records available to the E-MSA and/or the ERCA on demand. Complaints from component personalizers about the services provided by the E-MSCA shall be addressed to the responsible E-MSA to be dealt with.

The contact address of the **E-MSCA** is:

Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
Jorge Juan, 106
28009 Madrid

1.5.4. Spanish Card Personalizer

The E-MSA appoints the **Fábrica Nacional de Moneda y Timbre Real Casa de la Moneda** as Spanish card personalizer, **E-CP**. The E-CP is responsible for implementation of the E-MSA certificate policy and for the provision of key certification and key distribution services to the cards in Spain.

The E-CP shall document its implementation of the E-MSA CP in an E-CP Certification Practice Statement. The E-CP shall make its Certification Practice Statement available to the E-MSA.

The E-MSA shall be responsible to determine whether the E-CP CPS complies with the E-MSA certificate policy.

The E-CP shall maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National policy, in particular to bear the risk of liability damages.

The E-CP will ensure that all requirements on it, as detailed in this policy, are implemented and the E-CP has the responsibility for conformance with the procedures prescribed in this policy.

The contact address of the **E-CP** is:

Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
Jorge Juan, 106
28009 Madrid

1.6. Definitions and acronyms

1.6.1. Definitions

Card/Tachograph cards: Integrated Circuit equipped card, in this policy this is equivalent to the use of the terms “IC-Card” and “Smart Card”.

Cardholder: A person or an organization that is a holder and user of a Tachograph card. Included are drivers, company representatives, workshop workers and control body staff.

Certificate: In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.

Certificate Policy: A named set of rules that indicates the applicability of keys, certificates and equipment to a particular community and/or class of application with common security requirements.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual certificate policy.

Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.

Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy, most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.

Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.

Private key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called Secret key.

Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.

Tachograph cards/Cards: Four different type of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.

User: Users are equipment users and are either Card Holders for card or manufacturers for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

1.6.2. Acronyms

AES	Advanced Encryption Standard
CAR	Certification Authority Reference
CHR	Certificate Holder Reference
CIA	Card Issuing Authority
E-CP	Spanish Component Personalizer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSRC	Dedicated Short Range Communication
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
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
JRC	Joint Research Centre
KCR	Key Certificate Request
KDR	Key Distribution Request
KDM	Key Distribution Message
KID	Key Identifier
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_{DSRC}	DSRC Master Key
MA	Mutual Authentication
MoS	Motion Sensor
MSA	Member State Authority
E-MSA	Spanish Member State Authority
MSCA	Member State Certification Authority
E-MSCA	Spanish Member State Certification Authority
NCP	Normalized Certificate Policy
PKI	Public Key Infrastructure
RA	Registration Authorities
RFC	Request for Comment
TLV	Type-Length-Value
VU	Vehicle Unit
WC	Workshop Card

2. Publication and Repository Responsibilities

2.1. Repositories

The certificates signed by the E-MSCA are also be maintained in the E-MSCA database.

2.2. Publication of certification information

The E-MSA shall publish the E-MSA Certificate Policy for Smart Tachograph System on its website: www.mitma.gob.es.

The E-MSCA Certification Practices Statement is not public, but shall be communicated on request and on a need to know basis 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 policy.

2.4. Access Controls on Repositories

All information available via the E-MSA website repository shall have read-only access.

All information published on the E-MSA website repository 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 E-MSCA and the ERCA. I&A between the E-MSCA and equipment manufacturers or card personalizers is detailed in the E-MSCA CPS.

3.1. Naming

3.1.1. Types of names

3.1.1.1. Certificate subject and issuer

The Certification Authority Reference (CAR) and Certificate Holder Reference (CHR) identify the issuer and subject of a certificate. They shall be formed in the following way as described in Annex 1C, Appendix 11, CSM_136 and Appendix 1:

Entity	Identifier	Construction
E-MSCA	Certification Authority Key Identifier (KID)	Nation numeric (‘0F’) Nation alpha (E) Key serial number Additional info CA identifier (‘01’)

Table 1 Identifiers for MSCA certificate and subjects

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.

The value of the additionalInfo field in the CHR of E-MSCA certificates for Production shall have the value ‘FF FF’.

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 the E- 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 the 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.

3.1.2. Need for names to be meaningful

The meaning of the possible values for the CHR and CAR fields in a card certificate is explained in the Smart Tachograph ERCA certificate policy and in Annex 1C of EU Regulation 799/2016 [3].

3.1.3. Anonymity or pseudonymity of subscribers

The relation between the CHR field in a card certificate issued by the E-MSCA and the legal person (i.e. the Card Holder) holding that certificate is registered by the E-CIA. It cannot be established from the contents of the certificate itself.

Subscriber anonymity is not allowed.

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 E-MSCA defines a procedure for the authentication of organization identities in its Certification Practice Statements.

3.2.3. Authentication of Individual Identity

The E-MSCA defines a procedure for the authentication of individual identities. The procedure is documented in its Certification Practice Statements.

3.2.4. Validation of Authority

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

3.2.5. Criteria for interoperation

The E-MSCA 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 E-MSCA must rely on an external PKI for any other service or function, they shall review and approve the CP and/or CPS of the external certification service provider prior to applying for certification services as a subject.

3.3. I&A for Re-key Requests

The Identification and Authentication (I&A) procedures for re-key requests (see sections 4.1.8 and 4.2.9 of this policy) shall be the similar to those described in section 3.2 of this policy.

3.4. I&A for Revocation Requests

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 E-MSCA describes in its CPS how it will validate certification revocation requests for equipment certificates, if certificate revocation procedures are available.

4. Life-Cycle Operational Requirements for Certificates and Master Keys

This chapter describes the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates and symmetric keys for cards between the E-MSCA and the E-CP, as well as for the application and distribution of MSCA certificates and symmetric master keys between the ERCA and the E-MSCA.

4.1. 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 Application

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

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 Authorization	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 2 Identifiers 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 E-MSCA 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 Authorization** 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 1C, 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 1C.
- 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 1C, 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 1C, 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 1C, 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 1C, 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 E-MSCA applies for its initial certificate. The outer signature shall be required if the E-MSCA applies for a successive certificate. In this case, the Certificate Signing Request shall be additionally signed via an outer signature by the -MSCA, using one of its current valid E-MSCA private keys. The outer signature authenticates the request. Because the E-MSCA is subscribed to receive both MSCA_Card 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 E-MSCA key used for signing, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain, as specified in ISO/IEC 18033-2.

The E-MSCA 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 1C, 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 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 1C, 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 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 1C, 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 1C, 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 E-MSCA 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) or binary (.bin file) format.

The ERCA writes three copies of each certificate to the transport medium for return to the E-MSCA. 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 E-MSCA, respectively.

For both CSRs and certificates, the transport media and the printouts are handed over between an ERCA employee and the E-MSCAs courier in the ERCA controlled area.

4.1.5. Certificate Acceptance

The courier signs for receipt of the E-MSCA certificate at the ERCA premises.

Upon reception of the certificate at the E-MSCA premises, the E-MSCA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the certificate complies with Table 6 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 E-MSCA 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 E-MSCA 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 E-MSCA certificate, in replacement of an existing certificate.

Certificate re-key shall take place either:

- when the E-MSCA 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 E-MSCA 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 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

E-MSCA 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 an E-MSCA private key;
- loss of an E-MSCA private key;
- E-MSCA termination;
- E-MSA or E-MSCA 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 E-MSCA certificate revocation procedure is described in E-MSCA CPS.

4.1.10.4. Revocation request grace period

The grace period for the E-MSCA 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 ERCA repository.

4.1.10.7. Certificate status issuance frequency

The status of the MSCA public key certificates shall be 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 E-MSCA revocation / status information published in 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 one of the E-MSCA keys is compromised or suspected to be compromised, the E-MSCA shall report the incident to the ERCA and to the E-MSA it will be done without unnecessary delay and at least within 8 hours of detection. In their notification, the E-MSCA shall indicate the circumstances under which the compromise occurred. Any follow-up investigation and potential action by the MSA and/or E-MSCA shall be performed as indicated in the E-MSA certificate policy. The outcome of the E-MSA investigation shall be reported to the ERCA

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

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 E-MSCA's certificate signing services ends when the E-MSA and/or E-MSCA decides for E-MSCA termination. Such a change is notified to ERCA by the E-MSA as a change to the E-MSA certificate policy.

In the case of subscription ending, the decision to submit a certificate revocation request for any valid E-MSCA certificates, or to allow all E-MSCA certificates to expire, is the responsibility of the E-MSA.

4.1.13. Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that E-MSCA private keys shall not be exported to or stored in any system apart from the E-MSCA systems.

4.2. Symmetric Master Key Application and Distribution between the ERCA and the E-MSCA

4.2.1. Key Distribution Requests

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

A KDR shall be in TLV-format. Table 3 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 3 Key distribution request format

m: require;

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 Authorization** 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 E-MSCA 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 E-MSCA. For that reason, the ERCA copies the key identifier in the key distribution message, see Table 4

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

- The data element Public Point shall contain the public point of the ephemeral E-MSCA key pair to be used for key agreement. The E-MSCA 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 E-MSCA 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 1C, 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 3
- 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 1C, 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, ERCA shall proceed to prepare the key distribution message (KDM) by determining the symmetric key requested by the E-MSCA and following the steps as described in section 4.2.3 of this policy (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 1C, 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 1C:

- 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 3
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 1C, 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:

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

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)

$$S = \textit{Message Recipient Authorization} \,||\, \textit{Key Identifier}$$

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.

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

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 of this policy), ERCA shall construct a key distribution message as shown in Table 4. For the lengths, the DER encoding rules 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 ERCA for ECDH key agreement	m	'86'
Encrypted symmetric key	m	'87'
MAC	m	'88'

Table 4 Key distribution message format

The version of the profile is identified by the **Request Profile Identifier**. Version 1 specified in Table 4 shall be identified by a value of '00'.

The **Message Recipient Authorization** shall be identical to the Message Recipient Authorization 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 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 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) or 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 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 4;
- the message is genuine. The MSCA shall do this by contacting ERCA as described in ERCA CPS and verifying that the MAC in the received KDM matches the MAC in the KDM sent by 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 ERCA.

If any of these checks fail, the MSCA shall abort the process and contact 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 of this policy, using the MSCA's ephemeral private key indicated by the key identifier in the message and 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 ERCA. Else, the MSCA shall form the shared secret K by converting K_x to an octet string (Conversion between Field Elements and Octet Strings);
- derive the keys K_{ENC} and K_{MAC} as described in step 4 in section 4.2.3 of this policy,
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3 of this policy. If this verification fails, the MSCA shall abort the process and contact ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3 of this policy. 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 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 E-MSCA 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 E-CP shall be informed immediately as further described in the E-MSCA practice statement.

4.2.10. Symmetric Key Compromise Notification

If the E-MSCA detects or is notified of the compromise or suspected compromise of a symmetric master key, the E-MSCA shall notify this to the ERCA and the E-MSA without unnecessary delay and at least within 8 hours of detection. In their notification, the E-MSCA shall indicate the circumstances under which the compromise occurred.

Any follow-up investigation and potential action by the E-MSA and/or E-MSCA shall be performed as indicated in this E-MSA certificate policy. The outcome of the E-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 ERCA's key distribution services ends when E-MSA decides for E-MSCA termination. Such a change is notified to ERCA by the E-MSA as a change to the national policy.

In the case of subscription ending, the E-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 E-MSCA production and fallback systems.

4.3. Tachograph Card Certificate Application and Issuance

4.3.1. Certificate Application

The E-MSCA 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.

The E-MSCA shall only accept certificate applications for tachograph cards with a valid type approval as described in Annex 1C (chapter 8).

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 card manufacturers or card personalizers, as described in Annex 1C 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 E-MSCA in order to obtain a corresponding card certificate signed by the E-MSCA. The private key shall be used only by the tachograph card. Key certification requests that rely on transportation of private keys are not allowed.

4.3.2. Certificate Requests

Certificate requests are collected inside a request package. The private parts of the packages are cyphered by using a symmetric key generated by a dedicated HSM as described in the E-MSCA CPS. Each certificate request contains the following elements:

Data Object	Length	Format	Data
certificateRequestID	16 Byte	CertificateRequestID	Request ID
cardNumber	16 Byte	CardNumber	Card Number
CHR	16 Byte	Base64	Card Holder Reference
CAR	16 Byte	Base64	Card Authority Reference to sign the certificate
EquipmentType	1 Byte	INTEGER	Equipment type: - Driver card: ‘0x01‘ - Workshop card: ‘0x02‘ - Control card: ‘0x03‘ - Company card: ‘0x04‘
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 1C.
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 1C, Appendix 11, CSM_143)

Table 5 Tachograph Card Certificate Request Data

4.3.3. Certificate Issuance

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

If key generation takes place outside the E-MSCA, the E-MSCA shall only issue a certificate to the E-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 E-MSCA shall also ensure that a certificate request package originating from the E-CP is complete, accurate, and duly authorized. The E-MSCA 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 E-MSCA system as described in the E-MSCA CPS. The key component for authorization hereby is the symmetric key generated by a dedicated HSM.

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.

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.

4.3.4. Certificate Acceptance

The E-CP shall only accept the certificate if it matches the associated certificate request.

4.3.5. Key Pair and Certificate Usage

- The E-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 1C, 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 $K_{M\text{-}WC}$ and $K_{M\text{-}DSRC}$ for workshop cards.
    - Symmetric master key $K_{M\text{-}DSRC}$ 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 1C, 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 E-MSCA is not intended and revocation requests shall not be accepted and processed by the E-MSCA.

4.3.10. Certificate Status Services

Certificate status information for all issued Tachograph card certificates is maintained by the E-MSCA. 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 E-MSCA's certificate signing services ends when the E-MSA and/or E-MSCA decides for E-MSCA termination. Such a change is notified to ERCA by the E-MSA as a change to the E-MSA certificate policy.

In the case of subscription ending, the decision to submit a certificate revocation request for any valid E-MSCA certificates, or to allow all E-MSCA certificates to expire, is the responsibility of the E-MSA.

The E-CP is responsible for ensuring the equipment is provided with the appropriate keys and certificates. End of subscription for the equipment manufacturers ends when the E-CP subscription for the E-MSCA's certificate signing services ends.

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.

4.4. Symmetric Master Key Workshop Part (KM_{WC}) and DSRC Master Key (KM_{DSRC}) Application and Distribution

4.4.1. Key Distribution Requests

A formal Key distribution request (KDR) is not necessary.

4.4.2. Key Distribution Messages

A formal Key distribution request (KDM) is not necessary.

4.4.3. Issuance of Symmetric Master Keys

The E-MSCA shall only issue symmetric master keys to the E-CP.

4.4.4. Master Symmetric Key Requests

A formal Master Symmetric Key requests is not necessary.

4.4.5. Key Usage

Card personalizers shall use any received symmetric key in accordance to section 6.2.

4.4.6. KDM Renewal

KDM renewal is not allowed. In case the KDM is damaged or corrupted, a new KDM must be generated.

4.4.7. Key Re-key

In case the ERCA has generated a new version of a symmetric master key as specified in Appendix 11 sections 9.2.1.2 and 9.2.2.2 distributing new symmetric keys shall take place in a timely manner so that the key can be placed in time in newly issued components.

4.4.8. Symmetric Key Compromise Notification

If the E-CP detects or is notified of the compromise or suspected compromise of a symmetric key shall notify this to the E-MSCA and the E-MSA without unnecessary delay and at least within 8 hours of detection. In their notification, the E-CP shall indicate the circumstances under which the compromise occurred. The E-CP shall handle the incident according to a defined security incident handling procedure. Following the incident, the results of the follow-up investigation, initial and potential actions shall be reported to the E-MSCA and the E-MSA, for the first time not later than one week after the incident was detected.

In addition to immediate actions taken by the component manufacturer or card personalizer, E-MSCA and E-MSA check and agree on appropriate actions.

Symmetric key compromise is considered a severe security incident, which results in an extraordinary audit according to 8.1, which focuses on the actions related to the incident.

4.4.9. Key Status Service

No status service for symmetric keys will be published or especially maintained by the E-MSCA

4.4.10. Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that symmetric keys shall not be exported to or stored in any system apart from the systems of the equipment of the E-CP.

5. Facility, Management, and Operational Controls

5.1. Physical Security Controls

5.1.1. Site location and construction

The key management and certificate generation and revocation services of the E-MSCA and the E-CP shall be housed in a secure area, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorized access, damage, and interference. Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.
The E-MSCA, and the E-CP shall provide continuous monitoring and alarm facilities to detect and register any unauthorized or irregular attempts to access its resources, and to react upon them in a timely manner.

5.1.2. Physical access

The E-MSCA and E-CP shall ensure that physical access to trustworthy systems and critical services is controlled and registered. Physical access to facilities concerned with key generation, certificate generation and revocation management shall be limited to adequately identified and authorized individuals, i.e. persons in a trusted role as described in section 5.2.1 of this policy.

5.1.3. Power and air conditioning

Power supply and air conditioning for the E-MSCA systems must be appropriate and redundancy shall be established.

5.1.4. Water exposures

The E-MSCA, and E-CP shall take measures to minimize the risk of exposure to water of their critical systems, especially key management and certificate generation systems.

5.1.5. Fire prevention and protection

The E-MSCA, and E-CP shall take measures to minimize the risk of fire in the facilities housing their systems.

5.1.6. Media storage

The E-MSCA, and E-CP shall take measures to protect any storage media used to store confidential data, such as hard disks, smart cards and HSMs, against unauthorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
Confidential data shall be protected to safeguard data integrity and confidentiality when stored, in use and when exchanged over networks. Confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data.

5.1.7. Waste disposal

The E-MSCA, and E-CP shall control waste disposal in such a way that the risk of compromise of confidential data is minimized. Information stored on digital media to be disposed shall be permanently destroyed using a secure data wiping with a specific tool for this purpose.

5.1.8. Off-site backup

In their CPSs, the E-MSCA and the E-CP shall consider the use of an off-site backup of all critical information, especially E-MSCA private keys and master keys, in order to ensure disaster recovery.

5.2. Procedural Controls

5.2.1. Trusted roles and the responsibilities of each role

In their Certification Practice Statement, the E-MSCA, and E-CP shall identify the trusted roles on which the security of the operations is dependent, as well as the responsibilities of each trusted role. These trusted roles shall be used in secure operating procedures. The trusted roles and the associated responsibilities shall be documented in job descriptions. These job descriptions shall be defined from the viewpoint of separation of duties and least privilege.
E-MSCA, and E-CP personnel shall be formally appointed to a trusted role by senior management of the respective organization.

5.2.2. Number of persons required per task

The E-MSCA, and E-CP shall identify in their CPSs which tasks are considered critical and consequently need multiple-person control. Such tasks shall at least include key pair generation, use or export of private keys and symmetric key import or export. For each critical task, the CPSs shall list the number of persons in a trusted role that are needed to carry out that task.

5.2.3. Identification and authentication for each role

The E-MSCA, and E-CP systems shall ensure effective user administration and access management. Access to critical systems shall be limited to individuals who are properly authorized and on a need-to-know basis. Access to information and applications shall be restricted, only allowing access to resources as necessary for carrying out the role allocated to a user.
All users shall be identified, authenticated and authorized by assignment of a role before using any systems.

5.2.4. Roles requiring separation of duties

No single person shall be allowed to simultaneously assume more than one of the trusted roles identified according to section 5.2.2 of this policy.
E-MSCA, and E-CP shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. E-MSCA, and E-CP shall ensure that the ISMS policies address personnel training, clearances and roles. E-MSCA, and E-CP ISMS implementations should conform to the requirements described in ISO 27001 [19].

5.3. Personnel Controls

5.3.1. Qualifications, experience, and clearance requirements

All personnel involved with the E-MSCA, and E-CP operations shall be properly trained and shall possess the knowledge, experience and qualifications necessary for the services offered and appropriate to the job function.
All personnel in trusted roles shall have appropriate background screening with positive result. Detailed clearance requirements for personnel in trusted roles shall be discussed in the E-MSCA, and E-CP CPSs.

5.3.2. Background check procedures

Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the CPSs. Personnel in trusted roles shall have no conflicts of interest that might prejudice the impartiality of the E-MSCA and E-CP operations.

5.3.3. Retraining frequency and requirements

Retraining of personnel shall take place at least in case of changes to documented policies, procedures, or operations.

5.3.4. Independent contractor requirements

Tasks may be outsourced to a specialized company, or personnel from independent contractors may be hired to carry out the responsibilities. However, in such cases the personnel controls defined in this section and in the CPS shall be maintained.
The E-MSCA, and E-CP shall retain responsibility for all aspects of the provision of their services as described in this policy, even if some functions are outsourced to subcontractors. Responsibilities of any subcontractors shall be clearly defined by the respective PKI participant and appropriate arrangements made to ensure that third parties are bound to implement any controls specified in this policy.

5.3.5. Documentation supplied to personnel

The E-MSCA, and E-CP shall provide their personnel with up-to-date versions of the documentation necessary for carrying out their role. In their E-MSCA, and E-CP CPSs, each of these parties shall identify the documentation to be provided to each role.

5.3.6. Training requirements

E-MSCA, and E-CP personnel training shall be managed according to a training plan described in the E-MSCA, and E-CP CPSs.

5.4. Audit logging procedures

All significant security events in E-MSCA and E-CP software shall be automatically time-stamped and recorded in the system log files. These include 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 interactions with the database(s) containing data on critical processes, including connection attempts and read, write and update or removal operations;
- Reception of key certification requests;
- Successful and failed attempts to process a key certification request and sign a certificate;
- 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 inside an HSM;
- Successful and failed attempts to import or export a private key to or from an HSM;
- Successful and failed attempts to change the life cycle state of any key pair;
- Successful and failed attempts to use a private 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 E-MSCA an E-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 reasonably 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

E-MSCA shall generate new E-MSCA key pairs as needed. After E-MSCA 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 component personalizers as described in the re-keying sections in chapter 4 of this policy.

The E-MSCA 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

5.7.1. Incident and compromise handling procedures

The E-MSCA and E-CP shall define security incidents and compromise handling procedures in a Security Incident Handling Procedure manual, which shall be issued to administrators and auditors.

The E-MSCA and E-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 E-MSCA and E-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 (E-MSCA_Card.SK) and / or symmetric master key ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$);
- loss of a private key (E-MSCA_Card.SK) and / or a symmetric master key ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$);
- IT hardware failure.

In the event of compromise or theft of an E-MSCA private key used to sign the public key certificates of tachograph cards (E-MSCA_Card.SK), the E-MSCA shall immediately inform the E-MSA, the affected component personalizers 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 E-MSCA, ($K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$), the E-MSCA shall immediately inform the E-MSA, the ERCA and the E-CP. All affected parties shall take appropriate measures within a reasonable period of time.

There is effectively no recovery from a loss of the E-MSCA 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. MSCA OR CP TERMINATION

In the event of termination of E-MSCA activity by the appointed organization, the E-MSA shall notify the EA and the ERCA of this and optionally inform the EA and ERCA about the newly appointed E-MSCA.

If E-CP terminates its activities, the E-MSA shall be notified and optionally the E-MSA informs the EA and ERCA.

The E-MSA shall ensure that at least one card personalizer is operational at all times. The E-MSA informs the ERCA about the newly appointed card personalizer.

The E-MSA shall ensure that at least one E-MSCA is operational at all times.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

The E-MSCA and the E-CP shall generate private keys in accordance with Annex 1C 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 E-MSCA shall have available a Test E-MSCA system for interoperability test purposes, according to the Regulation. The Test E-MSCA system shall be a separate system and shall have its own E-MSCA private keys and symmetric master keys. The Test E-MSCA 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 E-MSCA shall also be able to sign test equipment certificates on request of the E-CP and to distribute symmetric test keys and encrypted data for motion sensors to the E-CP.

6.2. Private and symmetric key protection and cryptographic module engineering controls

The E-MSCA and the E-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 E-MSA certificate policy contains various functional requirements for the trustworthy dedicated device used in the E-MSCA 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 E-MSCA, component manufacturers and card personalizers’ 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 E-MSCA, component manufacturers and card personalizers’ private keys and the symmetric keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual person control in a physically secured environment.

Back-up copies of the E-MSCA, component manufacturers and card personalizers’ 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 E-MSCA 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 E-MSCA, export of KM-VU and KM-WC in encrypted form is allowed in response to a valid key distribution request from the E-CP by personnel in trusted roles under at least dual person control.

At the end of the life cycle of an E-MSCA private key or of a symmetric master key (as specified in the E-MSCA 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 E-MSCA public key certificates and hence the public keys shall be archived indefinitely.

The validity periods of all E-MSCA certificates shall comply with Annex 1C Appendix 1.

In accordance with Annex 1C Appendix 11, the private key usage period of E-MSCA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate. The E-MSCA shall not use a private key after the private key usage period is over.

6.4. Activation data

E-MSCA 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 E-MSCA software itself, user authentication shall take place using proper means (e.g. by a passphrase).

6.5. Computer security controls

The E-MSCA, and the E-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 E-MSCA and the E-CP shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built into 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 E-MSCA and the E-CP shall devise and implement its network 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 component manufacturers and card personalizers can be effectively controlled.

6.8. TIMESTAMPING

The time and date of an event shall be included in every audit trail entry. The E-MSCA CPS and the related documentation / CPS of the E-CP 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 1C, 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	'7F4E'	var	
Certificate Profile Identifier	m	CPI	'5F 29'	'01'	INTEGER (0…255)
Certification Authority Reference	m	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorization	m	CHA	'5F4C'	'07'	CertificateHolderAuthorization
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 6 Certificate profile

The algorithm is indicated via the Standardized Domain Parameters OID as specified in Table 1 of Appendix 11, Annex 1C of the Commission Implementing Regulation (EU) 2016/799, amended by the European Commission in 2018. 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
Brainpool P384r1	brainpoolP384r1	1.3.36.3.3.2.8.1.1.11
Brainpool P512r1	brainpoolP512r1	1.3.36.3.3.2.8.1.1.13
NIST P-521	Secp521r1	1.3.132.0.35

Table 7 Allowed Standardized Domain Parameters OIDs

7.2. CRL Profile

No CRL shall be published.

7.3. OCSP Profile

No OCSP shall be used.

8. Compliance Audit and Other Assessment

8.1. Frequency or Circumstances of Assessment

The first full and formal audit on the E-MSCA and the E-CP operation shall be performed within 12 months of the start of the operations covered by the E-MSA certificate policy. The E-MSA may also order a compliance audit by an auditor at any time at its discretion.

The E-MSCA and the E-CP audits shall establish whether the requirements on the E-MSA described in this document are being maintained.

If an audit finds no evidence of non-conformity, the next audit shall be performed within 24 months. If an audit finds evidence of non-conformity, a follow-up audit shall be performed within 12 months to verify that the non-conformities have been solved.

Before the start of the operations covered by the E-MSA certificate policy, the E-MSA shall carry out a pre-operational assessment to obtain evidence that the E-MSCA and the E-CP organizations are able to operate in conformance to the requirements in the E-MSA certificate policy.

8.2. Identity/Qualifications of Assessor

The audit shall be performed by an independent auditor.

Any person selected or proposed to perform the E-CIA, E-MSCA and E-CP compliance audit shall first be approved by the E-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, confidentiality regarding their relationship to the organization to be audited 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 information technologies, PKI and the related technical norms and standards.

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 organization being the subject of the audit.

8.4. Topics Covered by Assessment

The audit of the E-MSCA or the E-CP shall cover compliance to the ERCA policy, the E-MSA certificate policy, the E-MSCA CPS and the CPS or similar documents from the E-CP for Gen 2 Smart Tachographs as well as associated procedures and techniques documented by the E-MSCA or the E-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.

By assessment of the audit logs it shall be determined whether weaknesses are present in the security of E-MSCA or the E-CP systems. Determined (possible) weaknesses shall be mitigated. The assessment and possible weaknesses shall be recorded.

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 E-MSCA or the E-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 Spanish and English language to the audited entity (E-MSCA or the E-CP) and the E-MSA. The E-MSA shall send an audit report in English for the E-MSCA 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 E-MSA shall send the full results of the compliance audits of all requested entities to the ERCA.

9. Other Business and Legal Matters

9.1. Fees

No stipulation.

9.2. Financial Responsibility

The E-MSCA and E-CP shall have adequate arrangements to cover liabilities arising from their operations and/or activities.

No other stipulation.

9.3. Confidentiality of Business Information

Confidential data shall comprehend at least:

- Private keys;
- Symmetric master keys;
- Audit logs;
- Detailed documentation regarding the PKI management;

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

Certificates are not considered to be confidential.

Identification information or other personal or corporate information appearing on cards and in certificates is not considered to be confidential, unless statutes or special agreements so dictate.

9.4. Privacy of Personal Information

The E-MSCA and E-CP shall treat all personal information, especially information provided by Card Holders in the course of their application for a tachograph card, according to the General Data Protection Regulation 679/2016. Appropriate technical and organizational measures shall be taken to prevent unauthorized or unlawful processing of personal data and to prevent accidental loss or destruction of, or damage to, personal data.

Personally identifiable information, contact information, and authorizations of E-MSCA and E-CP staff are private.

Personally identifiable or corporate information and contact information of Card Holders that does not appear in a certificate issued by the E-MSCA, is private.

9.5. Intellectual Property Rights

No stipulation.

9.6. Representations and Warranties

The E-MSCA organization guarantees that the E-MSCA shall operate according to ERCA CP, E-MSA CP and the E-MSCA CPS.

9.7. Disclaimers and Warranties

E-MSCA 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 disclaim any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

9.8. Limitations of Liability

Spain 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 E-MSCA, and use of certificates beyond the prescribed use defined by this Certificate Policy and the E-MSCA CPS;
- caused by fraudulent or negligent use of certificates and/or certificate status information issued by the E-MSCA.

Spain 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 E-MSCA, or its associated public/private key pair, used by a subscriber or relying party;
- any symmetric key distributed by the E-MSCA, used by a subscriber or relying party;

Issuance of certificates, symmetric keys and encryption services by the E-MSCA does not make Spain or the E-MSCA 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 E-MSCA is not an intermediary to transactions between subscribers and relying parties. Claims against the E-MSCA are limited to showing that it operated in a manner inconsistent with this certificate policy and the E-MSCA CPS.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

E-MSA Certificate Policy is valid from the moment the E-MSCA becomes operational. It shall be valid until further notice.

The validity of this CP ends when the E-MSCA stops operating or when the E-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 Ministerio de Transportes, Movilidad y Agenda Urbana.

Notice of severance or merger may result in changes to the scope, management and/or operation of the E-MSCA. In such an event, this E-MSA certificate policy and the E-MSCA 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 E-MSA. The E-MSA may revise this CP if it deems this necessary. It is allowed to make editorial or typographical corrections to this policy without notification without an increase in version number.

For all other changes of this CP, the procedure for change proposals and approvals shall be as follows:

1. Comments or requests for changes to the CP shall be directed to the E-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.
2. The E-MSCA shall accept, accept with modifications, or reject the comment or proposed change after completion of the comment period. EMSCA disposition of proposed changes are reviewed by the E-MSA. Decisions with respect to the proposed changes are at the discretion of the E-MSCA and the E MSA.
3. A new version of this CP will be published on the E-MSA website and distributed to the ERCA.

9.13. Dispute Resolution Procedures

The E-CIA, E-MSCA and E-CP shall have policies and procedures for the resolution of complaints and disputes received from Card Holders or other parties about the provisioning of their services as described in this MSA certificate policy.

Any dispute related to key and certificate management between the E-MSA, E-MSCA, service agencies and equipment manufacturers 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 E-MSA.

9.14. Governing Law

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

9.15. Compliance with Applicable Law

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 [2] of the European Parliament and of the Council and with Commission Implementing Regulation (EU) 799/2016 [3], amended Commission Implementing Regulation (EU) 502/2018. 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. Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy, version 1.0, June 2018 [1]
2. 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]
3. Commission Implementing Regulation (EU) 799/2016, amended by the European Commission in 2018, Official Journal of the European Union L 139 [3]
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 [4]
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997 [5]
6. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0, June 2018 [6]
7. Smart Tachograph - Equipment Interoperability Test Specification, JRC, version 1.0, July 2018 [7]
8. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28 [8]
9. ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition, 2006-05-01 [9]
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 [10]
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 [11]
12. CEN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services [12]
13. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15 [13]
14. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001 [14]
15. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013 [15]
16. 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]
17. ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher. Third edition, 2006-02-01 [17]
18. 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]
19. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01 [19]
20. Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission, Adopted 29/05/2009 [20]
21. Commission Decision 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission [21]