Ministero dello Sviluppo Economico

Smart Tachograph
Italian MSA Policy
v.1.1

Amendment History

Version Control	Issue Date	Status
Version 0.9	March 2019	Draft
Version 0.9.1	5th April 2019	Draft, after 29th March ERCA Review
Version 0.9.2	10th May 2019	Draft, after 7h May ERCA Review Approved by the European Authority
Version 1.0	15th May 2019	Final version conforming v.0.9.2
Version 1.1	8th September 2020	Revised version, with amendments in: 1.5 – Policy Administration 2.1 – Repository

Table of Contents

1 Introduction

1.1 Overview

The second generation Digital Tachograph system (Smart Tachograph) has been introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council [1].

The Commission Implementing Regulation (EU) 2016/799 (Annex 1C) [2] lays down the technical requirements for the construction, testing, installation, operation and repair of Smart Tachographs and their components.

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.

The ERCA issues certificates to Member State Certification Authorities (MSCAs) and distributes symmetric master keys to the MSCAs.

The MSCAs are responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment.

This document forms the Italian Policy (I-MSA) for the Smart Tachograph system (second-generation), complying with requirements laid down in the ERCA Policy [5], in which are outlined roles and responsibilities within the tachograph Card Issuing system, more specifically referring to the entities managing keys and certificates: the Certification Authority and the Component Personaliser.

This I-MSA policy refers to Part B of Appendix 11, which affects elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems, used to realise the second-generation tachograph system.

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

1.2 Document Name and Identification

This document is named Smart Tachograph Italian MSA Policy.

This Policy does not have an ASN.1 object identifier, as the certificates used in the Smart Tachograph system do not contain a reference to this policy.

1.3 Participants

The participant within the Smart Tachograph PKI and Symmetric Key Infrastructure, and the exchanges between them are represented in Figure 1.

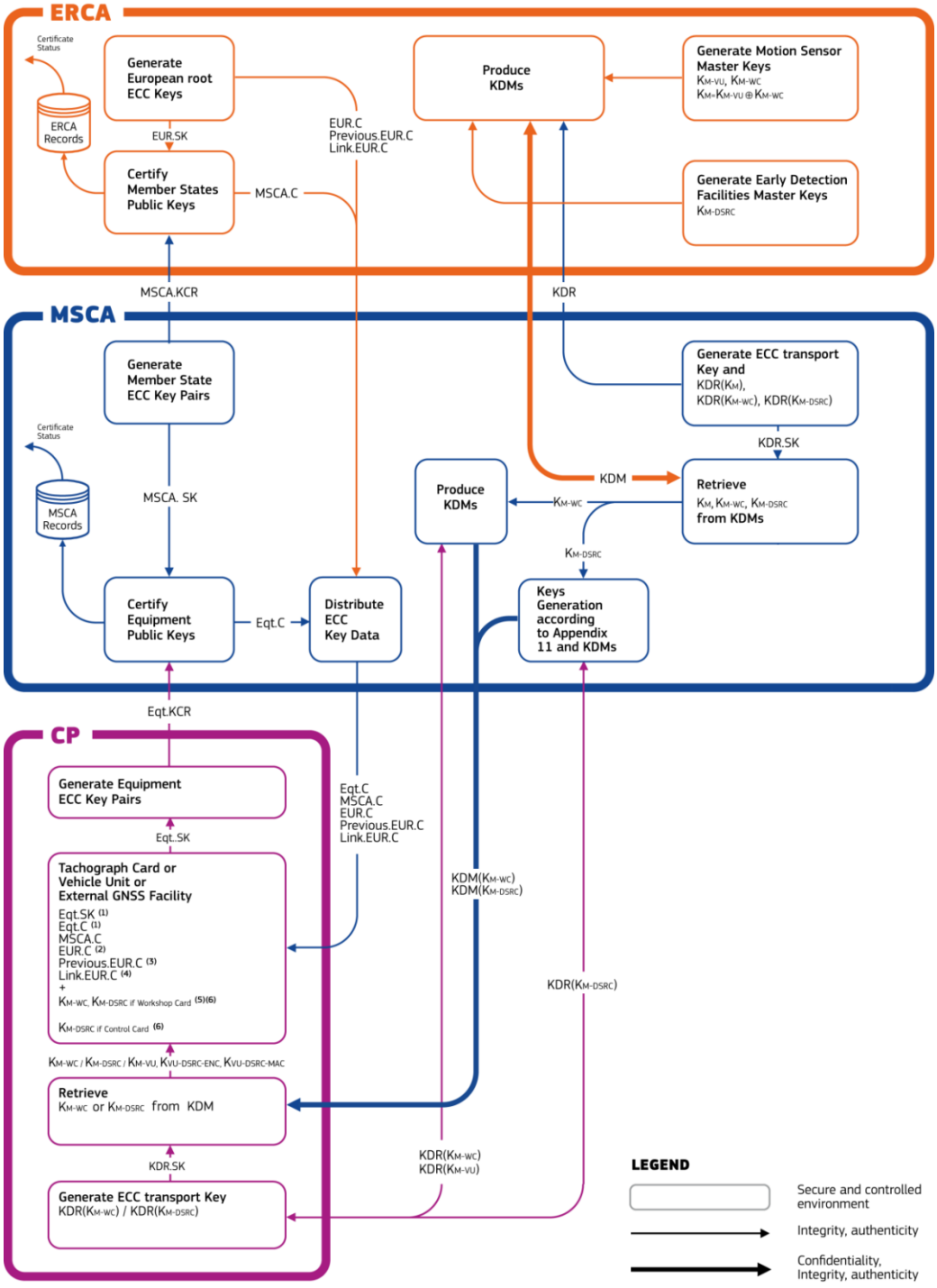

Figure 1 Description of Annex I(C) key management

Notes

1. For Tachograph Cards there are two certificates and relative keys, one for 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 on note 2 and 3, if existing.
5. All Km-wc keys associated to Km-vu keys currently in circulation have to be inserted.
6. All Km-dsrc keys currently in circulation have to be inserted.

With reference to the ERCA Policy ([5] section 1.3), key management services for the following stakeholders are outside the scope of this policy:

- Motion Sensor manufacturers
- Vehicle Unit manufacturers
- External GNSS Facility manufacturers

1.3.1 Certification Authority

1.3.1.1 ERCA

The 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.

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

The ERCA is also the entity generating, managing and distributing on request the symmetric master keys, i.e. the Motion Sensor Master Key–VU part (Km-vu), the Motion Sensor Master Key-Workshop Card part (Km-wc) and the DSRC Master Key (Kdsrc).

1.3.1.2 MSCA

The Italian Certification Authority (I-MSCA) operates as sub-CA under the ERCA, signing public key certificates for tachograph Cards.

Functional Role of the I-MSCA

The I-MSCA shall manage the following main functional tasks:

- Provide the ERCA with Certificate Signing Requests and Key Distribution Requests and obtain the I-MSCA Certificates and the symmetric keys required to operate the system as National Certification Authority.
- Receive by the I-CP the Key Distribution Requests, required for Card personalization.
- Provide the I-CP with Key Distribution Messages containing the symmetric keys, required for Card personalization.
- Receive by the I-CIA the Certificate requests. originated by the I-CP
- Disseminate the certificates to the I-CIA.

The I-MSCA receives the Card certificate requests, originated by the Component Personaliser (I-CP) and coupled to the Card owner by the Card Issuing Authority body (I-CIA), and generates the corresponding Card certificates, for dissemination.

The I-MSCA is responsible for the issuance of tachograph Card certificates, and as such it can be referred as an MSCA_Card, following the ERCA naming convention ([5] section 1.3.1.2).

The I-MSCA is also responsible for requesting the symmetric master keys from the ERCA. Km-wc and Kdsrc symmetric keys are distributed by the I-MSCA to the Card Personaliser, for Card personalization.

When a cooperation administrative arrangement exists between Italy and another State, the I-MSCA is authorised by the I-MSA to request the national keys on behalf of this other State to the ERCA. The two productions shall be logically separated.

Vehicle Unit (VU) and External GNSS Facilities (EGF) Certificates, namely MSCA_VU and MSCA-EGF, are out of scope of this policy.

1.3.2 Registration Authorities

Within the Smart Tachograph system, the final users are identified and registered through the Card Issuing Authority (I-CIA). The I-CIA ensures that correct and relevant user information from the application process is input to the I-MSCA and I-CP.

Functional Role of the I-CIA

The I-CIA shall manage the following main functional tasks:

- Identification of Card holders.
- Registration of Card applications.
- Request for Card Certificates to the I-MSCA.
- Dissemination of Card holders' personal data and Certificates to the I-CP.
- Handle personalized Cards, received by the I-CP, to the Cards holders.

1.3.3 Subscribers

1.3.3.1 Component Personaliser

The only subscribers to the I-MSCA public key certification service are the component personalisers. The Italian Component personaliser (I-CP) is responsible for the personalisation of the four different Tachograph Card's types, foreseen by the EU Regulation: driver cards, company cards, workshop cards and control cards.

Functional Role of the I-CP

The I-CP shall manage the following main functional tasks:

- Provide the I-MSCA with Key Distribution Requests (KDR) to obtain the symmetric keys, required for Card personalization.
- Receive by the I-MSCA the Key Distribution Messages (KDM) containing the symmetric keys, required for Card personalization.
- Send to the I-CIA the cryptographic data and corresponding private keys' proof of possession, needed for the Certificate request.
- Receive by the I-CIA the Cards' certificates and personal data required for Card personalization.
- Return to the I-CIA the personalized Cards.

The driver cards and workshop cards have two key pairs and corresponding certificates issued by the I-MSCA, 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 Km-wc and Kdsrc symmetric keys.

The company and control cards have a key pair and corresponding certificate issued by the I-MSCA for mutual authentication.

The control cards also contain Kdsrc.

The I-CP is responsible for ensuring the equipment is provided with the appropriate keys and certificates.

The I-CP, 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 I-MSCA;
- performs the application for Km-wc and Kdsrc (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).

The I-CP, for company and control cards;

- ensures generation of the card key pair for mutual authentication;
- performs the certificate application process with the I-MSCA;
- performs the application of Kdsrc (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).

When a cooperation administrative arrangement exists between Italy and another State, the I-CP is authorised by the I-MSA to perform personalization services for the CIA of this State.

1.3.4 Relying parties

Parties relying on the ERCA public key certification service are primarily the national authorities tasked with enforcing the rules and regulations regarding driving times and rest periods, who use the ERCA certificates to validate the authenticity of MSCA certificates.

MSCA certificates are then used to validate the authenticity of equipment certificates, which in turn are used to validate the authenticity of data downloaded from Vehicle Units and driver cards.

Other relying parties are drivers, companies, workshops and control officers.

1.4 Key and Certificate Usage

In conformity with the requirements laid down in the ERCA Policy ([5] section 1.4), the I-MSA recognises the ERCA public key certificates as the highest trust point for the PKI.

Keys and certificates generated by the I-MSCA shall be used only within the Tachograph system. In particular I-MSCA private keys shall be used only for:

- Signing of certificate signing requests (see section 4.1.1).
- Signing of equipment certificates, in accordance with Annex IC Appendix 11 [2].

The I-MSCA shall not use the symmetric master keys for any purpose except distribution to the I-CP.

The I-MSCA shall communicate the symmetric master keys to the I-CP by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11 [2].

The I-MSCA Card certificates shall be used to verify card certificates issued by the I-MSCA.

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.

Km-wc shall be provided by the I-MSCA to the component personaliser I-CP for the sole purpose of insertion into the Workshop Cards.

Kdsrc shall be provided by the I-MSCA to the component personaliser I-CP for the sole purpose of insertion into the Workshop and Control Cards.

1.5 Policy Administration

The organization responsible for the drafting, registering, maintaining, and updating of this policy is the Italian Tachograph Member State Authority I-MSA, appointed by national decree - Decreto Ministeriale 2003, 31st of October, n.361 - issued by the former Ministry Ministero delle Attività Produttive[1], is:

Ministero dello Sviluppo Economico
Direzione generale per il mercato, la concorrenza, la tutela del consumatore e la normativa tecnica
Div. VIII - Strumenti di misura e metalli preziosi
Via Sallustiana, 53 - 00187 Roma
Italy

The I-MSA policy, this document, complies with all applicable ERCA Policy requirements ([5] section 1.5.3), following the framework for certificate policies described in RFC 3647 [4].

Questions concerning this I-MSA policy shall be forwarded to the following address: dgmccnt.div08@pec.mise.gov.it

The Card Issuing Authorities (I-CIAs) are the Italian Chambers of Commerce, (Camere di Commercio, Industria, Artigianato e Agricoltura) appointed by the

[1]The “Ministero dello Sviluppo Economico” was formerly known as “Ministero delle Attività Produttive” before 2006.

national decree - Decreto Ministeriale 2003, 31st of October, n.361 - issued by the former Ministero delle Attività Produttive.

The Certification Authority(I-MSCA) and Card Personalizer (I-CP), appointed by the national decree – Decreto Ministeriale 2005, 23rd of June - issued by the former Ministero delle Attività Produttive, is:

InfoCamere S.C.p.A.
Corso Stati Uniti, 14 - 35127 Padova
Italy

The I-MSCA or I-CP may subcontract parts of its processes to subcontractors, Service Agencies. The use of Service Agencies in no way diminishes the I-MSCA's or I-CP's overall responsibilities.

I-MSCA and I-CP shall respectively document their implementation of this policy in a Practice Statement, a procedural document, which details how the I-MSA certificate policy is enforced in day-to-day management.

The I-MSCA_PS and I-CP_PS shall not be public, but treated as restricted information, and shall be communicated to the relevant parties only on request, on a need to know basis.

The I-MSA shall be responsible to determine whether the The I-MSCA_PS and I-CP_PS comply with this I-MSA CP.

1.6 Definitions and Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certification Authority
Card_MA	key pair and certificate for mutual authentication
Card_Sign	key pair and certificate for signing
CIA	Card Issuing Authority
CP	Component Personaliser
CP	Certificate Policy
CPA	Competent Party Authority
CPS	Certification Practice Statement
DSRC	Dedicated Short Range Communication
CSR	Certificate Signing Request
EC	Elliptic Curve
EC	European Commission
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman (key agreement algorithm)
ECDSA	Elliptic Curve Digital Signature Algorithm
Equipment	Tachograph Cards
EGF	External GNSS Facility
EA	European Authority
ERCA	European Root Certification Authority
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISSO	Information System Security Officer
JRC	Joint Research Centre
KDR	Key Distribution Request
KDM	Key Distribution Message
KM	Motion Sensor Master Key
Km-vu	VU part of KM
Km-wc	WC part of KM
KID	Motion Sensor Identification Key
KP	Motion Sensor Pairing Key
Kdsrc	DSRC Master Key
MA	Mutual Authentication
MoS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
NCP	Normalised Certificate Policy
PKI	Public Key Infrastructure
RFC	Request For Comment
VU	Vehicle Unit
WC	Workshop Card

2 Publication and Repository Responsibilities

2.1 Repository

The I-MSA shall be responsible for the public website[2] which shall be the repository for this I-MSA policy.

The I-MSCA shall be responsible for storing all issued equipment certificates in a non-public repository.

2.2 Publication of Certification Information

The status information shall be maintained and made available by the I-CIA at Tachograph equipment level.

2.3 Time or frequency of Publication

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

Changes to the Practices Statements shall not be public, but shall only be communicated to the relevant parties. Distribution policies for changes to the PSs shall be determined in the relevant documents.

2.4 Access Controls on Repositories

The I-MSCA and I-CP shall designate staff having write or modify access to the information in the respective Practices Statements.

3 Identification and Authentication

3.1 Naming

3.1.1 Certificate subject and issuer

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

Entity	Identifier	Construction
MSCA	Certification Authority Key Identifier (KID)	NationNumeric ('1A') NumericAlpha ('49 20 20')

[2] https://www.mise.gov.it/index.php/it/mercato-e-consumatori/normativa-tecnica/metrologia/tachigrafi

Entity	Identifier	Construction
		KeySerialNumber (1 byte) AdditionalInfo ('4E 47') CA Identifier (’01’)
Equipment	Certificate Holder Reference (KID)	CardSerialNumber (4 bytes) MonthAndYear (2 bytes) EquipmentType (1 byte) ManufacturerCode (1 byte)

Table 1 Identifiers for certificate issuers and subjects

3.1.2 Key Distribution Requests

Key Distribution Requests and Key Distribution Messages identify the master key that is requested and distributed, see section 4.2.1.

3.2 Initial Identity Validation

3.2.1 Method to Prove possession of Private Key

The certificate signing requests (CSRs), submitted by the I-MSCA to the ERCA, shall prove possession of the corresponding private key, in the form specified in the ERCA policy ([5] section 4.1.1).

The certificate signing requests (CSRs), submitted by the I-CP to the I-MSCA, shall prove possession of the corresponding private key, as specified in section 4.1.1 of this document.

3.2.2 Authentication of Organization Identity

The I-MSCA shall define a procedure for the authentication of organization identities in its own Certification Practice Statement.

3.2.3 Authentication of Individual Identity

The I-MSCA shall define a procedure for the authentication of individual identities in its own Certification Practice Statement.

3.2.4 Validation of Authority

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

3.2.5 Criteria for interoperation

The I-MSCA shall not rely on any external certificate authority for the certificate signing and key distribution services provided to the smart tachograph system.

3.3 Identification and Authentication for Re-key Requests

Not applicable; the I-CIA shall guarantee that issuing of replacement cards take place according to the requirements in EU Regulation 165/2014 [1].

3.4 Identification and Authentication for Revocation Requests

Not applicable (see section 4.1.10)

The Tachograph Card's Application is handled by the I-CIA, responsible for identification of final users.

4 Certificate Life-Cycle Operational Requirements

This chapter specifies the message formats, cryptographic mechanisms and procedures for the application and distribution of *equipment certificates and symmetric keys for cards*. The cryptographic strength of the security mechanisms shall be at least as strong as the strength of the transported keys and encrypted data.

4.1 Certificate Application and Issuance

4.1.1 Certificate Signing Requests

The I-CP shall ensure that the input data from the I-CIA contains information which renders the Certificate Holder Reference (CHR) unique.

The public key to be certified is extracted from the key generation process.

Certificate Signing Requests (CSR) which the I-CP shall forward to the I-MSCA shall be in TLV-format. The following table shows the certification request encoding, including all tags. For the lengths, the DER encoding rules specified in [8] shall be used.

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
Authentication			
ECC (CV) Certificate	7F 21	var	
Certificate Body	7F 4E	var	
Certificate Profile Identifier	5F 29	01	INTEGER (0.. 255)
Certification Authority Reference	42	08	KeyIdentifer
Certificate Holder Authorisation	5F 4C	07	Certificate Holder Authorisation
Public Key	7F 49	var	
Standardised Domain Parameters OID	06	var	OBJECT IDENTIFIER
Public Point	86	var	OCTET STRING
Certificate Holder Reference	5F 20	08	KeyIdentifer
Certificate Effective Date	5F 25	04	TimeReal

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
Authentication			
Certificate Expiry Date	5F 24	04	TimeReal
ECC Signature	5F 37	var	OCTET STRING

Table 2 Certificate signing request format

The **Certificate Profile Identifier** identifies the version of the profile; its value shall be '00'.

The **Certification Authority Reference** shall have the same value as the *Certificate Holder Reference*. In the issued certificate the field shall contain the Certification Key Identifier of the I-MSCA Member State Key which signed the certificate.

The **Certificate Holder Authorisation** shall be used to identify the type of the requested 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 ([2] Annex 1C, Appendix 11, CSM_141).

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

- The **Domain Parameters** data object shall reference the standardised 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 [2].
- The **Public Point** data object shall contain the public point. Elliptic curve public points shall be converted to octet strings as specified in [6]. The uncompressed encoding format shall be used ([2] Annex 1C, Appendix 11, CSM_143).

The **Certificate Holder Reference** shall identify the public key contained in the request and in the resulting certificate.

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.

The **Signature** shall be verifiable with the public key contained in the CSR. The signature shall be created over the value of the *Certificate Holder Reference* field, without tag and lenght (8 bytes). The signature algorithm shall be ECDSA, as specified in [11], using the hashing algorithm linked to the size of the *Public Key* field ([2] Annex 1C, Appendix 11, CSM_50). The signature format shall be plain, as specified in [6].

4.1.2 Certificate Application Processing

For each CSR it receives, the I-MSCA shall verify that:

- the Certificate Holder Reference is unique within its domain;

- the domain parameters specified in the request are listed in Table 1 of Annex 1C, Appendix 11 [2], 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 I-MSCA previously;
- the public point in the request is on the curve indicated in the request;
- the Certificate Effective Date is not precedent to the time of certificate issuing;
- the Certificate Expiration Date does not exceed the proper validity period;
- the signature can be verified using the public point and the domain parameters indicated in the request. This proves that the I-CP is in possession of the private key associated with the public key;

If any of these checks fails, the I-MSCA shall reject the CSR.

Driver certificates are issued only to successful applicants for a Driver card (section 4.3).

Workshop certificates are issued only to successful applicants for a Workshop card (section 4.3).

Control body certificates are issued only to successful applicants for a Control card (section 4.3).

Hauling company certificates are issued only to successful applicants for a Company card (section 4.3).

Vehicle unit certificates are out of the scope of this Policy.

4.1.3 Certificate issuance

If all checks succeed, the I-MSCA shall proceed to create, within the same device used to store the MS Private keys, the signature over the encoded certificate body, including the certificate body tag and length.

The signature algorithm shall be ECDSA, as specified in [11], using the hashing algorithm linked to the key size of the signing authority ([2] Annex 1C, Appendix 11, CSM_50). The signature format shall be plain, as specified in [6].

The format of the issued certificates can be found in section 7.1.

The following information shall be recorded in the I-MSCA database for each CSR received:

- the complete CSR;
- the complete resulting certificate, if any;
- the standardised domain parameters OID and the hash over the public point of the certified public key;
- the certificate effective date and certificate expiration date;
- the Certificate Holder Reference (for identification of the public key);
- the time at which the certificates has been issued.

The I-MSCA shall export all certificate data to the I-CIA register so that certificates, equipment and users are linked together.

4.1.4 Exchange of Requests and Responses

For transportation of certificate signing requests and certificates between the ERCA and I-MSCA, CD-R media shall be used. Requests and certificates shall be accompanied by a paper copy of the data. The I-MSCA shall respect the medias' format as described in the ERCA Policy ([5] section 4.1.4).

For transportation of certificate signing requests and issued certificates, between the I-MSCA and I-CP signed messages in XML format shall be used.

Beside the issued certificate, the XML response message should contain:

- the I-MSCA certificate to be used for verification of the issued certificates.
- the EUR certificate to be used for verification of the I-MSCA certificate.
- the EUR certificate whose validity period directly precedes the validity period of the EUR certificate to be used to verify the I-MSCA certificate, if existing.
- the link certificate linking these two EUR certificates, if existing.

For testing purposes, the I-MSCA shall accept and dispatch CSRs and certificates as e-mail attachments.

4.1.5 Certificate Acceptance

Upon reception of the MSCA certificates, issued by the ERCA, the I-MSCA shall perform the check procedure required in the ERCA Policy [(5) section 4.1.5].

Before to load the certificates into Tachograph Cards, a validation of the Certificates' chain should be performed by the I-CP; the I-CP should:

- verify the issued certificate using the I-MSCA certificate;
- verify the I-MSCA certificate using the EUR certificate;
- verify the EUR certificate using the link certificate, if present;
- verify the link certificate using the precedent EUR certificate, if present;

If any of these checks fails, the I-CP shall reject the issued certificate and communicate the certificate rejection to the I-MSCA.

4.1.6 Key Pair and Certificate Usage

Key pairs generated by the I-CP shall be used only within the Tachograph system, in particular:

- the Card_Sign private key may only be used to sign data downloaded from the card.
- the Card_MA private key shall be used exclusively to perform mutual authentication and session key agreement towards vehicle units.

Certificates issued by the I-MSCA shall be used only within the Tachograph system, in particular:

- the Card_MA certificate shall be used for mutual authentication and session key agreement between Card and VU.

- the Card_Sign certificate shall be used to verify the authenticity and integrity of data downloaded from the card.

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

Not applicable; the I-CIA shall guarantee that issuing of replacement cards take place according to the requirements in EU Regulation 165/2014 [1].

4.1.9 Certificate Modification

Certificate modification is not allowed.

4.1.10 Certificate Revocation and Suspension

Certificates are not revoked or suspended. Non-valid Tachograph equipment are put in a "black list".

4.1.10.1 Special requirements concerning key compromise

If the I-MSCA detects or is notified of the compromise or suspected compromise of an I-MSCA private key, the I-MSCA shall notify this to the ERCA and the I-MSA without unnecessary delay and at least within 8 hours of detection.

The notification shall indicate the circumstances under which the compromise occurred. The outcome of any follow-up investigation and potential action by the I-MSA and/or the I-MSCA shall be reported to the ERCA.

4.1.11 Certificate Status Services

Status information shall apply at Tachograph equipment level. Card Status Services shall be provided by the I-CIA (see section 2.2).

4.1.12 End of Subscription

In case the I-MSA decides for MSA termination, such a change shall be notified to the ERCA by the MSA as a change to the MSA certificate policy.

In case of subscription ending, the I-MSA shall take the decision whether to submit a certificate revocation request for any valid I_MSCA certificate or to allow all I_MSCA certificate to expire.

4.1.13 Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that equipment private keys shall be neither escrowed nor exported to or stored in any system apart from the I-CP systems.

4.2 Master Key Application and Distribution

The I-MSCA shall, as needed, request and obtain motion sensor master key Km-wc and DSRC master key Kdsrc, from the ERCA according to the master key distribution protocol described in ERCA Policy ([5] sections 4.2.1 – 4.2.6).

The I-MSCA shall forward the motion sensor master key Km-wc to the I-CP for the sole purpose of insertion into the Workshop cards.

The I-MSCA shall forward the DSRC master key Kdsrc to the I-CP for the sole purpose of insertion into the Workshop and Control cards.

The I-CP shall undertake the I-MSCA's task to ensure that the motion sensor master key Km-wc is inserted into all issued Workshop cards.

The I-CP shall undertake the I-MSCA's task to ensure that the DSRC master key Kdsrc is inserted into all issued Workshop and Control cards.

4.2.1 Key Distribution Requests

Key Distribution Requests (KDR) which the I-CP shall forward to the I-MSCA shall be in TLV-format. The following table shows the KDR encoding, including all tags. For the lengths, the DER encoding rules specified in [8] shall be used.

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
Key Distribution Request	A1	var	
Request Profile Identifier	5F 29	01	INTEGER (0.. 255)
Message Recipient Authorisation	83	08	Message Recipient Authorisation
RSA Public Key	7F 49	var	
Module	81	var	OCTET STRING
Public Exponent	82	var	OCTET STRING

Table 3 Key distribution request format

The **Request Profile Identifier** identifies the version of the profile; its value shall be '00' for version 1.

The **Message Recipient Authorisation** shall be used to identify the master 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 (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:

- '27': Km-wc, motion sensor master key workshop part,
- '09': Kdsrc, DSRC master key.

RSA Public Key nests two data elements:

- the data element **Module** shall contain the module of the RSA key pair to be used for ciphering the distributed master key,
- the data element **Public Exponent** shall contain the public exponent of the RSA key pair to be used for ciphering the distributed master key.

4.2.2 Master Key Application Processing

4.2.2.1 Verification of KDR contents

The KDR originated by the I-CP to the I-MSCA shall comply with the encoding format described in section 4.2.1.

Checks for correctness, completeness and authorisation shall be performed manually and in an automated way by the I-MSCA officers.

For each KDR it receives from the I-CP, the I-MSCA shall verify that:

- the transport media is readable; i.e. not damaged or corrupted;
- the KDR format complies with Table 3;
- the request is provided by duly authorised I-CP personnel;
- the requested master key type shall be Km-wc or Kdsrc;
- the module specified in the request shall have a strength that matches the length of the requested symmetric key, according to the NIST comparable algorithm strengths recommendation.[3]

4.2.2.2 The KDM generation, distribution and administration

If all checks succeed, the I-MSCA shall provide the I-CP with the key distribution message (KDM) by determining the symmetric key requested by the I-CP and following the rules described in sections 4.2.3 - 4.2.5.

4.2.3 Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys distributed by the ERCA to the I-MSCA shall be protected via an Elliptic Curve Integrated Encryption Scheme (ECIES). The I-MSCA shall manage the ephemeral keys as foreseen in the ERCA Policy ([5] section 4,2,3 Step 1).

The confidentiality and authenticity of symmetric keys distributed by the I-MSCA to the I-CP shall be guaranteed via the RSAES-PKCS1-v1_5 encryption schema [14].

[3] NIST Special Publication 800-57 Part 1 Rev.4 – Recommendation for Key Management- Section 5.6.1.

4.2.4 Key Distribution Messages

After performing the Master Key application processing (see section 4.2.2), the I-MSCA shall construct a key distribution message as shown in the following table. For the lengths, the DER encoding rules specified in [8] shall be used.

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
Key Distribution	A1	var	
Request Profile Identifier	5F 29	01	INTEGER (0.. 255)
Message Recipient Authorisation	83	08	Message Recipient Authorisation
Encrypted Key Value	87	var	OCTET STRING

Table 4 Key distribution message

The **Request Profile Identifier** identifies the version of the profile; its value shall be '00'.

The **Message Recipient Authorisation** shall be used to identify the distributed symmetric key. 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 the distributed master key (1 byte),
- the version number of the distributed master key (1 byte).

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

- '27': Km-wc, motion sensor master key workshop part
- '09': Kdsrc, DSRC master key

Encrypted Key Value shall contain the encrypted master key value. Encryption shall be performed using the RSAES-PKCS1-v1_5 encryption schema [14] with the RSA Public Key contained in the related Key Distribution Request.

4.2.5 Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages between the ERCA and I-MSCA, CD-R media shall be used. Requests and certificates shall be accompanied by a paper copy of the data. The I-MSCA shall respect the medias' format as described in the ERCA Policy ([5] section 4.2.5).

For transportation of key distribution requests and key distribution messages between the I-MSCA and the I-CP, 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 I-MSCA.

The key distribution request and message shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) or 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 I-MSCA CPS.

For both KDRs and KDMs, the transport media and the printouts shall be handed over between an I-MSCA employee and the authorised I-CP personnel in the I-MSCA controlled area.

4.2.6 Master Key Acceptance

Upon reception of the key distribution message at the I-MSCA premises, the I-MSCA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with the ERCA Policy requirements ([5] Table 4);
- the message is not corrupted; the I-MSCA shall verify that the MAC in the received KDM matches the MAC in the KDM sent by the ERCA;
- the public point specified in the message is on the curve specified by the key distribution request sent by the I-MSCA to the ERCA;

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

The duly authorized I-CP personnel signs for receipt of the key distribution message at the I-MSCA premises.

Upon reception of the key distribution message at the I-CP premises, the I-CP 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 not corrupted; the I-CP shall verify that the MAC in the received KDM matches the MAC in the KDM sent by the I-MSCA;
- the public point specified in the message is on the curve specified by the key distribution request sent by the I-CP to the I-MSCA;
- the master key type and version in the message matches the requested type and version.

If any of these checks fail, the I-CP shall abort the process and contact the I-MSCA.

4.2.7 Master Key Usage

The I-CP shall use Km-wc master key for the sole purpose of insertion into the Workshop Cards.

The I-CP shall use Kdsrc master key for the sole purpose of insertion into the Workshop and Control Cards.

The I-CP shall maintain the confidentiality, integrity, and availability of the the master keys according to section 6.2.

4.2.8 KDM Renewal

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

I-MSCA – ERCA

KDM renewal requested by the I-MSCA to the ERCA may take place only if the original transport media received at the I-MSCA are damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the I-MSA and the ERCA. Subsequent to this report, the I-MSCA may send a KDM renewal request to the ERCA, referring to the original key distribution request.

In case the I-MSCA needs to send a request to re-distribute a master key that was already successfully distributed to the I-MSCA, it shall generate a new key distribution request, using a newly generated ephemeral key pair.

I-CP – I-MSCA

KDM renewal requested by the I-CP to the I-MSCA may take place only if the original transport media received at the I-CP are damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the I-MSA and the ERCA. Subsequent to this report, the I-CP may send a KDM renewal request to the I-MSCA, referring to the original key distribution request.

In case the I-CP needs to send a request to re-distribute a master key that was already successfully distributed to the I-CP, it shall generate a new key distribution request, using a newly generated RSA key pair. Such e request may lead the I-MSCA to initiate an investigation of the possibility of key compromise.

4.2.9 Master Key Re-key

Each master key (and all related keys) is associated to a specific generation of the ERCA root key pair and needs to be replaced every 17 years.

I-MSCA – ERCA

To receive the new version of a master key generated by the ERCA, the I-MSCA shall submit a new KDR. Key application, processing, distribution and acceptance is the same as for the initial key.

I-CP – I-MSCA

To receive the new version of a master key distributed by the I-MSCA, the I-CP shall submit a new KDR. Key application, processing, distribution and acceptance is the same as for the initial key.

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.

4.2.10 Symmetric Key Compromise Notification

If the I-MSCA/I-CP detects or is notified of the compromise or suspected compromise of a symmetric master key, the I-MSCA/I-CP shall notify this to the ERCA and the I-MSA without unnecessary delay and at least within 8 hours of detection.

In their notification, the I-MSCA/I-CP shall indicate the circumstances under which the compromise occurred. The outcome of any follow-up investigation and

potential action by the I-MSA and/or the I-MSCA/I-CP shall be reported to the ERCA.

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 integrity of the status information shall be maintained by the ERCA.

4.2.12 End of Subscription

Subscription for the I-MSCA's key distribution services ends when the I-CP decides for CP termination. Such a change is notified to the ERCA by the I-MSA as a change to the national policy.

In the case of subscription ending, the I-CP 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 I-MSCA and I-CP system.

4.3 Tachograph Card Application

Cardholding users do not apply for certificates, their certificates are issued based on the information given in the application for a Tachograph card, captured from the I-CIA register.

The I-CIA is responsible for identification of cardholding users.

The I-CIA shall guarantee adherence to application procedures for cards, defined by the I-MSA according to the EU Regulation 165/2014 [1].

The applicant shall, by making an application for a card and accepting delivery of the card, sign an agreement with the I-CIA, accepting the terms and conditions regarding use and handling of the Tachograph card.

4.3.1 Application approval registration

The I-CIA shall register approved applications in a database. This data is made available for the I-MSCA/I-CP, which uses the information as input to the certificate generation and card personalization.

The applicant shall, by making an application for a card and accepting delivery of the card, sign an agreement with the I-CIA, accepting the terms and conditions regarding use and handling of the Tachograph card.

The issuance process of tachograph cards shall ensure that the effective date of the card's certificate(s) is equal to the begin of the validity of the card itself, as encoded in EF Identification.

4.3.2 Card renewal, replacement and exchange

Workshop cards shall be valid for no more than **one** year from issuance.

Driver cards shall be valid for no more than **five** years from issuance.

Company cards shall be valid for no more than **five** years from issuance.

Control cards shall be valid for no more than **two** years from issuance.

The I-CIA shall guarantee that issuing of replacement cards, card renewal and card exchange or update take place according to the EU Regulation 165/2014 [1].

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

The key and certificate generation services shall be housed in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorised access, damage, and interference.

Storage media used to store confidential information, such as hard disks, smart cards and HSMs, shall be protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).

Procedures for the disposal of waste shall be implemented in order to avoid unauthorised use, access, or disclosure of confidential data.

The I-MSCA/I-CP's facility shall have a place to store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. Backups shall be kept both for data recovery and for the archival of important information.

The I-MSCA/I-CP shall, during storage, use and distribution, protect the motion sensor and DSRC master keys with high assurance physical and logical security controls.

Backup media shall also be stored at a site different from where the I-MSCA/I-CP system resides, to permit restoration in the event of a natural disaster to the primary facility.

5.2 Procedural Controls

Procedural controls shall be implemented to ensure secure operations. In particular, separation of duties shall be enforced by implementing multiple-person control for critical tasks.

Access to the I-MSCA/I-CP systems shall be limited to individuals who are properly authorised and on a need-to-know basis. In particular, the following access control measures shall be in place:

- confidential data shall be protected to safeguard data integrity and confidentiality when stored;
- confidential data shall be protected to safeguard data integrity and confidentiality when exchanged over unsecure networks;
- confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data;
- the I-MSCA/I-CP systems shall ensure effective user administration and access management;

- the I-MSCA/I-CP systems shall ensure that access to information and application system functions is restricted to authorised staff and provide sufficient computer security controls for the separation of trusted roles. Particularly, the use of system utility programs shall be restricted and tightly controlled. Access shall be restricted, only allowing access to resources as necessary for carrying out the role(s) allocated to a user;
- the I-MSCA/I-CP personnel shall be identified and authenticated before using the I-MSCA/I-CP systems;
- the I-MSCA/I-CP personnel shall be accountable for their activities, which shall be logged in event logs as described in section 5.4.

The I-MSCA/I-CP shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. The I-MSCA/I-CP shall ensure that the ISMS policies address personnel training, clearances and roles.

The I-MSCA ISMS implementations should conform with the requirements described in ISO 27001 [12].

5.3 Personnel Controls

The I-MSCA/I-CP responsibilities may be outsourced to a specialised company, or personnel from contractors may be hired to carry out the I-MSCA responsibilities.

All personnel involved with the I-MSCA/I-CP shall be properly trained and shall possess the expert knowledge, experience and qualifications necessary for the services offered and appropriate to the job function. This pertains to personnel employed by the I-MSCA/I-CP directly, personnel from a specialised company to which tasks have been outsourced or personnel from contractors.

To ensure that one person acting alone cannot circumvent safeguards, responsibilities in I-MSCA/I-CP systems need to be attended by multiple roles and individuals. Each account on the systems shall have limited capabilities, commensurate with the role of the account holder.

The recommended roles are:

- Certification Authority Administrator or Personalization Administrator (CAA/PA);
- System Administrator (SA);
- I Information System Security Officer (ISSO).

The ISSO, not directly involved in issuing certificates, performs a supervisory function in examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security Policy.

For the I-MSCA/I-CP, different individuals shall fill each of the three roles described above and at least one individual shall be appointed per task. No single person shall be authorised to simultaneously perform more than one of the trusted roles.

Identification and authentication of CAA/PA, SA and ISSO shall be appropriate and consistent with practices, procedures and conditions stated in this Policy.

The individual assuming the CAA/PA role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

All I-MSCA/I-CP personnel in sensitive positions, including, at least, all CAA/PA and ISSO (Information System Security Officer) positions, shall:

- not be assigned other duties that may conflict with their duties and responsibilities as CAA/PA and ISSO;
- not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- have received proper training in the performance of their duties, according to a training plan described in the respective Pratices Statements.

The I-MSCA/I-CP personnel in trusted roles, as detailed in the respective Practice Statements, shall have an appropriate background screening, with positive results; these roles and the associated responsibilities shall be documented in job descriptions, from the viewpoint of separation of duties and least privilege.

5.4 Audit Logging Procedures

All significant security events in the I-MSCA and I-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 attempts to add or remove an entity from the register of subscribers to which the I-MSCA currently provide key certification services, or to change any details for any of the subscribers, or to retrieve information from the register;
- successful and failed attempts to process a certificate signing request or a key distribution request;
- successful and failed attempts to sign a certificate or generate a key distribution message;
- successful and failed interactions with the database(s) containing data on (the status of) issued certificates, including connection attempts and read, write and update or removal operations;
- successful and failed attempts to connect to or disconnect from an HSM;
- successful and failed attempts to authenticate a user to an HSM;
- successful and failed attempts to generate or destroy a key pair or a symmetric key inside an HSM;

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

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

The integrity of system event logs shall be maintained and shall be protected from unauthorised inspection, modification, deletion or destruction. System events logs shall be backed-up and stored in accordance with procedures described in the respective PS.

The log shall be processed regularly and analyzed against malicious behaviour. Log procedures will be described in the PS.

Audit log shall be retained for at least **2** years.

Audit logs shall be verified and consolidated at least monthly. At least dual control is required.

5.5 Records Archival

The records shall include all relevant evidence in the I-CIA's possession including, but not limited to:

- Certificate requests.
- Signed registration agreements from user's applications for certificates and cards, including the identity of the person responsible for accepting the application.
- Contractual agreements regarding certificates and associated cards.
- Currently and previously implemented Policy documents.

The records shall include all relevant evidence in the I-MSCA/I-CP's possession including, but not limited to:

- Contents of issued certificates (I-MSCA).
- Audit journals including records of annual auditing of I-MSCA/I-CP's compliance with its PS.
- Currently and previously implemented certificate Policy documents and their related PSs.

Records of all digitally signed electronic requests made by I-MSCA/I-CP or Service Agency personnel (CAA/PA) shall include the identity of the administrator responsible for each request together with all information required for non-repudiation checking of the request for as long as the record is retained.

Archives shall be retained and protected against modification, loss or destruction. Archival periods, for all archived information, shall be indefinite.

Procedures shall be in place to ensure integrity, authenticity and confidentiality of the records.

An overview of the events which shall be archived shall be described in internal procedures. The I-MSCA I-CP shall implement appropriate record archival procedures.

Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.

The I-MSCA/I-CP shall make available on request, produced documentation of the I-MSCA/I-CP's compliance with the applicable PS.

Subject to statute, a reasonable handling fee may be charged to cover the cost of record retrieval.

The I-MSCA/I-CP shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the I-MSCA/I-CP's operations are interrupted, suspended or terminated.

In the event that I-MSCA/I-CP services are to be interrupted, suspended or terminated, the I-MSCA/I-CP shall ensure the continued availability of the archive.

All requests for access to archived information will be sent to the I-MSCA/I-CP or to the entity identified by the I-MSCA/I-CP prior to terminating its service.

5.6 Key Changeover

I-MSCAs shall generate new I-MSCA key pairs as needed. After the generation of a new key pair, the I-MSCA shall submit a certificate re-key request as foreseen in section of ERCA Policy ([5] section 4.1.8).

The I-MSCA shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in this I-MSA certificate policy.

5.7 Compromise and Disaster Recovery

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

I-MSCA and I-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. I-MSCA and I-CP shall furthermore assume that technological progress will render their IT systems obsolete over time and shall define measures to manage obsolescence.

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:

1. compromise or theft of a private key and / or a master key;
2. loss of a private key and / or a master key;
3. IT hardware failure.

In the event of compromise or theft of I-MSCA root private key and / or a symmetric master key, the I-MSCA shall immediately inform the European

Authority and the MSCAs. The EA shall take appropriate measures within a reasonable time period.

Loss shall therefore be prevented by the use of multiple backup copies of the root 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 Termination

In the event of termination of the I-MSCA activity, by the appointed organisation, the I-MSA shall notify the European Authority and the ERCA of this and optionally inform the European Authority and ERCA about the newly appointed MSCA.

The I-MSA shall ensure that at least one I-MSCA is operational in its jurisdiction at all times.

Before the I-MSCA terminates its services, the I-MSA shall ensure that the tasks below are carried out:

- Inform all users and parties with whom the I-MSCA has agreements or other form of established relations.
- Make publicly available information of its termination at least 3 month prior to termination.
- The I-MSCA will terminate all authorization of subcontractors to act on behalf of the I-MSCA in the process of issuing certificates.
- The I-MSCA shall perform necessary undertakings to transfer obligation for maintaining event log archives for the remaining period of their life cycle.

5.8.1 Transfer of MSCA or CP responsibility

Transfer of I-MSCA or I-CP responsibility occurs when the I-MSA chooses to appoint a new I-MSCA or I-CP in place of the former entity.

The I-MSA shall ensure that orderly transfer of responsibilities and assets is carried out.

6 Technical Security Controls

6.1 Key Pair and Symmetric Key Generation and Installation

The I-MSCA shall generate private keys in accordance with Annex IC Appendix 11 [2].

Generation of key pairs 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 I-MSCA shall have available a Test MSCA system for interoperability test purposes, according to the Regulation. Test MSCA system shall be a separate system and shall have its own MSCA private keys and symmetric master keys.

The Test MSCA system shall be able to request the signing of test certificates and the distribution of symmetric test keys using the processes foreseen in the ERCA Policy ([5] sections 4.1 and 4.2). The Test MSCA shall also be able to sign test equipment certificates on request of component personalisers, and to distribute symmetric test keys to the I-CP.

6.2 Private Key and Symmetric Key Protection and Cryptographic Module Engineering Controls

The I-MSCA/I-CP shall maintain the confidentiality, integrity, and availability of the private keys and the master keys as described in this section.

The private keys and master keys shall be generated, inserted and used in a trustworthy dedicated Hardware Security Module (HSM) which:

- is certified to EAL 4 or higher in accordance with ISO/IEC 15408 [7] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [9] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [10]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

Private key operations and symmetric key operations shall take place internally in the HSM where the keys used are stored.

Key generation shall be covered by the security certification of the equipment, ensuring that publicly specified and appropriate cryptographic key generation algorithms are used.

On-board key generation shall not apply at Card personalization level.

The I-MSCA/I-CP symmetric master keys shall only be inserted into the HSM within a physically secure environment by personnel in trusted roles under at least dual control. All events of symmetric master key insertion shall be logged.

The I-MSCA/I-CP private keys and symmetric master 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 I-MSCA/I-CP private keys and the master 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.

Any copies of the I-MSCA/I-CP private keys and the master keys shall be subject to the same level of security controls as the keys in use.

Private key import and export shall only take place for back-up and recovery purposes. Master key import and export is only allowed for back-up and recovery purposes.

Export of Km-wc and the VU-specific keys for DSRC is allowed in encrypted form only, and only in response to a valid key distribution request from a component personaliser by personnel in trusted roles under at least dual person control.

At the end of private key usage period of an I-MSCA private key (as specified in Appendix 11 of Annex IC), the I-MSCA shall destroy all copies of the key such that it cannot be retrieved.

Similarly, at the end of the life cycle of a symmetric master key (as specified in Appendix 11 of Annex IC), the I-MSCA/I-CP shall destroy all copies of the key such that it cannot be retrieved.

All private keys and master keys shall immediately be deactivated (such that they cannot be used) if a compromise is suspected.

The I-MSCA/I-CP shall investigate the suspected compromise. If a compromise is confirmed or cannot be ruled out, the keys shall be destroyed. Also all copies of a compromised key shall be destroyed.

If a compromise can be ruled out, the keys shall be activated again.

Destroying of private keys and master keys shall be done by using the function of the HSM for key destroying.

6.3 Other Aspects of Key Pair Management

The I-MSCA public key certificates and hence the public keys shall be archived indefinitely.

The validity periods of all I-MSCA certificates shall comply with Annex IC Appendix 11 [2].

In accordance with Annex IC Appendix 11 [2], the private key usage period of I-MSCA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate.

The I-MSCA shall not use a private key after the private key usage period is over.

6.4 Activation Data

System activation, in order to generate, use or destroy a I-MSCA private key or to import or use a symmetric master key, shall take place in a physically secured environment by (I-MSCA/I-CP) personnel in trusted roles under, at least, dual control.

I-MSCA private keys and I-CP symmetric master keys, stored in an HSM, shall be activated for use, generated, imported or destroyed only if all necessary persons controlling the keys have authenticate themselves towards the HSM. Authentication shall take place by using proper means (e.g. authentication tokens). The duration of an authentication session shall not be unlimited.

I-MSCA and I-CP shall describe in their respective Practices Statements MSCA (as appropriate) the number of persons in a trusted role that are required in order to activate the system and generate, use or destroy a MSCA private key or to import or use a symmetric master key.

For activation of the I-MSCA software and the system on which this software is running, user authentication shall take place using proper means.

6.5 Computer Security Controls

The I-MSCA/I-CP shall specify and approve procedures and specific technical security measures for managing their computer systems. These procedures shall guarantee that the required security level is always being met.

The procedures and technical security measures shall be described in internal I-MSCA/I-CP documentation. Computer systems shall be arranged and managed conforming to these procedures.

6.6 Life Cycle Security Controls

The I-MSCA and I-CP shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built into their respective 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.

The I-CP shall ensure that any relevant prescription mandated by the Common Criteria security certification of the equipment is met during the complete life cycle of the equipment;

6.7 Network Security Controls

The I-MSCA shall devise and implement its network architecture in such a way that access from the internet to its internal network domain, and from the internal network domain to the Certification Authority systems, can be effectively controlled.

6.8 Timestamping

The time and date of an event shall be included in every audit trail entry.

The I-MSCA/I-CP PS shall describe how time is synchronised and verified.

7 Certificate and CRL Profiles

7.1 Certificate Profile

All certificates shall have the profile specified in Annex 1C, Appendix 11 and Appendix 1 [2]:

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	7F 21	var	
Certificate Body	7F 4E	var	
Certificate Profile Identifier	5F 29	01	INTEGER (0.. 255)
Certification Authority Reference	42	08	KeyIdentifer
Certificate Holder Authorisation	5F 4C	07	Certificate Holder Authorisation
Public Key	7F 49	var	

Data Object	Tag (hex)	Length (bytes)	ASN.1 data type
Standardised Domain Parameters OID	06	var	OBJECT IDENTIFIER
Public Point	86	var	OCTET STRING
Certificate Holder Reference	5F 20	08	KeyIdentifer
Certificate Effective Date	5F 25	04	TimeReal
Certificate Expiry Date	5F 24	04	TimeReal
ECC Signature	5F 37	var	OCTET STRING

Table 5 Certificate profile

The **Certificate Profile Identifier** identifies the version of the profile; its value shall be '00'.

The **Certification Authority Reference** shall contain the Key Identifier of the I-MSCA Member State Key which signed the certificate.

The **Certificate Holder Authorisation** shall be used to identify the type of the 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 (see Annex 1C, Appendix 11, CSM_141).

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

- the **Domain Parameters** data object shall reference the standardised 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 [6]. The uncompressed encoding format shall be used ([2] Annex 1C, Appendix 11, CSM_143).

The **Certificate Holder Reference** shall identify the public key contained in the certificate.

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.

The **Signature** shall be verifiable with the public key contained in the certificate. 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 [11], using the hashing algorithm linked to the size of the *Public Key* field, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain, as specified in [6].

The algorithm is indicated via the Standardised Domain Parameters OID as specified in Table 1 of Appendix 11, Annex 1C. 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 6 Allowed Standardised Domain Parameters OIDs

7.2 CRL Profile

No CRL shall be managed. Status information shall apply at Tachograph equipment level only. Non-valid tachograph cards shall be put in a ”black list”

7.3 OCSP Profile

No OCSP shall be used.

8 Compliance Audit and Other Assessment

8.1 Frequency or circumstances of assessment

The I-MSA is responsible for ensuring that audits of the I-MSCA and I-CP take place.

A formal audit on the I-MSCA and I-CP operation shall be performed regularly. The I-MSCA/I-CP audit shall establish whether the requirements on the I-MSCA/I-CP described in this document are being maintained.

The I-MSCA/I-CP shall be audited within 12 months of the start of the operations covered by this policy; the next audit shall be performed within 24 months in case of absence of non-conformity evidence. 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 this policy, the I-MSA shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements set in the policy.

8.2 Identity/qualifications of assessor

The audit shall be performed by an independent auditor. Any person selected or proposed to perform an I-MSCA/I-CP compliance audit shall first be approved by the I-MSA.

The auditors shall comply with the following requirements:

- ethical behaviour: trustworthiness, uniformity, confidentiality regarding their relationship to the organisation 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 relevant European Commission policies and regulations.

8.3 Assessor's relationship to assessed entity

The auditor shall be independent and not connected to the organisation being the subject of the audit.

8.4 Topics covered by assessment

The I-MSA audit shall cover the I-MSCA/I-CP´s practices, documented in CPS/PS. The audit shall cover the I-MSCA/I-CP´s compliance with this I-MSA Policy. The audit shall also consider the operations of any Service Agencies.

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 the systems of the organisation to be audited. 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 found by the auditor, corrective actions shall be taken immediately by the I-MSCA/I-CP. A follow-up audit shall take place within 12 month.

8.6 Communication of results

The auditor shall report the full results of the compliance audit to the I-MSCA/I-CP and to the I-MSA.

The I-MSA shall send an audit report 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 ERCA shall publish the audit report reception date on its website. If requested by the ERCA, the I-MSA shall send the full results of the compliance audit to the ERCA.

9 Other Business and Legal Matters

9.1 Fees

Not applicable.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

Confidential data shall comprehend 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.

9.4 Privacy of Personal Information

The only personal data processed or stored in the I-MSCA system are those of I-MSCA representatives.

Personal information pertaining Cardholders managed by the I-CIA, I-CP and Service Agencies shall be kept confidential and not disclosed to third parties.

The I-CIA shall be entitled or required to disclose Cardholders personal information only pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

Cardholders personal information shall be treated according to the General Data Protection Regulation 2016/679 [13].

9.5 Intellectual Property Rights

Not applicable.

9.6 Representations and Warranties

I-MSCA and I-CP shall operate according to the ERCA Policy [5], this I-MSA Policy and their own CPS/PS.

9.7 Disclaimers and Warranties

The I-MSA 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 authorised 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

Tachograph cards, keys and certificates are only for use within the Tachograph system. Any other certificates stored on Tachograph cards are in violation of this Policy, and hence neither the I-MSA, the I-CIA, the I-MSCA nor the I-CP carries any liability in respect to such use.

The I-MSA and I-CIA shall be liable for damages resulting from failures to fulfill their obligations only if they have acted negligently. If the I-MSA or I-CIA has acted according to this I-MSA Policy, and any other governing document, it will not be considered to have been negligent.

The I-CP or I-MSCA shall be liable for damages resulting from failures to fulfil these obligations only if it has acted negligently. If the organization has acted according to this I-MSA Policy and the corresponding PS, it will not be considered to have been negligent.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

This I-MSA Policy is valid from the moment of its publication. It shall be valid until further notice.

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.

Questions concerning this policy shall be forwarded to the I-MSA (see section 1.5)

Changes to these documents shall be made in a manner consistent with the requirements stipulated in section 9.12 of this document.

9.12 Amendments

9.12.1 Changes without notification

The only changes to this I-MSA policy not needing any notification are:

- Editorial or typographical corrections;
- Changes to the contact details.

9.12.2 Changes with notification

Any item in this certificate Policy may be changed with 90 days' Notice.

Changes to items which, in the judgment of the I-MSA, will not materially impact a substantial majority of the users or relying parties using this Policy may be changed with 30 days' notice.

Impacted users may file comments with the Policy administration organization within 16 days of original notice.

Information about changes to this Policy will be sent to:

- ERCA
- I-MSCA and I-CP including Service Agencies
- I-CIA
- MSAs / CPAs eventually supported if a cooperation administrative arrangement between countries is in place (see section 1.3.1.2)

9.13 Dispute Resolution Procedures

Any dispute related to key and certificate management between the I-MSA and an organisation or individual shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 of the European Parliament and of the Council [1] and with Commission Implementing Regulation (EU) 2016/799 [2]. In case discrepancies exist between this document and the Regulation or Implementing Regulation, the latter shall prevail.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.

10 References

[1]. Regulation (EU) No 165/2014 of the European Parliament and Council of 4 February 2014, Official Journal of the European Union L60

[2]. Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139, including ref. 3.

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

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

[5]. Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy Version 1.0 June 2018 PDF ISBN 978-92-79-79909-9 Luxembourg: Publications Office of the European Union, 2018. © European Union, 2018

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

[7]. 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

[8]. 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

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

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

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

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

[13]. Regulation (EU) No 2016/679 of the European Parliament and Council - 4 May 2016 - General Data Protection Regulation (GDPR)

[14]. RSA Laboratories. *RSA Cryptography Standard.* v2.1, June 14, 2002. URL: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html

11 List of Figures

12 List of Tables