European Commission

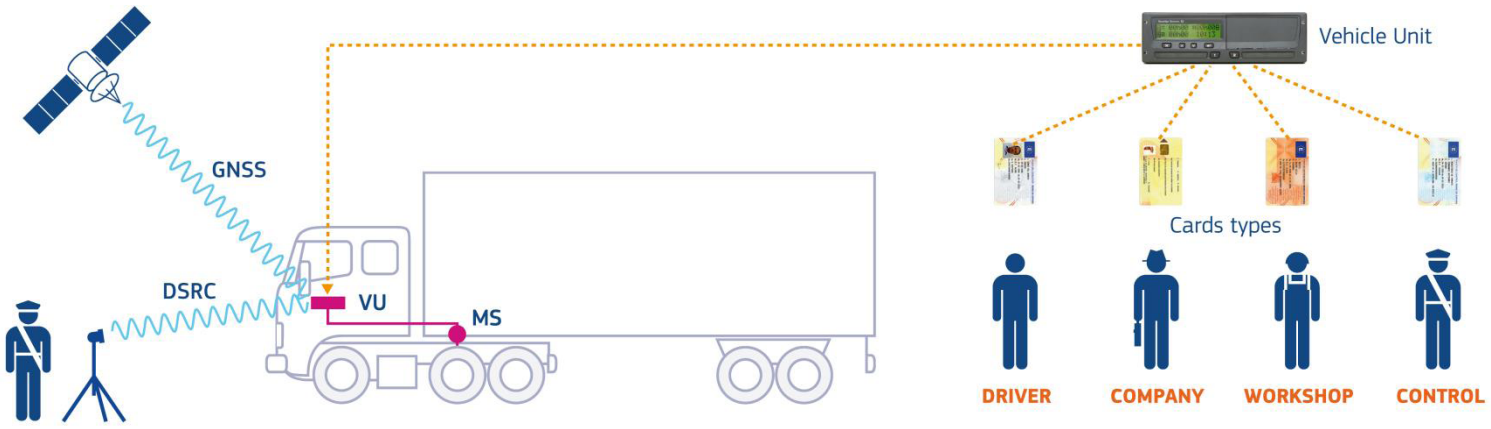
JRC TECHNICAL REPORTS

Smart Tachograph

European Root Certificate Policy and Symmetric Key Infrastructure Policy

Marjo Geers, David Bakker (UL)
Luigi Sportiello (JRC)

Version 1.0
June 2018



Joint Research Centre

EUR 29118 EN

Contact information
E-mail: jrc-erca@ec.europa.eu

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

JRC110814

EUR 29118 EN

PDF ISBN 978-92-79-79909-9 ISSN 1831-9424 doi: 10.2760/409258

Luxembourg (Luxembourg): Publications Office of the European Union, 2018.

How to cite this report: Marjo Geers, David Bakker, Luigi Sportiello, Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy - Ver.1.0, EUR 29118 EN, DOI 10.2760/409258.

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 [1].

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

Appendix 11 (Common Security Mechanisms) of Annex 1C specifies the security mechanisms ensuring

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

Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realise 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. 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.

Next to the production keys and certificates, the ERCA also issues test certificates and distributes test symmetric master keys to MSCAs to be used for Interoperability Testing purposes, see [7]. Using these test keys and certificates, MSCAs can sign and distribute certificates, symmetric keys and encrypted data for motion sensors to be installed in Smart Tachograph equipment for interoperability testing purposes.

This document forms the Certificate Policy (CP) for the PKI at the ERCA level. It lays down the policy at ERCA level for key generation, key management and certificate signing for the Smart Tachograph system. For the ERCA to issue certificates to an MSCA or to distribute symmetric keys to an MSCA, the MSCA shall comply with requirements also laid down in this document.

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. How the ERCA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the ERCA Certification Practice Statement (CPS) [6].

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

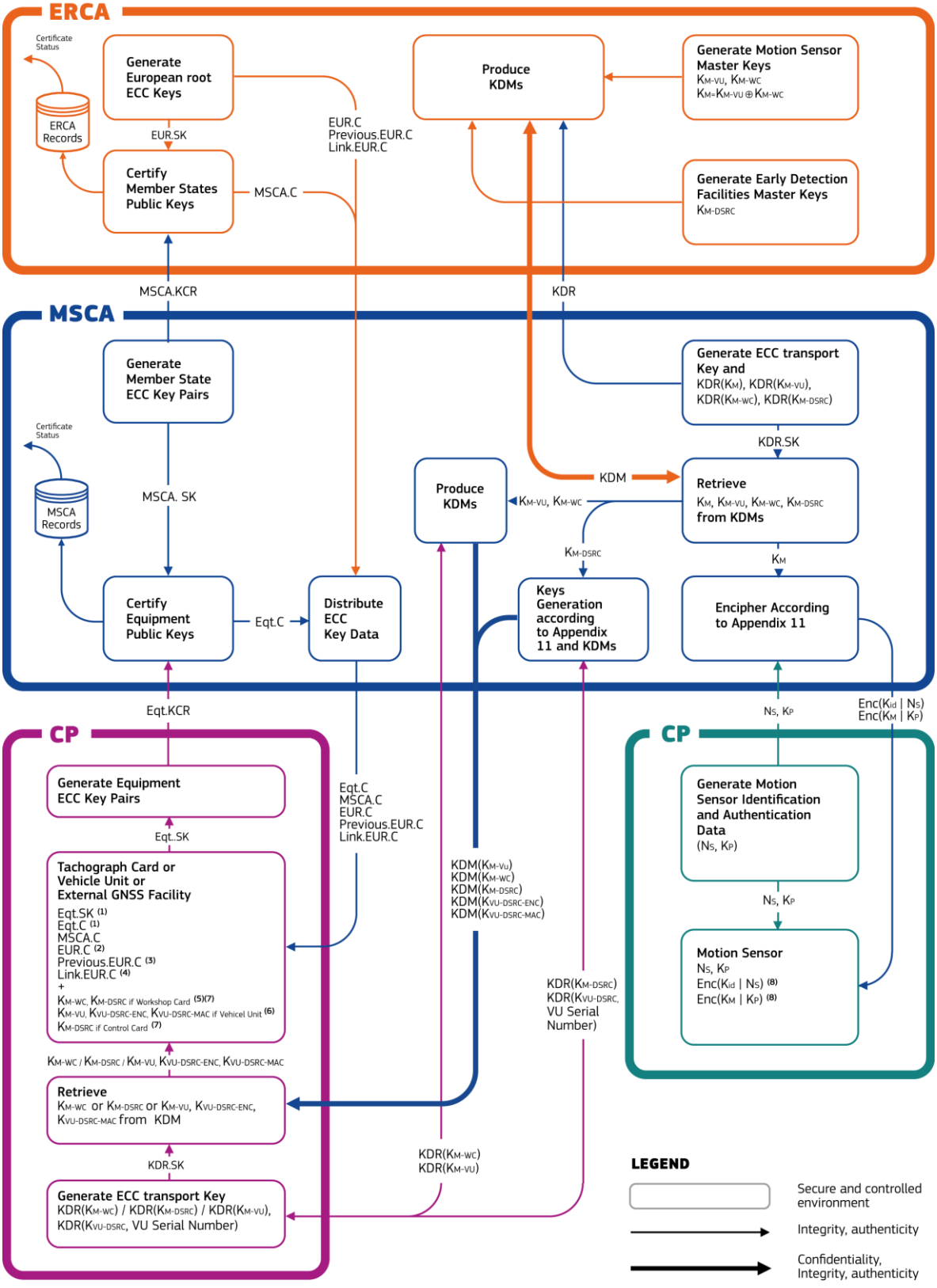
This document is named Smart Tachograph – European Root Certificate Policy and Symmetric Key Infrastructure Policy. This Certificate Policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the certificates used in the Smart Tachograph system do not contain a reference to this policy.

The current version is 1.0.

This policy was endorsed by EU Member States on 15 May 2018 and by the European Authority (see section 1.5.1) on 14 June 2018.

1.3 Participants

The participants in the Smart Tachograph PKI and in the Symmetric Key Infrastructure are described here and represented in Figure 1.



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

Figure 1 also represents the exchanges between the participants, namely ERCA, MSCAs and component personalisers (CPs). For more information on the symmetric and asymmetric keys mentioned in this section, refer to Appendix 11 Part B.

1.3.1 Certification Authorities

1.3.1.1 European Root Certification Authority (ERCA)

The ERCA is the root Certification Authority (CA) that 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 ($K_{M\text{-}VU}$), the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC}$) and the DSRC Master Key (K_{DSRC}).

1.3.1.2 Member State Certificate Authorities (MSCAs)

The MSCAs operate as sub-CAs under the ERCA. They sign public key certificates for equipment. For this, they operate a registration service, certificate generation service and dissemination service. The MSCAs receive the certificate requests from component personalisers and disseminate 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 a MSCA_VU-EGF key pair; and one for the issuance of Card certificates, called a MSCA_Card key pair. Each MSCA may request from the ERCA either or both types of MSCA certificate, depending on their responsibilities regarding the issuance of equipment. An MSCA responsible for the issuance of tachograph card certificates is indicated in this document as an MSCA_Card. An MSCA responsible for the issuance of VU and/or EGF certificates is indicated as an MSCA_VU-EGF.

The MSCAs are also the entities requesting symmetric master keys from the ERCA, again depending on their responsibilities. The MSCAs distribute $K_{M\text{-}VU}$ to VU manufacturers, and $K_{M\text{-}WC}$ and K_{DSRC} to card personalisers. The MSCAs may also use the Motion Sensor Master Key (K_M) to encrypt motion sensor pairing keys (K_P) on request of a motion sensor manufacturer and derive the motion sensor Identification Key (K_{ID}) from K_M, which they then subsequently use to encrypt motion sensor serial numbers on request of a motion sensor manufacturer. Finally, MSCAs may use K_{DSRC} to derive VU-specific keys by request of a VU manufacturer on basis of the VU serial number.

1.3.2 Registration Authorities

Within the Smart Tachograph PKI, registration authorities are part of the certification authorities described in the previous section. This document therefore does not contain any specific requirements for registration authorities.

1.3.3 Subscribers

The only subscribers to the ERCA public key certification service are the MSCAs.

The only subscribers to the MSCA public key certification service are the component personalisers. Component personalisers are responsible for the personalisation of:

- Vehicle Units (VUs)
- External GNSS Facilities (EGFs)
- Motion Sensors (MoSs)
- Tachograph Cards: four different types of tachograph cards exist: driver cards, company cards, workshop cards and control cards.

This equipment contains cryptographic keys. The VUs, EGFs and TCs also contain certificates:

- The VUs have two key pairs and corresponding certificates issued by an MSCA_VU-EGF, namely
    - a key pair and certificate for mutual authentication, called VU_MA;
    - a key pair and certificate for signing, called VU_Sign.

    The VUs also contain K_{M-VU}.

    The VUs also contain two VU-specific symmetric keys to secure the DSRC communication.
- The EGFs have one key pair and corresponding certificate issued by an MSCA_VU-EGF for mutual authentication.
- The MoSs contain a pairing key Kp, the encrypted pairing key and the encrypted MoS serial number.
- The driver cards and workshop cards have two key pairs and corresponding certificates issued by an MSCA_Card, namely
    - a key pair and certificate for mutual authentication, called Card_MA;
    - a key pair and certificate for signing, called Card_Sign.

    The workshop cards also contain K_{M-WC} and K_{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_{DSRC}.

Component personalisers are responsible for ensuring the equipment is provided with the appropriate keys and certificates.

- A VU manufacturer
    - generates the VU serial number (`ExtendedSerialNumber`) or the `CertificateRequestID` if the VU serial number is not yet known;
    - ensures generation of the two VU key pairs for mutual authentication and signing;
    - performs the certificate application process with a MSCA_VU-EGF;
    - performs the application for the VU-specific keys for DSRC with the MSCA;
    - performs the application for K_{M-VU};
    - ensures placement in the VU of keys pairs and certificates for mutual authentication and signing, VU-specific DSRC keys and K_{M-VU}.

- An EGF manufacturer
    - generates the EGF serial number (`ExtendedSerialNumber`);
    - ensures generation of the EGF key pair;
    - performs the certificate application process with the MSCA_VU-EGF;
    - ensures placement in the EGF of the EGF key pair and certificate.
- A MoS manufacturer
    - generates the MoS serial number;
    - generates the pairing key K_P required to pair a MoS to a VU;
    - requests the encryption of the pairing key with the MoS master key, K_M, and the encryption of the MoS serial number with the identification key K_{ID} from the MSCA_VU-EGF;
    - ensures the MoS serial number and pairing key are placed in plain and in encrypted form in the MoS.
- A card personaliser 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).
- A card personaliser 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 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 and workshops.

1.4 Key and Certificate Usage

The ERCA root certificates and ERCA link certificates shall be used to verify MSCA certificates issued by the ERCA. The ERCA certificates will be the highest trust point for the PKI and shall be placed in VUs, cards and EGFs, as specified in Appendix 11. All MSAs and PKI participants (see section 1.3) shall recognise the ERCA public key certificates, provided they are published by the ERCA according to the requirements in chapter 2.

The ERCA shall use its ERCA private keys only for:

- Signing of ERCA root, ERCA link and MSCA certificates, in accordance with Annex IC Appendix 11 [2].

An MSCA shall use its Member State private keys only for:

- Signing of equipment certificates, in accordance with Annex IC Appendix 11 [2].
- Signing of certificate signing requests (see section 4.1.1)
- Issuing Certificate Revocation Lists, if such a method is used for providing certificate status information.

The ERCA shall not use the symmetric master keys for any purpose except distribution to the MSCAs.

An MSCA shall use the master keys solely to derive VU-specific keys and encrypt motion-sensor related data as specified in Annex IC Appendix 11 [2].

The MSCAs shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to component personalisers 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 MSCA_VU-EGF certificates shall be used to verify VU and EGF certificates issued by the MSCA_VU-EGF.

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

The VU_MA certificates shall be used for mutual authentication, session key agreement and coupling between a VU and an EGF. The VU_MA certificates are also used for mutual authentication and session key agreement between a VU and a card.

The VU_Sign certificates shall be used to verify the authenticity and integrity of data downloaded from the VU. The VU_Sign private key may only be used to sign data downloaded from the VU.

The EGF_MA certificates shall be used for mutual authentication, coupling and session key agreement between EGF and VU.

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 shall be used by an MSCA_VU-EGF to encrypt MoS pairing keys, K_P, and to derive the MoS identification keys, K_{ID}. K_{ID} shall be used by an MSCA to encrypt MoS serial numbers.

K_{M-VU} and K_{M-WC} shall be provided to component personalisers for their installation respectively in VUs and Workshop Cards. K_{M-VU} shall be used by the VU together with K_{M-WC} to generate K_M during VU-MoS pairing.

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

1.5 Policy Administration

1.5.1 European Authority

The European Commission service responsible for this policy is referred to hereinafter as the European Authority (EA).

The contact address of the EA is:

European Commission
DG MOVE - Directorate General for Mobility and Transport
Directorate C – Land
Unit C.1 – Road Transport
Rue J.-A. Demot, 24-28
B-1040 Bruxelles

The EA appoints the organisation which implements this policy at ERCA level and provides key certification and key distribution services to the Member States, see next section.

1.5.2 ERCA

The European Commission service responsible for implementation of this policy at the European level and for the provision of key certification and key distribution services to the Member States is referred to hereinafter 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
DG JRC - Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

The EA shall ensure that the ERCA has the resources required to operate in conformity with this policy. The ERCA shall document its implementation of this policy in a Certification Practice Statement (CPS) [6]. The ERCA CPS is the ERCA's procedural document, which details how the ERCA certificate policy is enforced in day-to-day management. The document is developed by the ERCA. The ERCA CPS is owned by the ERCA. The ERCA CPS shall be treated as restricted information. The ERCA shall make the contents of its CPS available to Member State Authorities and Member State Certification

Authorities on a need-to-know basis. The ERCA CPS shall be managed, reviewed, and modified following document control procedures.

The EA shall be responsible to determine whether the ERCA CPS complies with this ERCA CP. The EA's statement of compliance is based on a security review performed by the European Commission's Security services, and the results of functional tests performed by the ERCA.

The ERCA shall maintain records of its operations as appropriate to demonstrate conformity with this policy, and shall make these records available to the EA on demand.

Complaints from MSAs about the services provided by the ERCA shall be addressed to the EA to be dealt with.

1.5.3 Member State Authorities

Each Member State shall set up a Member State Authority (MSA). Each Member State Authority shall lay down and document an MSA certificate policy in conformance with all applicable requirements in this ERCA certificate policy.

An MSA certificate policy may consist of a collection of documents, as appropriate to the organisation of its component services. An MSA certificate policy's contents shall comply with all applicable requirements in this ERCA certificate policy. Some specific attention points are:

- An MSA certificate policy should follow the framework for certificate policies described in RFC 3647 [4]
- An MSA certificate policy shall describe the roles and responsibilities involved in the overall equipment issuing process in the country concerned, including at least the MSCA and component personaliser roles. All organisations carrying out one or more of these roles shall be identified.
- An MSA certificate policy shall require that at least those organisations that generate or manage private or symmetric keys shall be audited regularly. An MSA certificate policy shall describe the scope of each audit, depending on the responsibilities of each organisation, e.g. by pointing out the sections of the MSA certificate policy especially relevant for the given audit.
- An MSA certificate policy shall specify how the MSCA(s) shall register component personalisers who are allowed to send certificate signing requests and key distribution requests.
- An MSA certificate policy shall cover the following processes, where applicable:
    - Issuing of tachograph card keys and certificates;
    - Issuing of vehicle unit keys and certificates;
    - Issuing of External GNSS facility keys and certificates;
    - Distribution of symmetric keys for cards and VUs and encrypted data for motion sensors to component personalisers;
    - Management of the Member State keys.

- An MSA certificate policy shall require that equipment keys are generated, transported and inserted into the equipment in such a way as to preserve their confidentiality and integrity. For this purpose, the MSA shall:
    - require that any relevant prescription mandated by the Common Criteria security certification of the equipment is met during the complete life cycle of the equipment;
    - require that if equipment private key generation is not done on-board the equipment, private key generation takes place within an HSM that complies with the requirements in section 6.2;
    - require that if equipment symmetric key generation is not done on-board the equipment, symmetric key generation takes place within an HSM that complies with the requirements in section 6.2;
    - require that insertion of private keys and symmetric keys into equipment takes place in a physically secured environment;
    - require that if equipment is capable of generating private or symmetric keys on-board, key generation shall be covered by the security certification of the equipment, ensuring that publicly specified and appropriate cryptographic key generation algorithms are used.
- An MSA certificate policy shall require that the user of each tachograph card is identified at some stage of the card issuing process.
- An MSA certificate policy shall require that the ERCA is notified without delay of loss, theft, or potential compromise of any MSCA private key or symmetric master key and shall indicate any follow-up investigation and potential action by the MSA.
- An MSA certificate policy shall indicate appropriate disaster recovery mechanisms, complying with the requirements in section 5.7.
- An MSA certificate policy shall require that all subscribers to an MSCA's services shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. The implementation of the ISMS should conform with the requirements described in ISO 27001 [18].
- An MSA certificate policy shall require that appropriate records of operations involving private or symmetric keys are maintained.
- An MSA certificate policy shall include provisions for MSCA termination.
- An MSA certificate policy shall include change procedures.
- An MSA certificate policy shall require that MSCA shall maintain certificate status information and make this information available to parties having a legitimate interest.
- An MSA certificate policy shall require that the issuance process of tachograph cards ensures that the effective date of the card's certificate(s) is equal to the begin of the validity of the tachograph card itself, as encoded in EF Identification.
- An MSA certificate policy shall forbid key escrow, meaning that MSCA private keys shall not be exported to or stored in any system apart from the systems of the respective MSCA.

The Member State Authority shall make an English version of its MSA certificate policy available to the ERCA. The ERCA shall review the MSA certificate policy for conformity with the requirements defined in this document. The Member State Authority shall adequately respond to any comment by the ERCA. The objective of the review process is to assure comparable levels of security in each Member State. 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 personalisers in its country. The ERCA shall archive the MSA certificate policy and the corresponding review report for reference purposes.

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.

1.5.4 MSCAs

Each MSA shall appoint one or more organisations which implement(s) the national policy and provide(s) key certification and key distribution services to the component personalisers in the Member State or acting on behalf of the Member State. The organisation(s) responsible for implementation of the MSA certificate policy and for the provision of key certification and key distribution services to the component personalisers in the Member State or acting on behalf of the Member State is/are referred to hereinafter as Member State Certification Authority (MSCA).

An MSCA shall document its implementation of the MSA certificate policy in a MSCA Certification Practice Statement. An MSCA shall make its Certification Practice Statement available to the MSA. The MSA shall be responsible to determine whether the MSCA CPS complies with the MSA certificate policy. An MSCA shall make its Certification Practices Statement available to its subscribers on a need-to-know basis. Upon request, an MSCA shall also make its Certification Practices Statement available to the ERCA.

The MSCA shall maintain record of its operations as appropriate to demonstrate conformity with the MSA certificate policy, and shall make these records available to the MSA and/or the ERCA on demand.

Complaints from component personalisers about the services provided by an MSCA shall be addressed to the responsible MSA to be dealt with.

1.6 Definitions and Acronyms

Acronym	**Definition**
AES	Advanced Encryption Standard
CP	Component Personaliser
CP	Certificate Policy
CPS	Certification Practice Statement

DSRC	Dedicated Short Range Communication
CSR	Certificate Signing Request
EC	Elliptic Curve
EC	European Commission
ECC	Elliptic Curve Cryptography
EGF	External GNSS Facility
EA	European Authority
ERCA	European Root Certification Authority
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
JRC	Joint Research Centre
KDR	Key Distribution Request
KDM	Key Distribution Message
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
MSCA	Member State Certification Authority
NCP	Normalised Certificate Policy
PKI	Public Key Infrastructure

RFC	Request For Comment
VU	Vehicle Unit
WC	Workshop Card

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

2 Publication and Repository Responsibilities

2.1 Repositories

The ERCA shall be responsible for the public website https://dtc.jrc.ec.europa.eu/, which shall be the repository for ERCA documents, certificates, and certificate status information.

The certificates signed by the ERCA shall also be maintained in a stand-alone database.

An MSCA shall be responsible for storing all issued equipment certificates in a repository. This repository does not need to be public.

2.2 Publication of Certification Information

The ERCA shall publish the following information on its website:

- ERCA Certificate Policy and Symmetric Key Infrastructure Policy (this document);
- ERCA Certificate Policy change proposal information;
- compliance statements for the ERCA and for each national policy;
- ERCA public key certificates and ERCA link certificates;
- all MSCA public key certificates issued by the ERCA;
- public key certificate status information;
- master keys status information.

The ERCA Certification Practices Statement [6] shall not be public, but shall be communicated on request to the relevant parties.

The ERCA compliance statement shall be issued by the EA on completion of the ERCA approval process. This process is defined by the EA identified in this policy.

The MSA certificate policy compliance statements shall be issued by the ERCA on completion of the MSA certificate policy review process defined in this policy.

By publishing MSCA certificate information in the ERCA repository, the ERCA certifies that:

- it has issued the MSCA certificate to the corresponding MSCA;
- the information stated in the certificate was verified in accordance with this policy and the CPS [6];
- the MSCA has accepted the certificate.

2.3 Time or Frequency of Publication

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

Similarly, information relating to the changes in the ERCA CPS [6], the MSA certificate policies and the MSCA CPSs shall be published according to the schedules defined by the change (amendment) procedures laid down in the ERCA CPS, the MSA CPs and the MSCA CPSs, respectively. Changes to the ERCA CPS shall not be public, but shall only be communicated to the relevant parties. Distribution policies for changes to the member

state certificate policies and the MSCA CPSs shall be determined in the relevant documents.

The ERCA shall bring the list of issued certificates, the certificate status information and the symmetric master key status information up to date on the first working day of each week.

2.4 Access Controls on Repositories

All information available via the website shall have read-only access. The ERCA shall designate staff having write or modify access to the information in the ERCA CPS [6].

All information published on the ERCA website shall be available via a secure Internet connection.

3 Identification and Authentication

This chapter describes how identification and authentication (I&A) shall take place for initial and re-key certificate requests and for symmetric key distribution requests.

3.1 Naming

3.1.1 Types of name

3.1.1.1 Certificate subject and issuer

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

Entity	Identifier	Construction
ERCA	Certification Authority Key Identifier (KID)	Nation numeric ('FD') Nation alpha (EC) Key serial number Additional info CA identifier ('01')
MSCA	Certification Authority Key Identifier (KID)	Nation numeric Nation alpha Key serial number Additional info CA identifier ('01')

Table 1 Identifiers for certificate issuers 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.

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 MSCA, see section 4.2.1. The key identifier value is determined according to section 3.1.1.1 with the following modifications:

- NationNumeric: as appropriate for the requesting entity
- NationAlpha: as appropriate for the requesting entity
- 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.
- CA identifier: '01'

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

MSCAs submitting certificate signing requests (CSRs) shall prove possession of the corresponding private key via an internal signature, as specified in section 4.1.1. 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.

3.2.2 Authentication of Organisation Identity

The ERCA and the MSCAs shall define a procedure for the authentication of organisation identities in their Certification Practice Statements. For the ERCA, this procedure is available in the ERCA CPS [6].

3.2.3 Authentication of Individual Identity

The ERCA and the MSCAs shall define a procedure for the authentication of individual identities. For the ERCA, this procedure is available in the ERCA CPS [6].

3.2.4 Validation of Authority

The ERCA and the MSCAs shall define a procedure for the validation of authority. For the ERCA, this procedure is available in the ERCA CPS [6].

3.2.5 Criteria for interoperation

The ERCA and the MSCAs shall not rely on any external certificate authority for the certificate signing and key distribution services they provide to the smart tachograph system.

If the ERCA or an 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 procedures for re-key requests (see sections 4.1.8 and 4.2.9) shall be the same as those described in section 3.2.

3.4 I&A for Revocation Requests

The ERCA shall validate any MSCA certificate revocation requests received from any source (see section 4.1.10) by direct communication with the MSA responsible for the certificate-holding MSCA, through the contact point.

In their CP or CPS, an MSA or an MSCA (as appropriate) shall describe if equipment certificate revocation is allowed, and if so, how revocation requests for equipment certificates will be validated.

4 Life-Cycle Operational Requirements for Certificates and Master Keys

This chapter specifies the message formats, cryptographic mechanisms and procedures for the application and distribution of MSCA certificates and symmetric master keys between the ERCA and the MSCAs.

In either the Certificate Policy or the Certification Practices Statement, an MSA or MSCA (as appropriate) shall describe the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates and symmetric keys for cards, VUs and EGFs, and for the application and distribution of encrypted data for motion sensors between the MSCA(s) and the component personalisers. 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 MSCA Public Key Certificate Application and Issuance

4.1.1 Certificate Signing Requests

Certificate signing requests (CSR) can only be submitted by MSCAs recognised by their MSA via a compliance statement. The European Authority is responsible for recognising MSAs.

A CSR shall be in TLV-format. Table 2 shows the CSR encoding, including all tags. For the lengths, the DER encoding rules specified in [11] shall be used. The values are specified in the remainder of this section.

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

Certificate Expiry Date	m	'5F 24'
Inner Signature	m	'5F 37'
Certification Authority Reference of Outer Signature Signatory	c	'42'
Outer Signature	c	'5F 37'

Table 2 Certificate signing request format

m: required

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 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 Authorisation** shall be used to identify the type of certificate. It consists of the six most significant bytes of the Tachograph Application ID ('FF 53 4D 52 44 54'), concatenated with the type of equipment for which the certificate is intended (Annex 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 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 [8]. 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 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 [14], 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 [8].

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 an MSCA applies for its initial certificate. The outer signature shall be required if an 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 MSCA private key(s). The outer signature authenticates the request. In case an MSCA is subscribed to receive both MSCA_Card and MSCA_VU-EGF certificates, the outer signature shall be placed using a private key linked to a certificate of the same type.

The Outer Signature shall be created over the encoded ECC (CV) Certificate (including the certificate's tag '7F 21' and its length) and the Certification Authority Reference of Outer Signature Signatory field (including the certificate's tag '42' and its length). The signature algorithm shall be ECDSA, as specified in [14], using the hashing algorithm linked to the size of the MSCA key used for signing, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain, as specified in [8].

The 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 to 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 shall ensure that a CSR originating from an MSCA is complete, accurate, and duly authorised. The ERCA shall only sign an MSCA certificate if this is the case.

Checks for correctness, completeness and authorisation shall be 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 authorise the signing of an MSCA certificate.

For each CSR it receives, the ERCA shall verify that

- the transport media is readable; i.e. not damaged or corrupted;
- the CSR format complies with Table 2;
- the request is duly authorised. If an outer signature is in place, the ERCA shall verify the correctness of this signature. In any case, the ERCA shall contact the MSCA as described in the ERCA CPS [6] and verify that a hash calculated over the received CSR matches the hash over the CSR sent by the MSCA;

- the MSCA is entitled to receive the requested type of certificate;
- the Certification Authority Reference contained in the request indicates the ERCA root private key currently valid for signing MSCA certificates;
- the Certificate Holder Reference is unique across the entire Smart Tachograph system. For MSCAs the Certificate Holder Reference is a Certification Authority Key Identifier (KID).
- 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 MSCA_VU-EGF or MSCA_Card certificate of the MSCA;
- If present, the outer signature can be verified using the public point and the domain parameters in the MSCA certificate referenced in the Certification Authority Reference of Outer Signature Signatory field. Moreover, the private key usage period of this key has not expired yet1.

If any of these checks fails, the ERCA shall reject the CSR. The ERCA shall communicate 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 shall proceed to sign the certificate as described in section 4.1.3.

The following information shall be 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 standardised domain parameters OID and 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 hash over the binary CSR data, see section 4.1.1. The hash length shall be linked to the key size of the signing authority, as specified in Annex 1C, Appendix 11, CSM_50;

[1] In case an MSCA fails to request a new MSCA certificate before the end of the private key usage period of their existing certificate(s), they may request the ERCA to waive this requirement. They may also do so in case the existing MSCA certificate is revoked (see section 4.1.8).

- 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 shall be verified afterwards using the ERCA public key. The ERCA shall also write 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 shall update the certificate status information in the ERCA repository. No other notification action is performed.

The ERCA shall retain the transport media with the CSR and archive it in their controlled premises.

The ERCA shall aim 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 shall be 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 shall create the signature over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in [14], 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 [8].

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 shall accept and dispatch CSRs and certificates as e-mail attachments.

The MSCA shall write one to three copies of each certificate signing request to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) or binary (.bin file) format.

The ERCA shall write three copies of each certificate 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 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 [6]. Another paper copy of the data shall be held by the ERCA or the MSCA, respectively.

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

4.1.5 Certificate Acceptance

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

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

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

If any of these checks fail, the 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 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 MSCA certificate, in replacement of an existing certificate. Certificate re-key shall take place either:

- when an 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 MSCA can continue operations after the end of this period;
- following certificate revocation.

Certificate application, processing, issuance, acceptance and publication is 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

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 MSCA private key;
- loss of an MSCA private key;
- MSCA termination;
- MSA or MSCA failure to meet obligations under the Regulation and the ERCA certificate policy.

4.1.10.2 Who can request revocation

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

- the European Authority;
- all MSAs.
- all recognised MSCAs;

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

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

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

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

4.1.10.3 Procedure for revocation request

The certificate revocation procedure is described in the ERCA CPS [6].

4.1.10.4 Revocation request grace period

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

4.1.10.5 Time within which ERCA shall process the revocation request

The ERCA shall process correct, complete and authorised revocation requests within three working days of receipt.

4.1.10.6 Revocation checking requirements for relying parties

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

4.1.10.7 Certificate status issuance frequency

The status of ERCA and MSCA public key certificates shall be retrievable online from https://dtc.jrc.ec.europa.eu/. The ERCA shall maintain the integrity of the certificate revocation status information.

Certificate status information published in the ERCA repository shall be updated on the first working day of each week.

4.1.10.8 Maximum latency for CRLs

Not applicable.

4.1.10.9 On-line revocation / status checking availability

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

4.1.10.10 On-line revocation / status checking requirements

No stipulation.

4.1.10.11 Other forms of revocation advertisements available

None.

4.1.10.12 Special requirements concerning key compromise

Private key compromise is a security incident that shall be processed.

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

In the event of the compromise or suspected compromise of an ERCA private root key, the ERCA shall handle the incident according to a defined security incident handling procedure and shall notify the European Authority without unnecessary delay and at least within 8 hours of detection. The European Authority shall act accordingly.

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 shall be guaranteed during normal working hours.

A list of MSCA certificate status information shall also be downloadable from this website in a common file format (e.g. .csv, Excel).

4.1.12 End of Subscription

Subscription for the ERCA's certificate signing services ends when an MSA decides for MSA termination. Such a change is notified to the ERCA by the MSA as a change to the MSA certificate policy.

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

4.1.13 Key Escrow and Recovery

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

4.2 Master Key Application and Distribution

4.2.1 Key Distribution Requests

Key distribution requests (KDR) can only be submitted by MSCAs recognised by their MSA via a compliance statement. The European Authority is responsible for recognising MSAs.

A KDR shall be in TLV-format. Table 3 shows the KDR encoding, including all tags. For the lengths, the DER encoding rules specified in [11] 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 Authorisation	m	'83'
Key Identifier	m	'84'
Public Key (for ECDH key agreement)	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'

Table 3 Key distribution request format

The version of the profile is identified by the **Request Profile Identifier**. Version 1, specified in Table 3, shall be identified by a value of '00'.

The **Message Recipient Authorisation** shall be 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': KM, motion sensor master key
- '27': KM-WC, motion sensor master key workshop part
- '67': KM-VU, motion sensor master key VU part
- '09': KDSRC, 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 an MSCA shall use a different ephemeral key pair for every key distribution request, the 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 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 MSCA key pair to be used for key agreement. The MSCA shall convert the public point to an octet string as specified in [8], using the uncompressed encoding format.
- The data element Domain Parameters shall contain the object identifier of the set of standardised domain parameters to be used in conjunction with the public point. For more information, see section 4.2.3.

The 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 shall ensure that a KDR originating from an MSCA is complete, accurate, and duly authorised. The ERCA shall only create a key distribution message if this is the case.

Checks for correctness, completeness and authorisation shall be 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 authorise the generation of a key distribution message by the key distribution service.

For each KDR it receives, the ERCA shall verify that

- the transport media is readable; i.e. not damaged or corrupted;
- the KDR format complies with Table 3;
- the request is duly authorised. The ERCA shall contact the MSCA as described in the ERCA CPS [6] and verify 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 key:
    - MSCAs responsible for issuing tachograph cards shall be entitled to receive KM-WC;
    - MSCAs responsible for issuing VUs shall be entitled to receive KM-VU;
    - MSCAs responsible for issuing motion sensors shall be entitled to receive KM;

  Note that in case an MSCA has received both $K_{M\text{-}WC}$ and $K_{M\text{-}VU,}$ it could generate 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[2].

- the requested master key type and version has not been requested by this MSCA before. If this is the case the ERCA shall investigate 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 shall reject the KDR. The ERCA shall communicate the rationale for any request rejection to the MSCA and the MSA.

4.2.2.2 KDM generation, distribution and administration

If all checks succeed, the ERCA shall proceed to prepare the key distribution message (KDM) by determining the symmetric key requested by the MSCA and following the steps as described in section 4.2.3 (from step 2).

The following information shall be recorded in the ERCA database for each key distribution request received:

- the complete KDR originating from the MSCA;
- the complete resulting KDM, if any;
- the standardised domain parameters OID, the ephemeral public point and the key identifier;
- the key type and version of the master key;
- the MAC value in the KDM, if any, see section 4.2.6;
- the hash over the binary KDR data, see section 4.2.1. The hash length shall be linked to the key size of the requested master key, as specified in Annex 1C, Appendix 11, CSM_50;
- a timestamp.

The ERCA shall retain the transport media with the KDR and archive it in their controlled premises.

Once the key distribution message has been generated, the ERCA shall send it to the MSCA as specified in section 4.2.5.

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

[2] This requirement is motivated, in part, by the possible practical difficulties encountered when trying to securely performing an XOR-operation between two keys.

4.2.3 Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys distributed by the ERCA to MSCAs shall be 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 standardised in ISO/IEC 18033-2 [9]. 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 [9];
- Message authentication code algorithm: AES algorithm in CMAC mode, as specified in [17];
- Symmetric encryption algorithm: AES in the Cipher Block Chaining (CBC) mode of operation, as defined in [16].

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, the Message Recipient Authorisation and the Key Identifier.

Step 1

For the generation of its ephemeral public key used for Diffie-Hellman key agreement, the MSCA shall choose one of the standardised 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 [8]. The uncompressed encoding format shall be used. The MSCA shall include the OID of the chosen standardised domain parameters and the octet string representing the public point in the KDR, which is sent to the ERCA.

Step 2

The ERCA shall generate an ephemeral key pair, using the standardised domain parameters specified in the received KDR. The ERCA shall use the ECKA-DH algorithm as defined in [8] 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 [8] (Conversion between Field Elements and Octet Strings).

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 shall use the key derivation function KDF2(*x, l*) defined in [9]. 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. if a 192-bits key is to be distributed), the ERCA shall pad the symmetric key to be distributed using padding method 2 defined in [15]. Subsequently, the ERCA shall encrypt the (padded) key with AES in the Cipher Block Chaining (CBC) mode of operation, as defined in [16], using K_{ENC} with an interleave parameter *m* = 1 and an initialisation vector SV consisting of binary zeros:

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

Step 5

The ERCA shall concatenate the encrypted symmetric key with a string *S*, which is the concatenation of the values (excluding tags and lengths) of the Message Recipient Authorisation and the Key Identifier used in the key distribution message (see section 4.2.4)

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

Using K_{MAC}, the ERCA then shall compute a MAC over the concatenation of the Encrypted symmetric key and *S*, using the AES algorithm in CMAC mode, as specified in [17]. The length of the MAC shall be linked to the length of the AES session keys, as specified in Appendix 11 CSM_50.

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

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 the MAC. As described in section 4.2.6, the MSCA will use these values to verify the authenticity of the key distribution message.

4.2.4 Key Distribution Messages

After performing the Master Key application processing (see section 4.2.2), the ERCA shall construct a key distribution message as shown in Table 4. For the lengths, the DER encoding rules specified in [11] 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 Authorisation	m	'83'
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	m	'84'
Public Point of the ERCA for ECDH key agreement	m	'86'
Encrypted symmetric key	m	'87'
MAC	m	'88'

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

The **Public Point** shall contain the public point of the ephemeral ERCA key pair used for key agreement, see section 4.2.3. The ERCA shall convert the public point to an octet string as specified in [8], 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 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}.

The key distribution message shall be 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 shall accept and dispatch key distribution requests and key distribution messages as e-mail attachments.

The MSCA shall write one to three copies of each key distribution request to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) or binary (.bin file) format.

The ERCA shall write 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 [6]. 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 courier in the JRC controlled area.

4.2.6 Master Key Acceptance

The courier signs for receipt of the key distribution message at the ERCA premises.

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

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with Table 4;
- the message is genuine. The MSCA shall do this by contacting the ERCA as described in the ERCA CPS [6] and verifying that the MAC in the received KDM matches the MAC in the KDM sent by the ERCA;
- the master key type and version in the message matches the requested type and version;
- the public point specified in the message is on the curve specified by the key distribution request sent by the MSCA to the ERCA.

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

If all of these checks succeed, the MSCA shall

- use the ECKA-DH algorithm to derive a shared point (K_x, K_y), as described in step 3 in section 4.2.3, using the MSCA's ephemeral private key indicated by the key identifier in the message and the ERCA's ephemeral public key. The MSCA shall verify that the shared point is not the infinity point; if it is, the MSCA shall abort the process and contact the ERCA. Else, the MSCA shall form the shared secret K by converting K_x to an octet string as specified in [8] (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;
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3. If this verification fails, the MSCA shall abort the process and contact the ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3. The MSCA shall verify that the padding of the decrypted key, if any, is correct. If this verification fails, the MSCA shall abort the process and contact the ERCA.

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

After successful recovery of the master key, or when the key distribution process is aborted and no KDM renewal (see section 4.2.8) is initiated, the MSCA shall securely destroy its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

4.2.7 Master Key Usage

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

4.2.8 KDM Renewal

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

KDM renewal may take place only if the original transport media received at the MSCA are 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 [6].

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 shall be published on the ERCA website, together with its version number and length.

To receive the new version, MSCAs 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 is the same as for the initial key.

4.2.10 Symmetric Key Compromise Notification

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

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

4.2.11 Master Key Status Service

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

Master key status information published in the ERCA repository shall be updated on the first working day of each week.

The availability of the website mentioned above shall be guaranteed during normal working hours.

4.2.12 End of Subscription

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

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

4.2.13 Key Escrow and Recovery

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

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

For both the ERCA and MSCAs:

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.

An off-site backup facility for ERCA critical data shall be implemented.

5.2 Procedural Controls

For both the ERCA and MSCAs:

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 ERCA and MSCA 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[3] 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 ERCA and MSCA systems shall ensure effective user administration and access management;
- The ERCA and MSCA 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;
- ERCA and MSCA personnel shall be identified and authenticated before using the ERCA or MSCA systems;
- ERCA and MSCA personnel shall be accountable for their activities, which shall be logged in event logs as described in section 5.4;

[3] Which data shall be considered confidential is specified in section 9.3.

The ERCA and the MSCAs shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. The ERCA and the MSCAs shall ensure that the ISMS policies address personnel training, clearances and roles. The ERCA ISMS implementation shall conform with the requirements in [19] and [20] and related standards and guidelines. The MSCA ISMS implementations should conform with the requirements described in ISO 27001 [18].

5.3 Personnel Controls

For the ERCA:

- Personnel shall be employees of the ERCA, possessing the expert knowledge, experience and qualifications necessary for the services offered and appropriate to the job function.

For MSCAs:

- The MSCA responsibilities may be outsourced to a specialised company, or personnel from contractors may be hired to carry out the MSCA responsibilities.
- All personnel involved with the MSCA 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 MSCA directly, personnel from a specialised company to which tasks have been outsourced or personnel from contractors.

For both the ERCA and MSCAs:

- Personnel training shall be managed according to a training plan described in the respective CPS.
- Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the respective CPS.
- Trusted roles, on which the security of the operation is dependent, shall be clearly identified in the respective CPS. These 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. No single person shall be authorised to simultaneously perform more than one of the trusted roles.

5.4 Audit Logging Procedures

All significant security events in the ERCA or MSCA 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 ERCA or MSCA 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 ERCA or 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 CPS.

5.5 Records Archival

For both the ERCA and MSCAs:

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 ERCA or MSCA 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

The ERCA shall generate new ERCA key pairs and new symmetric master keys in due time, according to Annex IC Appendix 11 [2].

MSCAs shall generate new MSCA key pairs as needed. After a MSCA has generated a new key pair, it shall submit a certificate re-key request as described in section 4.1.8.

The ERCA and MSCAs shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in this ERCA certificate policy.

5.7 Compromise and Disaster Recovery

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

The ERCA and the MSCAs 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 ERCA and the MSCAs 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:

a) compromise or theft of a private key and / or a master key;

b) loss of a private key and / or a master key;

c) IT hardware failure.

For the ERCA, the remaining clauses in this section specify which measures must be taken in case a disaster occurs. For the MSCAs, the MSA certificate policy shall likewise describe appropriate disaster recovery mechanisms. These mechanisms shall not depend on the ERCA response times.

In the event of **compromise or theft** of an ERCA root private key and / or a symmetric master key, the ERCA shall immediately inform the European Authority and the MSCAs. The EA shall take appropriate measures within a reasonable time period.

There is effectively[4] no recovery form a **loss** of the ERCA root key or of the master keys. 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.

[4] A possible scenario would be to apply exceptional measures within one of the MSCAs, such that the symmetric keys stored in their HSMs can be exported and imported again in an HSM at the ERCA. However, such measures should be viewed as last resort only.

5.8 CA or RA Termination

In the event of termination of ERCA activity by the currently appointed organisation (see section 1.5.2), the European Authority shall appoint a new organisation responsible for implementation of this policy and for the provision of key certification and key distribution services to the Member States. The current organisation shall transfer its ERCA-related assets to the European Authority ensuring that confidentiality and integrity are maintained.

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

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

6 Technical Security Controls

6.1 Key Pair and Symmetric Key Generation and Installation

The ERCA and the MSCAs shall generate private keys in accordance with Annex IC Appendix 11 [2]. Additionally, the ERCA shall generate master keys in accordance with Annex IC Appendix 11 [2]. The ERCA shall not generate key pairs for its subscribers (MSCAs).

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 ERCA shall have available a Test ERCA system for interoperability test purposes, according to the Regulation. The Test ERCA system shall be a separate system and shall have its own ERCA root keys and symmetric master keys. The Test ERCA system shall be able to sign test certificates and distribute symmetric test keys using the processes described in sections 4.1 and 4.2.

Similarly, the MSCAs should have available a Test MSCA system for interoperability test purposes, according to the Regulation. If present, the 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 described in 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 and encrypted data for motion sensors to component personalisers.

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

The ERCA and MSCAs 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 and used in a trustworthy dedicated device which:

- is certified to EAL 4 or higher in accordance with ISO/IEC 15408 [10] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [12] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised 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 ERCA certificate policy contains various functional requirements for the HSMs used in the ERCA and MSCA systems. 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.

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

The ERCA and MSCA 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 ERCA and MSCA 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 ERCA and MSCA 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 allowed for back-up and recovery purposes. In addition,

- For the ERCA, export of master keys is allowed in encrypted form only, and only in response to a valid key distribution request from a MSCA, by personnel in trusted roles under at least dual person control.
- For the MSCAs, export of $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ 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.

Master key import and export for any other reason is forbidden.

At the end of private key usage period of an ERCA or MSCA private key (as specified in Appendix 11 of Annex IC), the ERCA or MSCA (as applicable) 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 ERCA and MSCA shall destroy all copies of the key in their possession[5] 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 ERCA or MSCA 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 ERCA and MSCA public key certificates and hence the public keys shall be archived indefinitely.

The validity periods of all ERCA root certificates, ERCA link certificates and MSCA certificates shall comply with Annex IC Appendix 11 [2].

In accordance with Annex IC Appendix 11 [2], the private key usage period of ERCA private keys shall be 17 years. The private key usage period of MSCA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate. The ERCA and the MSCAs shall not use a private key after the private key usage period is over.

[5] Note that $K_{M\text{-}WC}$, $K_{M\text{-}VU}$ and K_{DSRC} are also stored on VUs and tachograph cards. The copies of these keys residing on a VU or card will not be destroyed until the moment that that VU or card is taken out of service.

6.4 Activation Data

In the CPS [6], the ERCA shall describe the number of persons in a trusted role that are required in order to activate the system and generate, use or destroy an ERCA private key or symmetric master key. Similarly, in their CP or CPS, an MSA or an MSCA (as appropriate) shall describe 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.

Generating, importing, using or destroying ERCA private keys, MSCA private keys and/or symmetric master keys stored in an HSM shall only be possible if the number of trusted persons specified in the CP or CPS for the specific task 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 ERCA or MSCA software and the system on which this software is running, user authentication shall take place using proper means (e.g. by a passphrase).

6.5 Computer Security Controls

The ERCA and the MSCAs 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 ERCA or MSCA documentation. ERCA and MSCA computer systems shall be arranged and managed conform these procedures.

6.6 Life Cycle Security Controls

The ERCA and the MSCAs shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built into ERCA and MSCA IT 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 ERCA and the MSCAs shall devise and implement their 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, can be effectively controlled. In particular, taking the CA signing system completely off-line ('air gapping') shall be considered.

6.8 Timestamping

The time and date of an event shall be included in every audit trail entry. The ERCA and MSCA CPS shall describe how time is synchronised 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 [2]:

Data Object	Field ID	Tag	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	C	'7F 21'	var	
Certificate Body	B	'7F 4E'	var	
Certificate Profile Identifier	CPI	'5F 29'	'01'	INTEGER (0…255)
Certification Authority Reference	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation	CHA	'5F 4C'	'07'	Certificate Holder Authorisation
Public Key	PK	'7F 49'	var	
Standardised Domain Parameters OID	DP	'06'	var	OBJECT IDENTIFIER
Public Point	PP	'86'	var	OCTET STRING
Certificate Holder Reference	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature	S	'5F 37'	var	OCTET STRING

Table 5 Certificate profile

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 published. For the ERCA, the status of all certificates issued can be found on the website https://dtc.jrc.ec.europa.eu/.

7.3 OCSP Profile

No OCSP shall be used.

8 Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

A full and formal audit on the ERCA operation shall be performed annually. The European Authority may order a compliance audit by an auditor at any time at its discretion. The ERCA audit shall establish whether the requirements on the ERCA described in this document are being maintained.

On the national level, a full and formal audit on the operations of at least those organisations that generate or manage private or symmetric keys shall be performed by order of the relevant Member State Authority. The MSA may at its discretion decide in the MSA Policy that also other organisations playing a role in the overall equipment issuing process in the country concerned must be audited.

A national audit shall establish whether the requirements on the organisation to be audited, as described in the MSA certificate policy, are being maintained. The MSA shall perform the first audit within 12 months of the start of the operations covered by the MSA certificate policy. 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 MSA certificate policy, the MSA shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in the 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 an ERCA compliance audit shall first be approved by the European Authority. Any person selected or proposed to perform a compliance audit on the national level shall first be approved by the relevant Member State Authority.

The names of the auditors which will perform the audits shall be registered. Such 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 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 organisation being the subject of the audit.

8.4 Topics Covered by Assessment

The ERCA audit shall cover compliance to this CP, the ERCA CPS [6] and the associated procedures and techniques documented by the ERCA.

An audit on the national level shall cover compliance to the MSA certificate policy, the MSCA CPS and the associated procedures and techniques documented by the organisation to be audited.

The scope 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 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 discovered by the auditor, corrective actions shall be taken immediately by the organisation that was audited. After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.6 Communication of Results

For an ERCA audit, the independent auditor shall report the full results of the compliance audit to the ERCA and the EA.

For an audit on national level, the independent auditor shall report the full results of the compliance audit to the organisation that was audited and to the relevant MSA. The 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 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 ERCA system is those of ERCA and MSCA representatives. The only personal data processed or stored in an MSCA system is those of ERCA, MSCA and component personaliser representatives.

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

9.5 Intellectual Property Rights

The ERCA owns the intellectual property rights of the ERCA software.

9.6 Representations and Warranties

ERCA guarantees that the ERCA shall operate according to this CP and the ERCA CPS[6].

MSCAs shall operate according to this CP, their MSA's CP and their own CPS.

9.7 Disclaimers and Warranties

The ERCA 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

The European Commission 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 unauthorised use of certificates issued by the ERCA, and use of certificates beyond the prescribed use defined by this ERCA Certificate Policy and the Certification Practice Statement [6];
- caused by fraudulent or negligent use of certificates and/or certificate status information issued by the ERCA.

The European Commission 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 ERCA, or its associated public/private key pair, used by a subscriber or relying party;
- any symmetric key distributed by the ERCA, used by a subscriber or relying party.

Issuance of certificates and key distribution messages by the ERCA does not make the European Commission or the ERCA 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 ERCA is not an intermediary to transactions between subscribers and relying parties. Claims against the ERCA are limited to showing that it operated in a manner inconsistent with this ERCA certificate policy and the CPS [6].

9.9 Indemnities

No stipulation.

9.10 Term and Termination

This ERCA Certificate Policy is valid from the moment the ERCA becomes operational. It shall be valid until further notice.

The validity of this CP ends when the ERCA stops operating[6] or when the ERCA 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 European Commission.

Notice of severance or merger may result in changes to the scope, management and/or operation of the ERCA. In such an event, this ERCA certificate policy and the ERCA CPS [6] 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.

[6] Note that this implies that the Smart Tachograph system as a whole stops operating. Section 5.8 covers the situation that the ERCA responsibilities are transferred to a different organisation.

9.12 Amendments

This CP is issued under responsibility of the European Authority. The EA, in cooperation with the ERCA, may revise this CP if it deems this necessary. It is allowed to make editorial or typographical corrections to this policy without notification to the MSAs and without an increase in version number. It is allowed to change the contact information in section 1.5 with notification to the MSAs, but without change to the document version number.

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

1. The MSAs and the ERCA may submit proposals for change to the ERCA certificate policy to the European Authority at any time.
2. The European Authority shall distribute any proposal to change the ERCA certificate policy to all MSAs and to the ERCA.
3. The European Authority shall set an appropriate period for comments. The MSAs and the ERCA may comment on the proposed changes within the defined period for comments.
4. The European Authority shall consider the comments and shall decide which, if any, of the notified changes to implement.
5. The European Authority shall notify the MSAs and the ERCA about its decision, and shall set an appropriate period for the changes to be implemented.
6. The European Authority shall publish a new version of the ERCA certificate policy including all implemented changes, accompanied by an increase in the version number of the document.

9.13 Dispute Resolution Procedures

Any dispute related to key and certificate management between the European Commission and an organisation or individual outside of the European Commission 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 European Authority.

9.14 Governing Law

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

References

1. Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014, Official Journal of the European Union L60
2. Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139, including ref. 3.
3. Commission Implementing Regulation (EU) 2018/502, amending Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 85
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
6. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0, Month year
7. Smart Tachograph - Equipment Interoperability Test Specification, JRC, version 1.0, Month year
8. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28
9. ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition, 2006-05-01
10. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 – 2014
11. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
12. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15
13. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001
14. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
15. ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
16. ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher. Third edition, 2006-02-01
17. National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
18. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01

19. 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. Commission Decision 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission

List of Figures

List of Tables

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

Freephone number (*)**:**

00 800 6 7 8 9 10 11

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

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

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

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

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

Priced publications:

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

KJ-NA-29118-EN-N

JRC Mission

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

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi: 10.2760/409258

ISBN 978-92-79-79909-9