EU-MIDT

Plenary

EU-MIDT/PLE/009-2006

Digital Tachograph System

ERCA Certification Practices Statement version 1.0

PREPARED BY: European Communities
DATE: 24/04/2006
EU-MIDT Plenary – 009-2006

REF : EU-MIDT/PLE/009-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	European Communities		2004
CHECKED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	24/04/2006
APPROVED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	24/04/2006
ISSUED BY	Secretariat	MIDT	17/05/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE
Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit
T.E.M.P.E.S.T Laboratory
TP 361
I-21020 Ispra (Va)

Special Publication I.04.178

Digital Tachograph System
European Root Certification Authority

Certification Practices Statement

Version 1.0

Administrative Agreement 17398-00-12 (DG-TREN)

Blank page

LEGAL NOTICE

Neither the European Commission nor any person
acting on behalf of the Commission is responsible for
the use which might be made of the following information.

A great deal of additional information on the
European Union is available on the Internet.
Ot can be accessed through the Europa server:
(http://europa.eu.int)

S.P.I.04.178

Blank page

Table of Contents

Blank page

1 INTRODUCTION

The European Commission is responsible for the European Root Certification Authority (ERCA) of the cryptographic key management infrastructure supporting the digital tachograph system introduced by Council Regulation 3821/85 as amended by Council Regulation 2135/98 [1], and Commission Regulation 1360/2002 [2], as last amended by Commission Regulation 432/2004[].

This key management infrastructure consists of systems, products and services, which provide and manage:

- digital tachograph public-key certificates;
- motion sensor data encryption keys.

The purpose of this document is to describe the certification practices implemented by the ERCA to ensure its trustworthiness.

This document has been drafted to comply with the requirements of the ERCA Policy [3] for the digital tachograph system. Users of this document should consult the reference [3] for information concerning the underlying policies for the ERCA Certification Practice Statement (CPS).

The ERCA CPS is based on the framework presented in IETF RFC 3647 [4].

The following typographical conventions are used in this document:

- Normal font: implemented and operational
- *Italic font: not yet implemented, for future developments*

1.1 Overview

This document is intended for use by the European Commission and others who need to assess the trustworthiness of the ERCA and determine its suitability in meeting the requirements of the digital tachograph system.

The cryptographic key management system (see Figure 1.1) is required to support the security mechanisms defined in:

- Commission Regulation 1360/2002, Annex I(B) Appendix 11 Common Security Mechanisms [5]
- ISO / IEC 16844-3 Road vehicles, Tachograph systems, Part 3: Motion sensor interface [6]

The ERCA is operated under the authority and responsibility of the European Authority (EA), defined in the ERCA Policy. National authorities are responsible for the operation of certification authorities (CA) and component personalisers (CP).

The ERCA generates and uses a single RSA key pair for the purpose of certifying RSA public keys generated by the NCAs.

The NCAs certify RSA keys inserted into tachograph vehicle units and smart cards by component personalisers (CPs). The vehicle units are fitted to trucks; different types of smart cards are issued to truck drivers, workshops, controllers / law enforcers, and road-haulage companies.

The technical specifications of the vehicle units do not allow the ERCA RSA key to be changed, however the NCAs change their keys at regular intervals.

The public key certificate format used by the digital tachograph is proprietary and incompatible with the X.509 public key certificates whose use is assumed, but not required, by IETF RFC 3647 [4].

The ERCA generates, splits, and distributes a single symmetric cryptographic key required for securing vehicle motion data, according to mechanisms defined in the standard ISO / IEC 16844-3 [6].

The master key (Km) is used by a NCA to encrypt identification data for insertion into motion sensors. The master key is split into two parts (KmVU and KmWC) which are inserted into the vehicle units and the workshop cards by a component personaliser (CP).

To assure the confidentiality of the the motion sensor keys during transport from the ERCA to a NCA or CP, the ERCA encrypts the motion sensor key using an RSA public key, to produce a key distribution message (KDM). The RSA keys used in KDM production are generated by the NCA or the CP and sent to the ERCA in a key distribution request (KDR).

The needs of the NCA or CP to receive the different motion sensor keys are defined in the service agreement established between the ERCA and the national authority.

Other documents drafted for the digital tachograph system refer to Member State (MS) instead of national (N) certification authorities. This CPS shall refer to nations, instead of Member States, for the simple reason that not all of the nations affected by this CPS are members of the European Union.

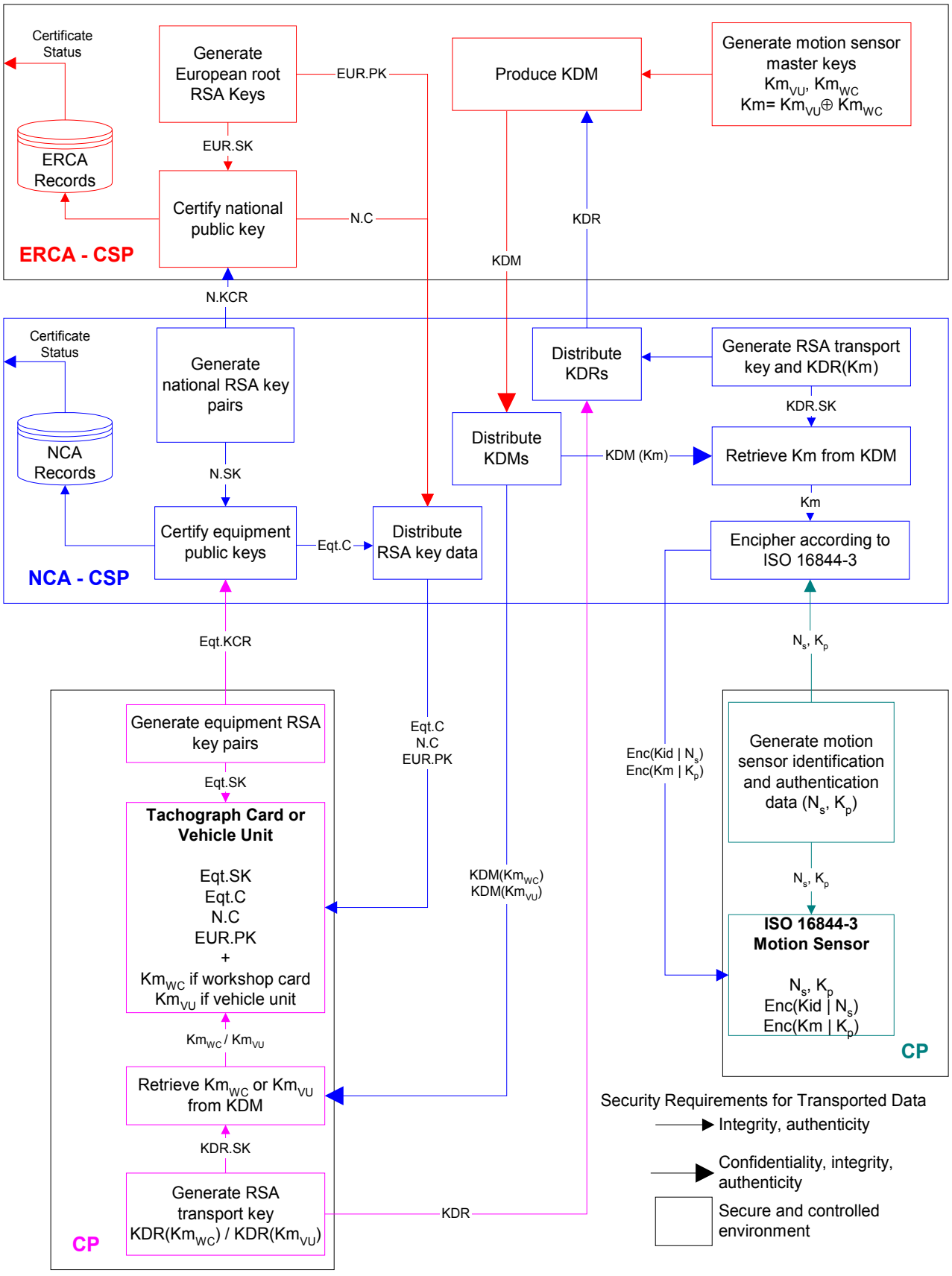


Figure 1.1 Overview of Annex I(B) digital tachograph key management process

1.2 Document Name and Identification

This document is the Digital Tachograph System European Root Certification Authority Certification Practices Statement.

This document is published as a Special Publication of the European Commission. The publication reference appears on the cover page, and in the centre of the footer of each page.

1.3 Participants

This CPS is designed to satisfy the requirements of the digital tachograph system only.

1.3.1 Certification authorities

The ERCA is operated under the authority and responsibility of the European Commission.

The NCAs and CPs are operated under the authority and responsibility of the appropriate national authorities. These may be organisational units of Ministries of Transport, vehicle or road inspectorates, or other entities, as determined by national practices. The NCAs are subjects of the ERCA.

1.3.2 Registration authorities

The ERCA registration authority (RA) is internal to the ERCA. The ERCA RA registers a national CA on completion of the approval process laid down in the ERCA Policy.

The approval process consists of a review of national policy documents provided by the national authorities. The review establishes whether or not the national policy conforms to the requirements defined in the ERCA Policy.

The ERCA RA registers a NCA only if the outcome of the policy review provides sufficient grounds to judge that the requirements of the ERCA Policy will be met.

The national RAs implement the systems, products, and services required for tachograph card issuing and vehicle unit personalisation.

RAs are responsible for maintaining the binding between certificate subject identifiers and physical persons or legal entities.

1.3.3 Subscribers

Only NCAs are subscribers of the ERCA public key certification service. The ERCA services required by a NCA are defined in the service agreement between the ERCA and the relevant NA.

Tachograph card and vehicle unit personalisers are subscribers of the NCA public key certification services.

Motion sensor personalisers are subscribers of the NCA data encryption service

1.3.4 Relying Parties

Relying parties are any other entities which require access to the information published in the ERCA repository.

1.3.5 Motion Sensor Key Recipients

Recipients of the motion sensor keys are:

- NCAs providing the data encryption service to motion sensor personalisers;
- personalisers of workshop cards;

- personalisers of vehicle units.

The recipients of motion sensor keys are identified in the service agreement between the ERCA and the relevant NA.

1.4 Certificate Usage

Digital tachograph public key certificates shall be inserted into digital tachograph components, as required by the mutual authentication process described in requirement CSM_020 [5].

Digital tachograph public key certificates may be used in applications related to the digital tachograph system (e.g. calibration equipment used by workshops, data download equipment used by controllers, fleet and / or freight management systems used by road haulage companies etc.).

Digital tachograph certificates shall not be used for any other purposes.

1.5 Key Distribution Message Usage

Key distribution messages shall be used for the sole purpose of securely transferring a motion sensor key from the ERCA to a NCA or CP.

1.6 Policy Administration

1. This CPS is drafted, maintained, and updated by the Traceability and Vulnerability Assessment unit of the Joint Research Centre:

   Digital Tachograph Root Certification Authority
   Traceability and Vulnerability Assessment Unit
   European Commission
   Joint Research Centre, Ispra Establishment (TP.361)
   Via E. Fermi, 1
   I-21020 Ispra (VA)

   Tel. +39-0332-789515
   Fax +39-0332-785680

   The Traceability and Vulnerability Assessment Unit of the Joint Research Centre is the ERCA Operating Agent.

2. Questions about this CPS should be addressed to:

   Dr. James Bishop
   Tel. +39-0332-789515
   Fax +39-0332-785680
   e-mail: james.bishop@jrc.it

3. Questions about ERCA operations should be addressed to the Operations Manager of the Operating Agent. The Operations Manager is appointed by the Operating Agent Head of Unit.
4. The EA shall determine that the ERCA CPS complies with the ERCA Policy for the digital tachograph system.
5. The EA's statement of compliance is based on a security review performed by the European Commission's Security Directorate [7], and the results of functional tests performed by the ERCA OA.

1.7 Definitions and Acronyms

Asymmetric encryption: encryption process in which one key is used to encipher a message, and a different key is used to recover the message from the ciphertext.

Central alarm station: an installation which provides for the complete and continuous alarm monitoring, assessment and communications with guards, facility management and the response force.

Guard: a person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.

Inner area: an area inside a protected area where Category I nuclear material is used and/or stored.

Intrusion detection: detection of an intruder by a guard or by a system comprising of a sensor(s), transmission medium and control panel to annunciate an alarm.

Key escrow: the submission of a copy of a key to an entity authorised to use this copy for some purpose other than returning it to the originating entity.

Protected area: an area under surveillance, containing Category I or II nuclear material, and/or vital areas surrounded by a physical barrier.

Symmetric encryption: encryption process in which the same key is used to encipher a message, and to recover the message from the ciphertext.

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CP	Component Personaliser
CPI	Certificate Profile Identifier
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DES	Data Encryption Standard (symmetric encryption scheme)
EA	European Authority
ENI	ESSOR Nuclear Island
EOV	End Of Validity
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
Km	Motion sensor master key
Km_{VU}	Motion sensor master key inserted in vehicle unit
Km_{WC}	Motion sensor master key inserted in workshop card
NA	National Authority
NCA	National Certification Authority

OA	Operating Agent
OE	Operational Entity (used to refer to both a NCA and a CP)
OM	Operations Manager
PK	RSA public key
PKI	Public Key Infrastructure
PR	Permanent Representation of Member State
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SAS	Single access system
SK	RSA secret key
TDES	Triple DES

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The ERCA Operations Manager (see Section 1.6) is responsible for the public web-site http://dtc.jrc.it, which is the repository for ERCA documents, certificates, and certificate status information.

The certificates produced by the ERCA are also maintained in a stand-alone database.

2.2 Publication of ERCA information

The ERCA publishes the following information on its web-site:

- ERCA Policy;
- ERCA CPS (this document);
- ERCA Policy and CPS change proposal information;
- compliance statements for the ERCA and for each national policy;
- ERCA public key;
- all public key certificates issued by the ERCA;
- public key certificate status information.

The ERCA Policy and CPS documents are published as Special Publications according to European Commission DG-JRC publication procedures.

The ERCA compliance statement is issued by the European Authority (EA) on completion of the ERCA approval process. This process is defined by the EA identified in the ERCA Policy.

The national policy compliance statements are issued by the ERCA on completion of the national policy review process defined in the ERCA Policy.

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

- it has issued the certificate to the corresponding national CA;
- that the information stated in the certificate was verified in accordance with this CPS;
- that the national CA has accepted the certificate.

2.3 Frequency of publication

Information relating to Policy and CPS changes are published according to the schedules defined by the change (amendment) procedures laid down in each document.

The list of certificates issued by the ERCA, and certificate status information are brought up to date on the first working day of each week.

2.4 Access controls on repositories

All information available via the web site has read-only access. The ERCA OM designates staff having write or modify access to the information published.

All information published on the ERCA web-site is digitally signed, using a key certified by an external PKI.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The concept of name as identifier of a physical person or a legal entity (subject) does not apply to the public key certificates or the KDMs produced by the ERCA. The names of, and the contact information for, the OEs to which the ERCA provides its services are defined in the service agreement established between the NA and the ERCA.

Certificate issuer and certificate subject are identified by fixed-length octet strings containing information required by the mutual authentication protocol between tachograph components defined in Annex I(B) Appendix 11 [5], requirement CSM_020.

3.1.1 Types of Name

Certificate and Key Distribution Message Issuer

The issuer of a digital tachograph public key certificate, and of a motion sensor KDM is identified by:

- the Certification Authority Reference (CAR): an 8-octet string defined in [2], Annex I(B) Appendix 1 – Data Dictionary, Section 2.36 CertificationAuthorityKID.

The CAR is also used during the mutual authentication procedure between tachograph components to identify the public key used to verify a certificate.

Certificate Subject

The subjects of digital tachograph public key certificates issued by the ERCA are the NCAs. These entities are identified by:

- the Certificate Holder Reference (CHR): an 8-octet string defined in [2] Annex I(B) Appendix 1, Section 2.36 CertificationAuthorityKID;
- the Certificate Holder Authorisation (CHA): a 7-octet string defined in [2] Annex I(B) Appendix 1, Section 2.34 and including the EquipmentType: 1 octet as defined in [2] Annex I(B) Appendix 1, Section 2.52. For public key certificates issued by the ERCA, the EquipmentType designates a certification authority.

The CHR appears in printouts and vehicle unit data downloads. The EquipmentType encoded in the CHA is used during the mutual authentication procedure, and selects one of the four operating modes of the vehicle unit (e.g. operating, calibration, control, company).

Key Distribution Message Recipient

The recipients of motion sensor KDMs may be NCAs or CPs. For the purposes of motion sensor key distribution, each KDR is identified by:

- the Key Identifier (KID): an 8-octet string defined in ERCA Policy [3] Annex D.1.
- the Message Recipient Authorisation (MRA): a 7-octet string defined in ERCA Policy [3] Annex D.1.

The KID uniquely identifies the RSA public key used to encrypt the motion sensor key. The MRA identifies the motion sensor key.

3.1.2 Need for names to be meaningful

The meanings of the certificate issuer, certificate subject, and KDM recipient are defined in [2] Annex I(B) Appendix 1; and ERCA Policy [3] Annex D.

3.1.3 Anonymity or pseudonymity of subscribers

The binding between a name and physical persons (e.g. drivers, control officers) or legal entities (e.g. NCAs, workshops, haulage companies) is assured by the RA; it cannot be established from the contents of the public key certificates.

The names used by the ERCA for the purposes of digital tachograph key certification and distribution are therefore pseudonyms for the ERCA subscribers.

Subscriber anonymity is not allowed.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

For the mutual authentication process (see [5] CSM_020) to function correctly, the certificate issuer identifier must uniquely identify an RSA key pair.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Subscribers submitting KCRs and KDRs are required to prove possession of the corresponding private key. The KCR and KDR protocols are defined in the ERCA Policy [3].

KCRs and KDRs consist of two parts: plaintext, and a digital signature of the plaintext. The plaintext always includes an RSA public key. The digital signature of the plaintext is produced with the corresponding private key.

Verification of the digital signature using the public key included in the plaintext proves:

- possession of the private key;
- integrity of the plaintext.

Signature verification is performed by the ERCA RA. If signature verification fails, the request is rejected.

3.2.2 Authentication of organisation identity

The identity of the NA responsible for the OEs is determined by the European Authority (EA - see ERCA Policy, Section 2) by means of a request for information transmitted through the Permanent Representations of the national governments (Member States and other countries participating in the digital tachograph system), according to the procedure depicted in Table 3.1.

Step	EA	ERCA	MSA	PR	Flow Chart	Supporting Document	Proof
1	R			I	EA sends application form to MS		Covering letter
2			R	I	MS returns completed form to EA	Explanatory note	Application form
3	R			I	EA confirms application		Letter of confirmation
4	R	I			EA instructs MSA to submit policy to ERCA		Instruction
					MSA identified and authenticated		

A = Authorises C = Collaborates D = Decides I = Informed R = Responsible

Table 3.1 NA Identification Procedure

The procedure assumes that official communications through the Permanent Representations of national governments are subject to checks and controls sufficient to assure their authenticity, and to establish an audit trail.

The objective of the procedure is to establish a single point of contact between the NA and the ERCA, for the purposes of:

- national policy approval;
- establishment and administration of the service agreement between the NA and the ERCA;
- identification and authentication of couriers transporting KCRs, KDRs, public key certificates and KDMs on behalf of the NCAs;
- authentication of KCRs and KDRs received by the ERCA from an OE;
- authentication of public key certificates and KDMs received by the OE from the ERCA;
- authentication of certificate revocation requests received by the ERCA;
- notification of ERCA Policy or CPS changes;
- notification of national policy changes.

All communications shall be in written form, and subject to the registration procedures for correspondence in force within the European Commission.

3.2.3 Authentication of individual identity

The subjects of certificates issued by the ERCA are not individuals.

This section only addresses identification and authentication requirements for the couriers who transport key certification requests, key distribution requests, public key certificates, and key distribution messages between the OEs and the ERCA.

The procedure for identifying and authenticating couriers is depicted in Table 3.2.

The NA defines the set of credentials required to identify couriers authorised to transport KCRs, KDRs, public key certificates, and KDMs between the OE and the ERCA. The set of credentials is documented in annex to the service agreement between the NA and the ERCA.

At minimum, the credentials are required to demonstrate the courier's:

- personal identity;
- affiliation with the NA or OE;
- authorisation to transport specific items (e.g. KCRs / KDRs / certificates / KDMs).

Access of couriers to the JRC controlled area is managed through the normal procedures for visitors. This requires notification of courier identity, affiliation, and authorisation to the ERCA OM not less than five working days before the visit.

Access is granted only if a visitor presents valid personal identification documents at the JRC Reception. Personal data are held in the JRC visitor log for a limited period of time, in conformity with privacy legislation.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

The ERCA validates courier authorisations by direct communication with the NA through the contact point specified in see Section 3.2.2.

Step	ERCA	NA	OE	CO	Flow Chart	Supporting Document	Proof
1	I	R	I		NA defines CO credentials		List of credentials
2	I	R	C		NA nominates CO		Letter of nomination
3	R			I	ERCA establishes CO as visitor to JRC		Visitor log
4	R	C			Authentication of credentials		Credentials presented
5	D				Credentials valid? (Yes / No)	ERCA CPS	
6	R				Courier identified and authenticated		ERCA log
7	R	I	I		Rationale provided to CO; Courier refused		Rationale

A = Authorises C = Collaborates D = Decides I = Informed R = Responsible

Table 3.2 Courier identification procedure

If the courier's credentials are deemed to be valid, the ERCA shall accept the KCR(s) / KDR(s) presented by the courier for further processing.

Otherwise, all KCRs / KDRs presented by the courier shall be rejected. The rationale for rejection is provided to the courier in writing, and communicated to the NA and the OE.

3.2.6 Criteria for interoperation

The ERCA is not required to rely on any other CA for the services it provides to the digital tachograph system. The ERCA shall rely on an external PKI to certify any keys used for purposes of authentication (e.g. digital signature of electronic documents published by the ERCA) or encryption. The ERCA shall review and approve the CPS of external certification service providers prior to applying for certification services as a subject CA.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key requests

As for Section 3.2 Initial Identity Validation.

3.3.2 Identification and authentication for re-key after revocation

As for Section 3.2 Initial Identity Validation.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests received by the ERCA OM from any source shall be validated by direct communication with the NA responsible for the certificate holding NCA, through the contact point specified in Section 3.2.2.

A NCA shall replace revoked certificates by applying the Routine Rekey procedure in the shortest possible time.

Changes to certificate status information are described in Section 4.9.

3.5 Identification and Authentication for Motion Sensor Key Redistribution

Redistributing a motion sensor master key means that a new key distribution message is created with:

- the same Certification Authority Reference;
- a new Key Identifier;
- a new public key.

Identification and authentication requirements are as for Section 3.2 Initial Identity Validation.

However, as motion sensor master key distribution needs to be performed only once for each OE identified in the national policy, all requests for redistribution shall initiate an investigation which shall establish:

- the rationale for redistribution;
- the risk of compromise of the key originally distributed.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The ERCA only accepts key certification requests submitted by a NCA approved by the relevant NA. NCA approval is performed according to national practices, and is attested by a compliancy statement published by the NA.

4.1.2 Enrollment process and responsibilities

The enrollment procedure for ERCA subscribers is depicted in Table 4.1:

Step	EA	ERCA	NA	OE	Flow Chart	Supporting Document	Proof
1	A	R			ERCA approves NA policy	ERCA Policy Section 5	NA compliancy statement
2		R	C		ERCA and NA establish service agreement		Service agreement
3	I	I	R	C	NA approves OE(s)	NA Policy	OE compliancy statement
					OE enrolled		
A = Authorises C = Collaborates D = Decides I = Informed R = Responsible							

Table 4.1 Enrollment procedure for ERCA subscribers

By adhering to the practices described in this CPS, subscribers fulfil the obligations imposed upon them by the ERCA Policy.

The ERCA only provides public key certification services to a national key management system after approving the NA's key management policy. The procedure for national policy approval is depicted in Table 4.2.

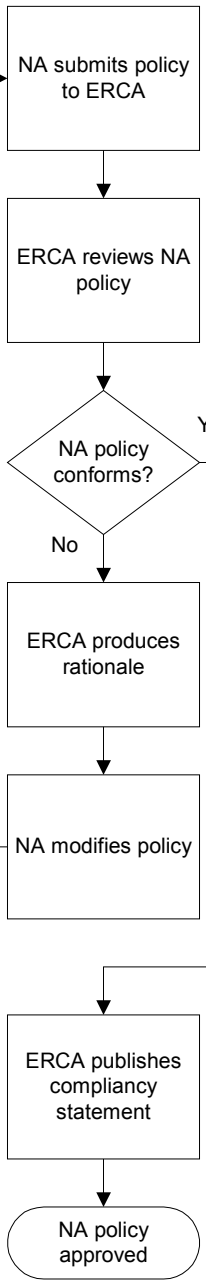
The policy approval process aims to assure that comparable levels of security are implemented in each state participating in the digital tachograph system, despite differences in national practices.

The NA (identified in Section 3.2.2) submits English translations of its national policy documents to the ERCA. The use of a single language for the purposes of policy approval is adopted to facilitate a common interpretation of the documents. Legally authoritative texts in the national language may be provided in support of the review, but will only be consulted for clarification.

In addition to the documentation submitted for the purposes of approval, the ERCA may request additional information from the NA as required to support the policy review.

The national policy compliancy statement is published in the ERCA repository. Publication of the compliancy statement attests that:

1. The ERCA has completed the national policy review and deemed that the requirements on national policies defined in the ERCA Policy have been met.
2. The ERCA shall notify the NA of changes to the ERCA Policy and CPS.
3. The ERCA shall establish the service agreement with the NA.

Step	EA	ERCA	NA	Flow Chart	Supporting Document	Proof
1	I		R		ERCA Policy Section 5.2	Receipt
2	A	R			ERCA Policy Section 5.3	
3		D			ERCA Policy Section 4.3	
4	I	R	I			Report
5			R			
6	I	R	I			Compliancy statement

A = Authorises C = Collaborates D = Decides I = Informed R = Responsible

Table 4.2 National key management policy approval procedure

The service agreement defines:

- the types of public key certificate (e.g. limited or undefined end-of-validity) and motion sensor key required by the national key management system;
- the identities and addresses of the NCA(s) that will submit KCRs;
- the identities and addresses of the OEs that will submit KDRs and receive the KDMs.

4.2 Certificate Application Processing

The procedure for processing public key certification requests is depicted in Table 4.3.

By submitting a key certification request a subscriber acknowledges the terms of this CPS.

4.2.1 Performing identification and authentication functions

The ERCA performs identification and authentication functions (step 3 in the flowchart of Table 4.3) during normal working hours on two normal working days in each month. The schedule is established by the OM and published on the ERCA website. The authentication function requires the collaboration of the NA.

Couriers are identified by their credentials and granted or denied access to the JRC controlled area, according to the procedures in force for visitors to the JRC (see Section 3.2.3).

The ERCA only accepts KCRs from couriers granted access to the JRC controlled area.

Courier identities and KCR contents are authenticated by direct communication with the contact point of the NA concerned (see Section 3.2.2).

Courier identity is authenticated if the NA can demonstrate knowledge of the courier credentials.

KCR contents are authenticated if the NA can demonstrate knowledge of the KCR contents. For this purpose, it is recommended that the NCA provides the NA contact with the KCR data formatted as in Table 4.4. At minimum the ERCA requires proof of knowledge of the SHA-1 message digests of either the KCR data file (SHA-1(File) in Table 4.4) or of the binary KCR contents (SHA-1(KCR) in Table 4.4).

4.2.2 Approval or rejection of certificate applications

The ERCA only produces certificates from KCRs that are correct, complete, and duly authorised.

Checks for correctness and completeness are performed by the ERCA Officer who receives the transport media from the courier. These checks are performed in the JRC controlled premises.

The transport media are retained and archived in the JRC controlled premises.

The ERCA Officer copies correct and complete KCRs from the transport media for transfer to the ERCA protected premises.

Checks of due authorisation are performed from the ERCA protected premises.

Circumstances for KCR rejection are:

- failure to prove possession of the corresponding private key;
- non-unique public key modulus;
- public key parameters not compliant with system security requirements [5];
- non-unique Certificate Holder Reference;
- incorrect KCR contents;
- failure to establish due authorisation.

The ERCA OM communicates the rationale for KCR rejection to the NCA and the NA.

4.2.3 Time to process certificate applications

The ERCA aims to complete public key certification operations in the course of one working day.

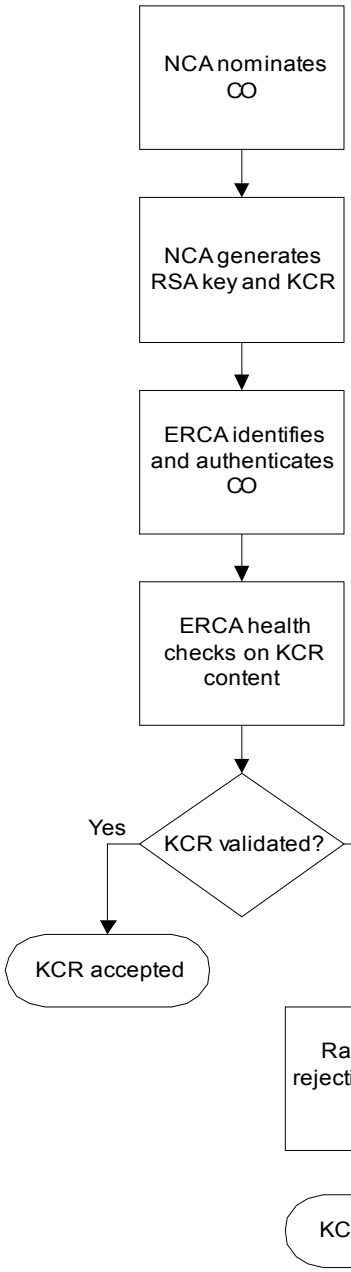
Step	ERCA	NA	NCA	CO	Flow Chart	Supporting Document	Proof
1	I	I	R			ERCA CPS Sec.3.2.3	Letter of nomination
2		I	R			NA policy	
3	R	C		I		ERCA CPS Sec.3.2.3	ERCA log
4	R	C					ERCA log
5	D					ERCA CPS Sec.6	ERCA log
							ERCA log
6	R	I					ERCA log
A = Authorises C = Collaborates D = Decides I = Informed R = Responsible							

Table 4.3 Key certification request procedure

File	TestKeys/Germany/MSCA/D_TC_eMin.KR
SHA-1(File)	12625309 7612044C DA459295 100F55F2 B5E26094
CPI	1
CAR	FD45432000544B01 NationNumeric European Community NationAlpha EC Key Serial No. 0 AdditionalInfo TK CA identifier 1
CHA	FF544143484F00 EquipmentType Certification Authority
EOV	48682200 End of validity 2008-06-30 00:00:00
CHR	0D44202003544B01 NationNumeric Germany NationAlpha D Key Serial No. 3 AdditionalInfo TK CA identifier 1
n	C8E8E24C 58A00FA2 4A62D8A6 6EDA7CF9 8ADB8AB0 F12C79A2 98B8B7A3 04D1F27C D49DD208 9A864A63 D98B9138 BAFD6ED3 4A53DA27 43E20552 182CDDE8 831B74FB 3F080B21 305709B0 627A88A7 F48AB313 969AE479 ABA932EE C7551FEF ABA23CF6 A4BE42F4 E66C4E36 7888B612 BA0E24FA F5B0B5F7 F9215A77 E30AA67C 4AF903C1
e	03
Signature	503700D4 C8A08AB5 61B84B88 C072BB4F 315231BC ECDB7D81 BE509242 7807A3E7 7E983295 C929D5F8 9BB6E715 FEBEBDE0 6229F068 78E03B0A C1271FD2 26ECCAD8 510BA5F5 4CC33DC4 00960E0B BE6E717A E7A547D7 6C65D42E 9232C3F6 0676E468 2A47FADC A13EB4EB D4B58844 32185FF1 7642D138 BB1AD069 42E552D9 FD857A5F
SHA-1(KCR)	50BFEA46 76CD7C97 71A2CE6D AC6013B4 E3D11B25

Table 4.4 Listing of key certification request content

4.3 Certificate Issuance

4.3.1 ERCA actions during certificate issuance

The following information is recorded in the ERCA database for each key certification operation:

- the complete certificate;
- the RSA modulus (*n*) and public exponent (*e*) of the certified public key;
- certificate end-of-validity;
- Certificate Holder Reference (for identification of the RSA public key);
- SHA-1 message digest of the binary certificate data;
- SHA-1 message digest of the binary KCR data;
- certificate status "Valid";
- timestamp.

Certificate(s) are written to transport media for return to the NCA together with a copy of the ERCA public key.

Copies of the certificate are written in each encoding format defined in the ERCA Policy.

Every certificate copy written on transport media is verified using the ERCA public key.

The ERCA public key is distributed in the following byte sequence format:

CAR:	Certification Authority Reference. 8 byte octet string identifying the ERCA, as defined in Regulation 1360/2002 Annex I(B), Appendix 1, Section 2.36 [2]. This field shall be the octet string: 'FDh' NationNumeric: European Community '45h' '43h' '20h' NationAlpha: 'EC ' '00h' keySerialNumber 'FFh' 'FFh' additionalInfo '01h' caIdentifier Test keys shall contain the values '54h', '4Bh' ('TK') in the additionalInfo field.
n	The modulus of the ERCA public key; size 128 bytes (1024 bits)
e	The exponent of the ERCA public key, size of 8 bytes (64 bits)

Table 4.5 ERCA public key distribution format

The ERCA produces printed copies of the certificate contents, formatted as in Table 4.6. One copy is attached to the certificate transport media, and one copy is held by the ERCA OM.

The transport media and the printouts are handed over to the courier in the JRC controlled area, for return to the NCA.

4.3.2 Notification to subscriber by the ERCA of issuance of certificate

The ERCA OM is responsible for publication of issued certificates in the ERCA repository.

No other notification action is performed.

File	TestKeys/Germany/D_TC1.C
SHA-1(File)	201B9DD7 44DFCC3F FEE91222 42944855 10BF8FA9
CPI	1
CAR	FD45432000544B01 NationNumeric European Community NationAlpha EC Key Serial No. 0 AdditionalInfo TK CA identifier 1
CHA	FF544143484F00 EquipmentType Certification Authority
EOV	48682200 End of validity 2008-06-30 00:00:00
CHR	0D44202003544B01 NationNumeric Germany NationAlpha D Key Serial No. 3 AdditionalInfo TK CA identifier 1
n	C8E8E24C 58A00FA2 4A62D8A6 6EDA7CF9 8ADB8AB0 F12C79A2 98B8B7A3 04D1F27C D49DD208 9A864A63 D98B9138 BAFD6ED3 4A53DA27 43E20552 182CDDE8 831B74FB 3F080B21 305709B0 627A88A7 F48AB313 969AE479 ABA932EE C7551FEF ABA23CF6 A4BE42F4 E66C4E36 7888B612 BA0E24FA F5B0B5F7 F9215A77 E30AA67C 4AF903C1
e	03
PK.C	65B9C601 74447B6F 5E7123BF 5D9CA2FC 6295D24D B494E6D2 E8208705 62E408E1 D178E0D7 C1CD6DAF 8F25B817 7EC71CFD 4A810126 68D79119 DE6C7743 E6230CFD 6454C886 EC93103D 0BC3F42A 10DEE278 1BDAC087 865DE051 857DC68E 07BE102C 2159605B 75632898 7C62D3E0 9AAF726B CF4EAD15 A6F054AE 963E65EF FEF62727 B313969A E479ABA9 32EEC755 1FEFABA2 3CF6A4BE 42F4E66C 4E367888 B612BA0E 24FAF5B0 B5F7F921 5A77E30A A67C4AF9 03C10000 00000000 0003FD45 43200054 4B01
SHA-1(C)	597AA546 A8AE8C69 7BB90176 4921657D 5D74008B

Table 4.6 Listing of public key certificate content

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

No actions for certificate acceptance are stipulated. It is assumed that the NA / NCA will verify the certificate using the ERCA public key.

Certificate rejection is managed according to the certificate revocation procedure (see Section 4.9).

4.4.2 Publication of the certificate by the ERCA

Newly issued certificates are published in the ERCA repository at the next scheduled repository update, with a status “Valid”.

If rejected, certificate status is changed to “Rejected” at the next scheduled repository update.

4.4.3 Notification of certificate issuance by the ERCA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers use of their private key(s) and certificate(s) are restricted to those purposes authorised by the ERCA Policy for the digital tachograph system [3] and in conformance with this CPS.

Subscribers apply for the routine re-key procedure in a timely manner to ensure that the usage period of the key-pair is not exceeded. Usage periods for key-pairs, starting from the date of certificate acceptance, are defined in Table 4.7

Key-pair usage	Key-pair usage period	Component service life	Key-pair certificate validity
Driver card issuing	2 years	5 years	7 years
Workshop card issuing	6 years	1 year	7 years
Vehicle unit personalisation	Unlimited	No stipulation	EOV undefined

Table 4.7 Usage periods for NCA key-pairs

Subscribers cease to use their key-pair after the usage period of the key-pair has expired.

Subscribers cease to use their key-pair if the corresponding certificate is revoked.

4.5.2 Relying party public key and certificate usage

Relying parties only use Annex I(B) public keys and certificates for the purposes laid down in the Regulation [2].

Relying parties are responsible for verifying the status of a NCA certificate using the ERCA repository.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new certificate to a subscriber without changing the subscriber's public key or any other information in the certificate.

Certificates are published on the ERCA web-site (see Section 2.1) and may be downloaded by subscribers as needs dictate.

4.7 Certificate Re-key

Certificate re-key means the issuance of a new certificate to the subject NCA with:

- the same Certification Authority Reference
- a new Certificate Holder Reference;
- a new public key;
- a new validity period.

4.7.1 Circumstances for certificate re-key

Certificate re-key must take place:

- in a timely manner to ensure that the subject NCA does not exceed the usage period of the key-pair (see Table 4.7)
- following certificate revocation.

4.7.2 Who may request certification of a new public key

Same as initial key certification request, Section 4.1.1.

4.7.3 Processing certificate re-keying requests

Same as initial key certification request, Section 4.2

4.7.4 Notification of new certificate issuance to subscriber

Same as initial key certification request, Section 4.3.2.

4.7.5 Conduct constituting certificate acceptance

Same as initial key certification request, Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the ERCA

Same as initial key certification request, Section 4.4.2.

4.7.7 Notification of certificate issuance by the ERCA to other entities

No stipulation.

4.8 Certificate Modification

Certificate modification means the issuance of a new certificate to a subscriber following changes in the information in the certificate other than the subscriber's public key.

For the purposes of the Regulation [2], certificate modification is not permitted under any circumstances.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for certificate revocation

Subscriber certificates are revoked in the following circumstances:

- rejection on receipt of a newly issued certificate (see section 4.4);
- compromise or suspected compromise of NCA private keys (see 4.13.6 also);
- loss of NCA private key;
- NCA termination;
- NA or NCA failure to meet obligations under the Regulation [2], the ERCA Policy [3], or this document.

4.9.2 Who can request revocation

The EA is authorised to request revocation of any NCA certificate.

The NA is authorised to request revocation for certificates issued to the NCAs listed in its national policy.

Revocation requests originating from the following entities are authoritative:

- certificate subjects;
- the ERCA;
- all NAs.

The ERCA rejects revocation requests originating from any other entity.

4.9.3 Procedure for revocation request

The certificate revocation procedure is depicted in Table 4.8.

The originator submits a written certificate revocation request to the ERCA OA. A complete request contains the following data:

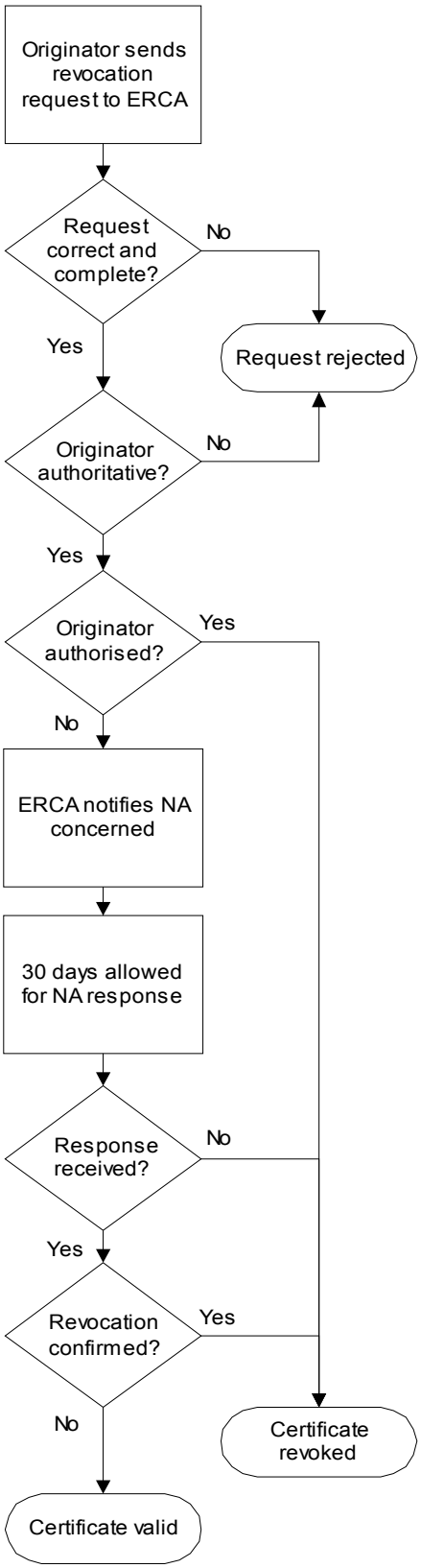
- name, title, affiliation, and contact information of the originator;
- date of the revocation request;
- certificate subject;
- rationale for the request;
- signature of the originator.

Authorised revocation requests (see 4.13.3.1 and 4.13.3.2) become effective from the next scheduled update of certificate status information published in the ERCA repository. Revoked certificates are published with a status “Revoked”; the rationale for revocation is not published.

Authoritative revocation requests (see 4.13.3.3) are notified to the NA concerned and the EA. The NA has 30 days in which to respond to the revocation request. If no response is received within this period, revocation becomes effective from the next scheduled update of certificate status information published in the ERCA repository.

The NA investigates revocation requests notified to it and reports its findings to the ERCA. The ERCA bases its decision on revocation on the NA report. A revocation decision becomes effective from the next scheduled update of certificate status information published in the ERCA repository.

All decisions on certificate revocation are notified to the EA and the NA concerned.

Step	EA	ERCA	NA	OR	Flow Chart	Supporting Document	Proof
1				R			Revocation request
2		D				ERCA CPS Sec.4.13	
3	I	R		I			Letter of rejection
4		D				ERCA CPS Sec.4.13	
5	I	D	I			ERCA CPS Sec.4.13	Decision
6	I	R					Notification
7			R			NA policy	
8	I	D	I			Notification	Decision
9	I	D	I			NA report	Decision
							ERCA repository

A = Authorises C = Collaborates D = Decides I = Informed R = Responsible

Table 4.8 Certificate revocation request processing

4.9.4 Revocation request grace period

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

4.9.5 Time within which ERCA must process the revocation request

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

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 Certificate status issuance frequency

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

4.9.8 Maximum latency for CRLs

Not applicable.

4.9.9 On-line revocation / status checking availability

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

4.9.10 On-line revocation / status checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

None.

4.9.12 Special requirements concerning key compromise

Key compromise is a security incident that must be processed.

If a NCA key is compromised, or suspected to be compromised, the NCA shall report the incident to the ERCA and to the NA. The follow-up investigation and potential action are governed by the national policy.

In the event of the compromise, or suspected compromise, of the ERCA signing key, the ERCA shall immediately notify the European Authority. The European Authority shall act accordingly.

4.9.13 Certificate suspension

Certificate suspension means temporary withdrawal from service of a certificate. After suspension, a certificate may be reinstated, or definitively revoked. For the purposes of the Regulation [2], certificate suspension is not supported.

4.10 Certificate Status Services

4.10.1 Operational characteristics

Certificate status information is published on-line in the form of a list which may be downloaded from the ERCA repository.

4.10.2 Service availability

The ERCA repository is hosted on the ERCA repository website whose availability is only guaranteed during normal working hours.

4.11 End of Subscription

1. Subscription ends when a NA decides for NCA termination. Such a change is notified to the ERCA by the NA as a change to the national policy (see Section 4.1).
2. The decision to submit a certificate revocation request for any valid NCA certificates, or to allow NCA certificates to expire is the responsibility of the NA.

4.12 Key Escrow and Recovery

Key escrow is expressly forbidden by the ERCA Policy [3].

5 MOTION SENSOR KEY LIFE-CYCLE REQUIREMENTS

The security mechanisms of the digital tachograph motion sensor are described in ISO / IEC 16844-3 [6]. The motion sensor keys are generated by the ERCA, and have to be distributed securely to NCAs and CPs.

Normal operation is for the ERCA to distribute a motion sensor key once to each OE identified in the service agreement, on a need-to-know basis. A request to re-distribute the same motion sensor key to the same OE may initiate an investigation of the possibility of key compromise.

RSA transport keys shall have a 1024-bit modulus. Transport key generation is performed in a secure and controlled environment by the OE according to the national key management policy.

No services analogous to suspension, revocation or status information are foreseen for the motion sensor KDMs.

5.1 Application for Motion Sensor Key Distribution Service

5.1.1 Who can submit a motion sensor key distribution request

The ERCA only accepts key distribution requests submitted by an OE approved by the relevant NA. OE approval is performed according to national practices, and is attested by a compliancy statement published by the NA.

5.1.2 Enrollment process and responsibilities

The enrollment procedure for motion sensor master key recipients is the same as that for subscribers to the ERCA key certification service described in Section 4.1.2.

5.2 Motion Sensor KDR Processing

The procedure for processing motion sensor KDRs is depicted in Table 5.1.

By submitting a key distribution request, a motion sensor key recipient acknowledges the terms of this CPS.

5.2.1 Performing identification and authentication functions

The ERCA performs identification and authentication functions (step 3 in the flowchart of Table 5.1) during normal working hours on two normal working days in each month. The schedule is established by the OM and published on the ERCA website. The authentication function requires the collaboration of the NA.

Couriers are identified by their credentials and granted or denied access to the JRC controlled area, according to the procedures in force for visitors to the JRC (see Section 3.2.3).

The ERCA only accepts KDRs from couriers granted access to the JRC controlled area.

Courier identities and KDR contents are authenticated by direct communication with the contact point of the NA concerned (see Section 3.2.2).

Courier identity is authenticated if the NA can demonstrate knowledge of the courier credentials.

KDR contents are authenticated if the NA can demonstrate knowledge of the KDR contents. For this purpose, it is recommended that the OE provides the NA contact with the KDR data formatted as in Table 5.2. At minimum the ERCA requires proof of knowledge of the SHA-1 message digests of either the KDR data file (SHA-1(File) in Table 5.2) or of the binary KDR contents (SHA-1 (KDR) in Table 5.2).

5.2.2 Approval or rejection of key distribution requests

The ERCA only processes KDRs that are correct, complete, and duly authorised.

Checks for correctness and completeness are performed by the ERCA Officer who receives the transport media from the courier. These checks are performed in the JRC controlled premises.

The transport media are retained and archived in the JRC controlled premises.

The ERCA Officer copies correct and complete KDRs from the transport media for transfer to the ERCA protected premises.

Checks of due authorisation are performed from within the ERCA protected premises.

Circumstances for KDR rejection are:

- unjustified request for specific motion sensor key;
- failure to prove possession of the corresponding private key;
- non-unique public key modulus;
- public key parameters not compliant with ERCA policy requirements [3];
- non-unique Key Identifier;
- incorrect KDR contents;
- failure to establish due authorisation.

The ERCA OM communicates the rationale for KDR rejection to the OE and the NA.

5.2.3 Time to process key distribution requests

The ERCA aims to complete motion sensor key distribution operations in the course of one working day.

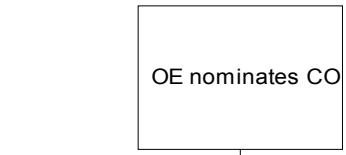
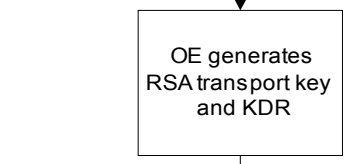
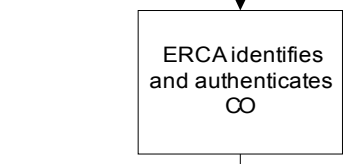
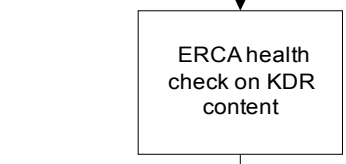
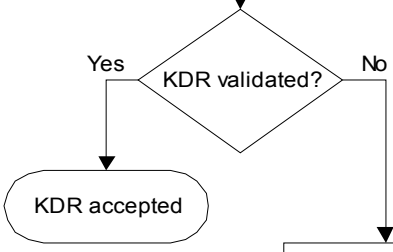
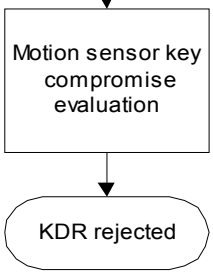
Step	ERCA	NA	OE	CO	Flow Chart	Supporting Document	Proof
1	I	I	R			ERCA CPS Sec.3.2.3	Letter of nomination
2		I	R			NA policy	
3	R	C		I		ERCA CPS Sec.3.2.3	ERCA log
4	R	C					ERCA log
5	D					ERCA CPS Sec.6	ERCA log ERCA log
6	R	C					Evaluation report
A = Authorises C = Collaborates D = Decides I = Informed R = Responsible							

Table 5.1 Motion sensor key distribution request procedure

File	TestKeys/Germany/MSCA/D_KmR.KR
SHA-1(File)	ADEC89C1 91D35EB6 D7445CC2 DE13DEB6 FF93D7DF
CPI	1
CAR	FD45432000544B01 NationNumeric European Community NationAlpha EC Key Serial No. 0 AdditionalInfo TK CA identifier 1
MRA	FF544143484F07 EquipmentType Motion Sensor Km
EOV	FFFFFFFF End of validity Undefined
KID	0D442020FF4B5207 NationNumeric Germany NationAlpha D Key Serial No. 255 AdditionalInfo KR Master Key Type 7
n	A8C2399E 8946FB63 442A896C B398DFAE 447C7291 51E944ED 4A16BD64 D7DC69F6 B25F07C9 BACA441B 1C83313B 703E99B2 E91629A6 836B43E0 E3CC67AD C29DBE18 FED1FA7E 4CAB4473 3E5CD5A6 4DF01FE0 324AA8CF 82C18C06 5142E147 810666AE E221A1CE 2B3E239D 612BDE64 1AD93355 DAD9B490 19914044 840DD4FA FF9CF31B
e	10001
Signature	4042F9C5 59DABAC4 DC75A00B 0E7776CB B7C6E438 AC2649A1 F63FBEE8 2A311E18 C6D7281A 1681EE26 80D362C6 4FB635A3 6504CBB3 D65FA380 B5077120 60CC51D7 A9354715 B817E983 0530DB86 83A700CC 959AF0E0 5FFDC39B A3FF527E D786016A 05FFBEBE 04E916B5 328695DA 70ACC873 66BF1F0B 8663B435 400AAED5 5A3241E3
SHA-1(KDR)	2A76DE62 26CA93C6 36E032EF 6289CB9C 088946DE

Table 5.2 Listing of key distribution request content

5.3 Motion Sensor KDM Issuance

5.3.1 ERCA actions during motion sensor key distribution message issuance

The following information is recorded in the ERCA database for each KDM operation:

- the RSA modulus (*n*) and public exponent (*e*) of the KDM recipient's public key;
- Key Identifier (for identification of the RSA public key);
- SHA-1 message digest of the binary KDM data;
- SHA-1 message digest of the binary KDR data;
- KDM status “Pending acceptance”;
- timestamp;
- one-time distribution flag for the specific motion sensor key.

Each KDM is written to transport media for return to the OE.

Copies of the KDM are written in each encoding format defined in the ERCA Policy.

The integrity of every KDM copy written on transport media is verified by production of a printout of the KDM contents, formatted as in Table 5.3. The printouts are retained by the ERCA OM.

Note: the ERCA cannot verify a KDM, as it is not in possession of the KDM recipient's private key.

All KDMs are retained to protect against loss or corruption of the transport media.

5.3.2 Notification to subscriber by the ERCA of issuance of KDM

The transport media are handed over to the courier in the JRC controlled area, for return to the OE.

No further actions for notification of KDM issuance are stipulated.

File	TestKeys/Germany/MSCA/D_KmR.Kdm
SHA-1(File)	FDFFEEE5 04B3B3F8 5059820F 18AEBBC7 7CE56E5B
KID	0D442020FF444B07 NationNumeric Germany NationAlpha D Key Serial No. 255 AdditionalInfo DK TDES Key Motion Sensor Km
SHA-1(KDM)	DFA47FB7 3034EDF5 2224F69B 53AC71C6 59769650

Table 5.3 Listing of key distribution message contents

5.4 Motion Sensor KDM Acceptance

The procedure for KDM acceptance is depicted in Table 5.4.

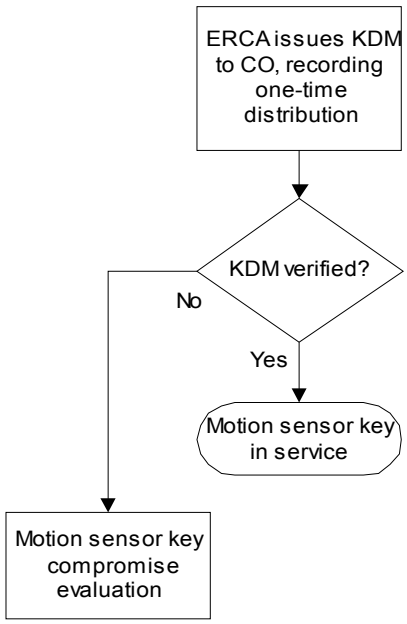
Step	ERCA	NA	OE	CO	Flow Chart	Supporting Document	Proof
1	R						ERCA log
2			D	C		ERCA Policy Ann.D 4.2	
3	R	C				Incident Handling Manual	Evaluation report
A = Authorises C = Collaborates D = Decides I = Informed R = Responsible							

Table 5.4 Motion sensor KDM acceptance procedure

5.4.1 Conduct constituting KDM acceptance

The OE shall verify the KDM using the appropriate private key before putting the enclosed motion sensor key into service.

KDM verification failure is a security incident that must be processed.

The NA may request the KDM information of Table 5.3 from the ERCA OM.

In the absence of notification of KDM verification failure within 30 days from KDM hand-over to the courier, the ERCA shall set KDM status to “Accepted”.

5.4.2 Publication of the KDM by the ERCA

None.

5.4.3 Notification of KDM issuance by the ERCA to other entities

None.

5.5 Motion Sensor Master Key Usage

5.5.1 Recipient key usage

Motion sensor master key usage is restricted to those purposes authorised by the ERCA Policy for the digital tachograph system [3] and in conformance with this CPS.

Recipients only use the RSA transport key-pair for the purposes of preparing a KDR, and recovering the motion sensor key from a KDM.

Recipients only use a motion sensor master key after successful verification of the KDM.

There is no stipulation for motion sensor master key usage periods.

5.5.2 Relying Party Responsibilities

No stipulation.

5.6 KDM Renewal

KDM renewal means the issuance of a copy of an existing KDM to a subscriber without changing the subscriber's private key or any other information in the KDM.

5.6.1 Circumstances for KDM renewal

KDM renewal may take place only if the original transport media received at the OE are damaged or corrupted.

Damage or corruption of transport media is a security incident which must be processed.

5.6.2 Who may request KDM renewal

An approved OE may submit a KDM renewal request.

The ERCA only accepts a KDM renewal request endorsed by the NA which approved the OE.

5.6.3 Processing KDM renewal requests

The procedure for processing KDM renewal requests is depicted in Table 5.5.

The ERCA performs identification and authentication functions (step 2 in the flowchart of Table 5.5) during normal working hours on two normal working days in each month. The schedule is established by the OM and published on the ERCA website. The authentication function requires the collaboration of the NA.

Couriers are identified by their credentials and granted or denied access to the JRC controlled area, according to the procedures in force for visitors to the JRC (see Section 3.2.3).

Courier identities are authenticated by direct communication with the contact point of the NA concerned (see Section 3.2.2).

Courier identity is authenticated if the NA can demonstrate knowledge of the courier credentials.

The ERCA aims to complete motion sensor KDM renewal operations in the course of one working day.

The following information is recorded in the ERCA database for each KDM renewal operation:

- Key Identifier of the KDM;
- KDM status “Renewed”;
- timestamp.

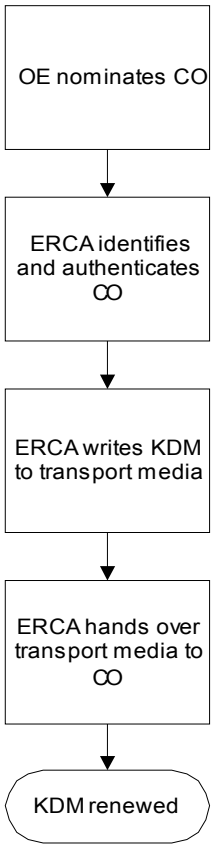
Step	ERCA	NA	OE	CO	Flow Chart	Supporting Document	Proof
1	I	I	R			ERCA CPS Sec.3.2.3	Letter of nomination
2	R	C		C		ERCA CPS Sec.3.2.3	
3	R						ERCA log
4	R	I		C			ERCA log
A = Authorises C = Collaborates D = Decides I = Informed R = Responsible							

Table 5.5 Motion sensor KDM renewal procedure

Copies of the KDM are written to the transport media for return to the OE in each encoding format defined in the ERCA Policy.

The integrity of every KDM copy written on transport media is verified by production of a printout of the KDM contents, formatted as in Table 5.3. The printouts are retained by the ERCA OM.

5.6.4 Notification of renewed KDM issuance to subscriber

The transport media containing a renewed KDM are only handed over to the courier in the JRC controlled area, for return to the OE.

No further actions for notification of renewed KDM issuance are stipulated.

5.6.5 Conduct constituting KDM acceptance

Same as initial key distribution request, Section 5.4.1.

5.6.6 Publication of the renewed KDM by the ERCA

None

5.6.7 Notification of renewed KDM issuance by the ERCA to other entities

None.

5.7 KDM Redistribution

KDM redistribution means the issuance of a new KDM to an OE using a KDR with:

- the same Message Recipient Authorisation (identifies the same motion sensor master key);
- a new Key Identifier;
- a new public transport key.

Motion sensor master key distribution is foreseen as a one-time process.

Redistribution is a security incident which must be processed before the redistribution request can be accepted.

5.7.1 Circumstances for motion sensor key redistribution

KDM redistribution must take place after loss of the motion sensor master key.

KDM redistribution may take place after OE termination.

5.7.2 Who may request redistribution of a motion sensor key

An approved OE may submit a motion sensor key redistribution request.

The ERCA only accepts a key redistribution request endorsed by the NA which approved the OE.

5.7.3 Processing motion sensor redistribution requests

Same as initial key distribution request, Section 5.2

5.7.4 Notification of new KDM issuance to subscriber

Same as initial key distribution request, Section 5.3.2.

5.7.5 Conduct constituting KDM acceptance

Same as initial key distribution request, Section 5.4.1.

5.7.6 Publication of the re-distributed KDM by the ERCA

None

5.7.7 Notification of KDM issuance by the ERCA to other entities

None.

5.8 Special requirements concerning key compromise

Key compromise is a security incident that must be processed.

If an OE copy of a motion sensor key is compromised, or suspected to be compromised, the OE shall report the incident to:

1. The ERCA OM, indicating the circumstances under which the compromise occurred.
2. To the NA for a follow-up investigation and potential action in accordance with the national policy. The outcome of the NA investigation is reported to the ERCA.

In the event of the compromise, or suspected compromise, of a motion sensor key, the ERCA OM shall immediately notify the EA. The EA shall act accordingly.

6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

6.1 Physical Controls

The ERCA signing system is housed in a nuclear material storage facility licensed according to the IAEA INFCIRC/225/Rev.4 – The physical protection of nuclear material, category I. The Ispra Site Directorate is responsible for the security operations of the facility.

The JRC Ispra site security services maintain and implement the physical protection plan (Piano di protezione fisica) for the site. The physical protection plan is not publicly available. The information presented below summarises the contents of the physical protection plan.

6.1.1 Site location and construction

The facility, named PERLA (Performance Laboratory), is housed in the Isola Nucleare Essor (INE) which is the protected area (see Definition, Section 12) surrounding the main nuclear reactor within the controlled area of the JRC Ispra site.

The central alarm station (see Definition, Section 11) and the INE entrances are located in the PCZ-A building (Posto Controllo Zona A). The central alarm station, known as PCS (Posto Controllo Sicurezza) maintains contact with a Carabinieri (Italian military police) station at the JRC main entrance.

6.1.2 Physical access

Controlled Area

The JRC Ispra controlled area is protected by a 3-metre high fence fitted with intrusion detection systems.

Statutory staff are authorised to enter the controlled area during normal working hours. Authorisation to enter outside normal working hours is requested from the JRC security service by the hierarchical superior of the subject.

Staff are issued with an identity card bearing a recent photograph of the subject and encoding identity information (e.g. on a magnetic strip).

On entrance to the site during normal working hours, staff must present this card for a visual check by the guard on duty at the main entrances. Outside normal hours, the visual check is supplemented by a reading of the card data, to record entrances and exits.

A specific authorisation procedure for visitors is in force. Visitors' identity, date, and the purpose of the visit are recorded.

Vehicles bearing a badge issued by the security service may enter the controlled area. On exit, vehicles are subject to random checks.

Protected Area

The INE perimeter consists of a series of barriers under continuous video surveillance and monitoring.

Authorisation to enter the INE and the facilities inside it is requested by the hierarchical superior of the subject, but may only be granted by upper management (e.g. Institute Director or delegate). Requests for authorisation are approved by the JRC security service.

All entrances to the INE and to the PERLA facility are single access systems (SAS) controlled by guards on duty in the PCS.

Staff entering through a SAS are identified, by means of the staff card; and authenticated, by entry of a PIN. Visitors are issued with a temporary card and PIN by the guards at the PCZ-A reception area.

SAS passages block automatically on detection of metal objects or radiation. Manual intervention by a guard is required to return the SAS to service.

The presence of personnel in the protected area is recorded for compliance with security and safety requirements. The identities of the persons present in the protected area is known at all times.

All transfers of material into and out of the INE and PERLA are controlled by guards.

6.1.3 Power and air conditioning

Backup electrical power is provided by a group of three diesel generator sets, any two of which must be serviceable for the PERLA facility to operate (licensing requirement).

The air conditioning system of the PERLA facility is designed to create a depression with respect to external atmospheric pressure, to mitigate accidental releases of radioactive material. Operation of the air conditioning system is a licensing requirement.

6.1.4 Water exposures

The PERLA facility is designed to prevent exposure to water. The risk of exposure of the ERCA CA system to water is considered to be minimal.

6.1.5 Fire prevention and protection

The PERLA operating license forbids the use of naked flame and the presence of cylinders containing flammable gases while any sample of fissile material is in use.

The PERLA facility has a fire detection system connected to alarms at the JRC Emergency Services. Operation of the fire detection system is a licensing requirement.

6.1.6 Media storage

On-site media for the ERCA CA system are held in safes.

6.1.7 Waste disposal

The operations of the ERCA CA system create normal office waste. Prior to disposal, paper waste and CD media are shredded.

Magnetic storage media are erased by degaussing.

Disposed waste is removed by the cleaning contractor.

6.1.8 Off-site backup

To be defined

6.2 Procedural Controls

6.2.1 Trusted roles

1. ERCA operations are conducted by statutory staff assigned to one of the following roles:
    - Administrator;
    - Officer;
    - Auditor.
2. The operator role described in the ERCA policy is incorporated in the administrator role.
3. The administrator role is authorised to:
    - generate and backup the ERCA RSA key pair and the motion sensor master keys;
    - install, configure and maintain the ERCA system for certificate production and motion sensor key distribution;
    - perform system backup and recovery.
4. The officer role is authorised to:
    - authenticate MSCA key certification and key distribution requests;
    - produce RSA public key certificates for NCAs;
    - produce motion sensor KDMs for OEs.
5. The auditor role is authorised to:
    - produce, view and maintain archives and audit logs of the ERCA trustworthy systems;
    - perform tests and checks on the ERCA system on demand;
    - quarantine the ERCA system on detection of an incident;
    - report incidents to higher management.

6.2.2 Number of persons required per task

1. ERCA private and secret key generation and backup is performed according to the Key Generation Ceremony secure operation procedure. This process is witnessed by the EA and the Commission Security Directorate. Minutes of the key generation ceremony are published.
2. ERCA system installation and configuration requires one administrator and one auditor. The administrator carries out the installation and configuration operations. The auditor verifies these operations, and performs the baseline system integrity check prior to entry into service.
3. ERCA system maintenance operations require one administrator. Any changes are detected and verified by system integrity checks performed by the auditor.
4. ERCA system backup requires one administrator. ERCA system recovery requires one administrator and one auditor.
5. Officer tasks require one officer. Key certification and distribution operations are recorded in the ERCA database and system logs controlled by the auditor. ERCA workstation startup requires the intervention of the administrator.
6. Trustworthy system auditing requires the intervention of one administrator and one auditor. The audit consists of system integrity checking using software held on read-only media. The administrator configures the system to permit the auditor to execute the integrity checks. Test results are maintained by the auditor.

7. Incident reports are prepared by the auditor and sent directly to higher management, with a copy to the ERCA OM.

6.2.3 Identification and authentication for each role

Staff assigned to all roles are identified in the course of passage through the physical access controls surrounding the ERCA workstation.

The workstation login process requires a username and password; roles are mapped to user groups.

Operations involving the ERCA private and secret keys require knowledge of PIN codes, keyed in to the ERCA workstation.

6.2.4 Roles requiring separation of duties

No single person is permitted to cover more than one role simultaneously.

6.3 Personnel Controls

6.3.1 Qualifications, experience, and clearance requirements

1. The operations manager (OM) is responsible for:
    - establishing the ERCA operations schedule;
    - accomodating auditor-initiated requests for system checks;
    - maintenance of the ERCA repository website;
    - authorising system maintenance activities;
    - appointments to trusted roles;
    - maintaining relationships between the ERCA and the EA, and the ERCA and the NAs.

    The OM requires general knowledge in the following areas:
    - the key management processes specific to the digital tachograph system;
    - the ERCA secure operating procedures;
    - maintenance of auditable records of ERCA operations;
    - European Commission administrative procedures.

    The OM is not required to handle sensitive information, and therefore no clearance requirements are stipulated.
2. The administrator is a trusted role in the ERCA system. Administrators require detailed knowledge in the following areas:
    - installation, configuration and maintenance of the ERCA cryptographic hardware;
    - installation, configuration and maintenance of ERCA general-purpose IT equipment and operating systems;
    - the key management processes specific to the digital tachograph system;
    - the ERCA secure operating procedures;
    - the operation of the ERCA software.

    Administrators require general knowledge in the following areas:
    - principles of IT security;
    - principles of cryptography and issues involved in cryptographic key management.

    The administrator role is required to handle the root keys. This CPS does not stipulate clearance requirements according to the European Commission provisions on security [7] but persons assigned to this role are encouraged to apply for security clearance under the vetting procedure described in [7].
3. The officer is a trusted role in the ERCA system. Officers require general knowledge in the following areas:
    - the key management processes specific to the digital tachograph system;
    - the ERCA secure operating procedures;
    - the operation of the ERCA software.

    The officer role is not required to handle sensitive information, and therefore no clearance requirements are stipulated.

4. The auditor is a trusted role in the ERCA system. Auditors require detailed knowledge in the following areas:
    - the ERCA secure operating procedures;
    - IT security auditing, with emphasis on system integrity checking;
    - the operation of the ERCA software.

    Auditors require general knowledge in the following areas:
    - IT forensics.

    The auditor role is not required to handle sensitive information, and therefore no clearance requirements are stipulated.

    To ensure the auditors' true independence, staff assigned to the auditor role shall not belong to the same organisational unit as the ERCA OA.

6.3.2 Background check procedures

1. Any background checks are performed in accordance with the European Commission security policy [7].

6.3.3 Training requirements

1. The personnel training plan is managed by the OM.
2. Trainees are required to familiarise themselves with the documentation issued to the appropriate role.
3. Trainees are required to observe a number of ERCA operations performed according to the schedule established by the OM.
4. Trainees are subjected to a number of practical tests on the development / test systems under the supervision of a staff member appointed to the appropriate role.
5. A trainee is deemed qualified by a staff member appointed to the appropriate role.

6.3.4 Retraining frequency and requirements

Retraining is required in case of changes to ERCA policies, procedures, or operations.

6.3.5 Job rotation frequency and sequence

1. Appointment to the administrator and officer roles are proposed by the OM and authorised by the head of unit of the OA.
2. Appointments to the auditor role are proposed by the OM and authorised by the head of unit of the OA in accordance with the head of unit of the auditor.
3. Key activation data (i.e. PIN values) are changed on job rotation or new appointments.
4. No frequency or sequence for job rotation are stipulated.

6.3.6 Sanctions for unauthorized actions

Articles engaging the responsibility of Commission officials for their actions in carrying out their duties are defined in the Staff Regulations for officials of the European Communities.

Articles engaging the responsibility of contractual staff for their actions in carrying out their duties are defined in their contract of employment.

6.3.7 Contracting personnel requirements

Only persons covered by the Staff Regulations for officials of the European Communities are involved in ERCA operations.

6.3.8 Documentation supplied to personnel

1. ERCA staff are provided with the following documentation:
    - ERCA Policy, as published on the ERCA web-site (see Section 2.1);
    - ERCA CPS (this document);
    - Secure operating procedures as appropriate to the assigned role;
    - Legislative documents [1] and [2].
2. The ERCA OM is responsible for ensuring that staff are provided with up-to-date versions of the documentation.

6.4 Audit Logging Procedures

6.4.1 Types of event recorded

All significant security events in the ERCA software are automatically time stamped and recorded in the system log files. These include events such as:

- successful and failed attempts to initialise, remove, update, and recover public keys, certificates, and national CA rights;
- successful and failed attempts to create, remove, login as, set, reset, and change passwords of, revoke privileges of, create, update, and recover access keys of ERCA personnel;
- successful and failed interactions with the ERCA database including connection attempts, read, update, and write operations made by the ERCA software;
- all events related to certificate status information, security policy modification and validation, ERCA software start-up and stop, database backup, certificate and certificate chain validation, motion sensor key distribution, and audit trail;
- management, certificate life-cycle management and other miscellaneous events;
- system start-up and shutdown.

The ERCA administrator maintains information concerning:

- system configuration changes and maintenance;
- administrator privileges.

The ERCA auditor maintains:

- system integrity checking software
- system integrity checking results;
- discrepancy and compromise reports.

The ERCA facility has an electronic monitoring and access control system that records physical access to the ERCA signing system.

6.4.2 Frequency of system integrity checks

The operations schedule foresees that the ERCA auditors perform system integrity checks before starting and after completion of each signing session.

The ERCA auditors investigate any alerts or irregularities in the integrity checks, and may quarantine the system, suspending operations until the alerts or irregularities are resolved.

The ERCA auditors have the right to request performance of system integrity checks outside the established operations schedule. Such “out of band” requests are submitted to the OM who is required to make the necessary arrangements with the shortest possible delay.

Security incidents detected by the system integrity checks are defined in the Incident Management manual issued to the ERCA auditors.

6.4.3 Frequency of processing system logs

The operations schedule foresees that the ERCA auditors inspect system logs after completion of each signing session.

The auditors investigate any alerts or irregularities in the logs, and may quarantine the system, suspending operations until the alerts or irregularities are resolved.

The ERCA auditors have the right to inspect system logs outside the established operations schedule. Such “out of band” requests are submitted to the OM who is required to make the necessary arrangements with the shortest possible delay.

Security incidents resulting from system log inspection are defined in the Incident Management manual issued to the ERCA auditors.

6.4.4 Retention period for audit log

The audit trails are retained indefinitely. Section 4.11 Audit Log Backup Procedures describes the archive procedures for these logs.

6.4.5 Protection of audit log

The audit logs are written to CD-R media. At least two copies of each CD-R are created. The checksum of the CD-R filesystem is recorded in the ERCA log book by the administrator, and by the auditor.

The checksums are used to identify the CD-R media as authentic and integral sources of audit log information.

The CD-R media copies are kept in physically separate locations within the JRC controlled area to ensure the availability of the audit logs.

6.4.6 Audit log backup procedures

The ERCA audit log consists of two parts:

1. system integrity check results;
2. dataset of signing session records.

These two parts are used for different purposes, and are therefore written to separate CD-R media.

The system integrity check results are backed up in two copies retained by the auditor. These are used as the baseline for the integrity checks on mutable system files (e.g. the ERCA database files) performed at the start of the next signing session.

The dataset of signing session records consists of:

1. the ERCA signing system database;
2. the ERCA signing system log file;
3. the ERCA cryptographic hardware log file.

This dataset is backed up in three copies, one of which is retained by the auditor. The other two copies are retained in the ERCA protected premises, and at the ERCA OA. All three copies are sources for data recovery.

These arrangements are designed to ensure that the auditor role is in possession of all the information it needs to document the history of the ERCA operations.

6.4.7 Audit collection system

Audit trail information is generated both internally, by the ERCA hardware, the ERCA software, and the underlying operating system; and externally by the JRC security services.

6.4.8 Notification to event-causing subject

Logging and auditing events are not notified to the event-causing subject. Actions are logged and audited, but audit records are retained within the ERCA.

6.4.9 Vulnerability assessments

The auditor role is provided with a baseline integrity check of ERCA system software on entry into service of a new signing system. This provides integrity checking data on the immutable system files (e.g. operating system and application binaries, configuration files etc.).

The auditor role builds up a collection of session records and integrity checks in the course of system operation.

The auditor role is authorised to implement and perform any tests and checks on copies of the session records and integrity check data which it sees fit, in order to investigate susceptibility of the ERCA system to published vulnerabilities.

The administrator and auditor roles are encouraged to monitor on-line information sources (e.g. http://www.cert.org) for advisories and incident notes, and to evaluate whether these may have an impact on ERCA operations.

Tests may be performed on the ERCA development / training systems, using copies of ERCA data from the audit log sources.

6.5 Records Archival

6.5.1 Types of data archived

Various documents are provided in the execution of RA functions. These documents include:

- courier identification information,
- public key certification requests;
- motion sensor key distribution requests;
- certificate status change requests;

Some information provided is personal information and falls under the Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000. This information is not stored in the ERCA systems. It is managed by the JRC Security Service, according to the procedures in force for visitors to the JRC.

The types of events recorded in the ERCA system database include:

- creation of the ERCA signing key pair;
- insertion, removal, and update of national CA identities;
- insertion, removal, and update of national CA rights to ERCA services;
- certificate issuance events;
- motion sensor key distribution events.

6.5.2 Retention period for archive

Audit information (per Section 6.4 of this CPS), national CA key certification, certificate status, and motion sensor master key distribution requests are archived indefinitely.

Personal identification information are archived in accordance with European Commission regulations.

6.5.3 Protection of archive

The ERCA signing system database is stand-alone and protected by physical security (see Section 6). Protection of the audit trail is as described in Section 6.4.5. The database archive media are protected by physical security in that they are retained in the same restricted access facility as the signing system, to which only the ERCA staff have access.

6.5.4 Archive backup procedures

The ERCA signing system database, system logs, and cryptographic hardware logs are backed up after each signing session. Three copies of the backup dataset are created on CD-R media.

The checksum of each CD-R copy is recorded in the ERCA log book, and by the auditor. These checksums are used to identify a CD-R as an authorised source of recovery data. The CD-R copies are retained in three different locations:

1. an operational backup is retained in the ERCA protected area;
2. one backup CD is retained at a location accessible to the ERCA OA;
3. one backup CD is retained at a location accessible to the auditors.

The backup copies of the ERCA database require no assurances of confidentiality, as no sensitive data are held database.

The ERCA database may be copied from the backup held by the ERCA OA for the following purposes:

1. as the source of certificate status information for the ERCA repository;
2. maintenance of copies used for training / documentation / operations analysis.

6.5.5 Requirements for time-stamping of records

The ERCA signing system clock is adjusted in the course of the system integrity checks performed on the day before signing operations. The system clock shall be adjusted to compensate for deviations greater than 5 minutes from local time.

System clock adjustments shall be notified to, and recorded by the auditor.

6.5.6 Archive collection system

ERCA archive collection is a function of the ERCA application software. The backup facility for the system log files is described in Sections 6.4.6 and 6.4.7, and is external to the ERCA application software. These data stores are archived on to separate media, copies of which are stored outside the ERCA protected area.

6.5.7 Procedures to obtain and verify archive information

Once per year, the archive media are retrieved by the ERCA administrator and auditor and verified to ensure that no damage or loss of data has occurred, by attempting a data recovery operation to the ERCA development / training system. If any irregularity occurs during this operation, a new data backup is produced in the shortest possible delay.

6.6 Key Changeover

The Regulation [2] does not foresee change of the ERCA signing key and of the motion sensor master keys.

Key changeover is not contemplated.

6.7 Compromise and Disaster Recovery

6.7.1 Incident and compromise handling procedures

Security incidents and compromise handling procedures are defined in the Incident Management manual issued to the ERCA administrators and auditors.

On detection of an incident, the ERCA signing system may be quarantined, and ERCA operations suspended, until the level of compromise has been established.

6.7.2 Computing resources, software, and/or data are corrupted

The steps for recovering a secure environment , depending on the nature of the disaster, are as follows:

1. Immediate replacement of signing system with backup or development systems;
2. Regeneration of ERCA application software from source code backups;
3. Recovery of ERCA database from backups;
4. Generation of new CA Officer access keys;
5. Recovery and activation of ERCA secret key from backups;

6.7.3 Entity private key compromise procedures

In case of ERCA signing key or motion sensor key compromise, the ERCA shall notify the EA.

The EA shall notify all NAs of the compromise and convene an emergency meeting of the NAs to identify a course of action.

6.7.4 Business continuity capabilities after a disaster

Reconstruction of a secure environment from off-site data backups, and most recent system image in an alternative restricted access area on European Commission premises.

6.8 ERCA Termination

Termination of the ERCA service at JRC Ispra, with removal of ERCA services to another organisational unit, is managed as a change of secure facility.

The procedure for cessation of ERCA services follows:

1. Notification of cessation of ERCA service to all subscribers;
2. Secure erasure of working copies of the ERCA root and motion sensor master keys, by tampering of the HSM, and secure erasure of system disks;
3. Recovery and secure destruction of all ERCA root and motion sensor master key backup copies;
4. Transfer of ERCA archive and audit records to the European Authority.

The termination procedure shall be under dual control of the ERCA and the European Authority.

7 TECHNICAL SECURITY CONTROLS

7.1 ERCA Key Pair Generation and Installation

7.1.1 ERCA key pair generation

Support of the cryptographic mechanisms defined in Annex I(B)[5] requires the generation of a root RSA key pair, and of a pair of DES-EDE2 keys.

RSA and DES-EDE2 key generation is performed in certified hardware security modules.

The key generation ceremony is defined in a separate document. The key generation ceremony is performed in the presence of witnesses from the EA and the Commission Security Directorate. The proceedings of the key generation ceremony are published as part of the ERCA approval procedure.

7.1.2 Private key delivery to entity

The ERCA does not provide RSA key pairs to its subscribers.

A specific protocol (see [3], Annex D) has been developed for encryption of the motion sensor master keys.

7.1.3 Public key delivery to certificate issuer

The ERCA does not use an external certification services provider.

7.1.4 ERCA public key delivery to relying parties

The ERCA public key is written to the transport media together with the key certificate(s) provided to subscribers.

The ERCA public key is also available from the ERCA web-site: http://dtc.jrc.it

7.1.5 Key sizes

Key sizes are mandated by [5]. RSA keys shall have 1024-bit modulus and 64-bit public exponent.

7.1.6 Public key parameters generation

No stipulation.

7.1.7 Parameter quality checking

Using certified hardware security modules, parameterised to generate 1024-bit modulus RSA keys.

7.1.8 Hardware/software key generation

The ERCA root keys are generated in certified hardware security modules.

7.1.9 ERCA key usage purposes

The ERCA root RSA key is used for the sole purposes of certifying NCA RSA public keys according to the mechanisms prescribed by [5]

The ERCA makes no use whatsoever of the DES-EDE2 motion sensor master keys. The ERCA encrypts these keys prior to distributing them to a NCA or CP.

7.2 Private Key Protection

7.2.1 Cryptographic module standards and controls

The ERCA only uses certified cryptographic hardware security modules for generation and storage of root keys.

The HSM operation is verified by means of internal tests prior to any cryptographic operations.

The HSM firmware upgrade status is checked once per year by the administrator.

7.2.2 Private key multi-person control

Private key generation and backup are performed according to the Key Generation Ceremony secure operation procedure. This process is witnessed by the EA and the Commission Security Directorate.

Private key recovery operations require the intervention of one administrator and one auditor.

Public key certification operations and motion sensor master key distribution operations require the intervention of one administrator and one officer.

7.2.3 Private key escrow

Key escrow is forbidden by the ERCA Policy.

7.2.4 Private key backup

The ERCA RSA keys and the motion sensor master keys are encrypted and stored in chip cards supplied with the certified cryptographic hardware.

The key backups are verified once per year by attempting a key restoration operation into an identical HSM. The key backup verification is performed in a protected area in the presence of an administrator and an auditor. The HSM is maintained in the same environment unless required elsewhere, in which case it is tampered to erase sensitive data in its memory before leaving the protected area.

If the key backup verification fails, new backups are produced from the signing system in the shortest possible delay. The off-site backup copies of the keys are exchanged with the most recent backup copies and verified to establish their condition.

7.2.5 Private key archival

As 7.2.4

7.2.6 Private key transfer into or from a cryptographic module

ERCA private keys are inserted into the cryptographic module only as required for key recovery or business continuity, as defined in Section 6.7.4.

7.2.7 Private key storage on cryptographic module

The ERCA private keys are stored in the cryptographic module used to generate them.

7.2.8 Method of activating private key

The ERCA private keys are activated by entry of the officer PIN prior to each signing operation.

7.2.9 Method of deactivating private key

The ERCA private key is deactivated automatically on termination of the cryptographic operations.

7.2.10 Method of destroying private key

Simulation of a tamper event to cause erasure of the private keys held in cryptographic modules.

7.2.11 Cryptographic module rating

The ERCA uses cryptographic modules certified to FIPS 140-2 Level 3 or higher.

7.3 Other Aspects of Key Pair Management

7.3.1 Public key archival

The ERCA public key is maintained in the ERCA repository.

7.3.2 Usage periods for the public and private keys

The usage periods for the ERCA private key is set at thirty years by the ERCA Policy.

The usage periods for the ERCA public key and the motion sensor master keys are undefined.

7.4 Activation Data

7.4.1 Activation data generation and installation

1. Activation data may be any of the following data:
    - boot password for the ERCA signing system.
    - administrator and officer PINs keyed in to the cryptographic hardware;
    - key backup PINs;
    - username / password combinations for logging in to the ERCA signing system;
    - checksums of CD-R media containing executable code (e.g. integrity checkin software) or backed up data;
    - auditor keys used for authentication of integrity check data;
    - combinations of safes, strong-boxes etc.
2. The ERCA system boot password is decided by common accord of the persons assigned to the administrator role on system installation.
3. Administrator and officer PINs are different for each role. They are decided by common accord of the staff assigned to a specific role. The administrator defines the PIN length, and sets the initial officer PIN in the course of the ERCA root key generation ceremony.
4. Key backup PINs are defined on creation of key backups.
5. Usernames are inserted by the administrator on user account creation according to the naming conventions in use at the JRC (first five characters of the user's surname, followed by the first two characters of the user's first name).
6. Initial login passwords are set by the administrator, and changed on first login of the user. Login passwords are changed on a regular basis.
7. Safe combinations are set by the designated owner of the safe.

7.4.2 Activation data protection

The boot password, administrator PIN, officer PIN, key backup PIN(s) and safe combinations are stored in separate labelled and sealed envelopes maintained by the Local Information Security Officer (LISO) [7].

The key backup PIN(s) are stored in separate strong-boxes.

The ERCA OM may apply to the LISO for access to the sealed envelopes.

Loss of activation data is a security incident which must be investigated.

7.4.3 Other aspects of activation data

The boot password and PINs are changed under the following circumstances:

- once per year, or when instructed to do so by the OM;
- on rotation of staff between the administrator and officer roles.

Safe combinations are changed under the following circumstances:

- once every five years, or when instructed to do so by the OM;
- on rotation of safe owners to other duties.

7.5 Computer Security Controls

7.5.1 Specific computer security technical requirements

No stipulation.

7.5.2 Computer security rating

ERCA IT systems use general-purpose, commodity IT hardware.

Security sensitive information is stored in FIPS 140-2 Level 3 approved hardware security modules.

7.6 Life Cycle Technical Controls

7.6.1 System development controls

Access to system source code is limited to designated software developers.

The source code repository is backed up once per month.

Prior to accepting software for ERCA operations, the Administrator:

- reviews source code for conformity with functional specifications;
- reviews the results of acceptance tests performed according to the acceptance test specification.

7.6.2 Security management controls

System software developers are excluded from ERCA trusted roles.

7.6.3 Life cycle security ratings

No stipulation.

7.7 Network Security Controls

The ERCA CA system is a stand-alone workstation, not connected to any IT network.

8 CERTIFICATE, CRL, AND OCSP PROFILES

8.1 Certificate Profile

8.1.1 Version number(s)
This CPS supports the digital tachograph certificate profile identifier 1 [5].

8.1.2 Certificate extensions
No stipulation.

8.1.3 Algorithm object identifiers
No stipulation.

8.1.4 Name forms
No stipulation.

8.1.5 Name constraints
No stipulation.

8.1.6 Certificate policy object identifier
No stipulation.

8.1.7 Usage of Policy Constraints extension
No stipulation.

8.1.8 Policy qualifiers syntax and semantics
No stipulation.

8.1.9 Processing semantics for the critical Certificate Policies extension
No stipulation.

8.2 CRL Profile

8.2.1 Version number(s)

No stipulation.

8.2.2 CRL and CRL entry extensions

No stipulation.

8.3 OCSP Profile

The ERCA does not provide OCSP service.

8.3.1 Version number(s)

No stipulation.

8.3.2 OCSP extensions

No stipulation.

9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

9.1 Frequency or circumstances of assessment

A full and formal audit on the ERCA operation is performed annually.

The EA may order a compliance audit by an auditor at any time at its discretion.

The auditor role may initiate a system audit by application to the ERCA OM.

9.2 Identity / qualifications of assessor

The EA must approve any person or entity seeking to perform a compliance audit.

The auditor must possess significant experience, or be accredited for:

- performance of information system security audits;
- PKI and cryptographic technologies;
- the operation of relevant PKI software;
- familiarity with the European Commission policies and regulations.

9.3 Assessor's relationship to assessed entity

The auditor approved by the EA shall either be:

- an entity within the European Commission organisational structure but separate from the ERCA

or

- an entity external to the European Commission.

9.4 Topics covered by assessment

The subjects of the compliance audit are the ERCA implementation of those technical, procedural and personnel practices described in this CPS.

Some areas of focus for the audit are:

- identification and authentication;
- operational functions/services;
- physical, procedural and personnel security controls;
- technical security controls.

9.5 Actions taken as a result of deficiency

There are three possible actions to be taken, should a deficiency be identified:

1. continue to operate as usual;
2. continue to operate a limited service;
3. suspend operation.

If a deficiency is identified, the auditor, with input from the EA, determines which of these actions to take. The decision regarding which of these actions to take will be based on the severity of the deficiency, the risks imposed, and the disruption to the subscriber and relying party community.

If Action 1 is taken, the EA and the ERCA OA are responsible for ensuring that corrective actions are taken within the time limit stipulated in the audit report. At that time, or earlier if approved by the EA and auditor, the audit team shall reassess. If, upon reassessment, corrective actions have not been taken, the auditor determines if more severe action (e.g. actions 2 or 3) is required.

If Action 2 is taken, the ERCA continues with the operation of a limited service stipulated in the audit report. The level of service may include or exclude any of the following activities:

- ERCA repository operation;
- NA policy approval or maintenance;
- ERCA maintenance operations;
- public key certification operations;
- motion sensor key distribution operations.

If Action 3 is taken, the status of all ERCA certificates affected by the deficiency shall be modified appropriately. The EA and the ERCA OA are responsible for reporting the status of any corrective action to the auditor on a weekly basis. The EA and auditor together determine when the reassessment is to occur. If the deficiencies are deemed to be corrected upon reassessment, the ERCA shall resume service and update affected certificate status information appropriately.

9.6 Communication of results

Results of the annual audit are provided to the EA and the ERCA. In the case of Actions 2 and 3, the European Authority ensures that all subscribers are informed of the action. Communication with the purpose of informing subscribers of any deficiency and action is performed by the usual procedures for communicating with national authorities.

10 OTHER BUSINESS AND LEGAL MATTERS

10.1 Fees

10.1.1 Certificate issuance or renewal fees
No stipulation.

10.1.2 Certificate access fees
No stipulation.

10.1.3 Revocation or status information access fees
No stipulation.

10.1.4 Fees for other services
No stipulation.

10.1.5 Refund policy
No stipulation.

10.2 Financial responsibility

10.2.1 Insurance coverage
No stipulation.

10.2.2 Other assets
No stipulation.

10.2.3 Insurance or warranty coverage for end-entities
No stipulation.

10.3 Confidentiality of business information

10.3.1 Scope of confidential information

All information that is not considered by the EA to be public domain information is for Commission internal use only..

Information held in audit trails is restricted to the European Commission and shall not be released outside the institution, unless required by law, regulations, or provisions of this CPS.

The results of annual audits are restricted, with exceptions as outlined in Section 9.6 of this CPS.

Audit logs are restricted, with exceptions as outlined in Section 9.6 of this CPS.

10.3.2 Information not within the scope of confidential information

The following information is public:

- information included in public key certificates issued by the ERCA;
- certificate status information in the ERCA repository;
- the ERCA Policy [3] and this CPS.

When certificate status is changed by the ERCA, a reason code is included in the certificate status entry for the action. The reason code is public and may be shared with all other subscribers and relying parties. However, no other details concerning the change of status are disclosed.

10.3.3 Responsibility to protect confidential information

The ERCA does not disclose keys, certificates, key distribution messages, or related information to any third party, except when:

- authorised by the ERCA Policy [3] and this CPS;
- required to be disclosed by law, European Commission, European and Member State regulations, or court order;
- authorised by the subscriber when necessary to effect an appropriate use of the certificate or key distribution message.

Any requests for disclosure of non-public information must be signed and delivered to the ERCA.

Any keys held by the ERCA shall be released only to an authorised European Commission organisational authority, in accordance with this CPS, and the ERCA Policy [3], or a law enforcement official, in accordance with European Commission regulations, European and State Members Law and this CPS.]

10.4 Privacy of personal information

10.4.1 Privacy plan

The ERCA does not archive personal information subject to the collection, maintenance, retention and protection requirements of Regulation N° 45/2001 of the European Parliament and of the Council of 18 December 2000.

10.4.2 Information treated as private

Personal identification information, contact information, and authorisations of the couriers transporting data between the national OEs and the ERCA are private.

Personal identification information, contact information, and authorisations of ERCA staff are private.

10.4.3 Information not deemed private

The affiliation of couriers transporting data between the national OEs and the ERCA is not deemed private.

10.4.4 Responsibility to protect private information

Personal information stored locally by the ERCA is restricted, and access is only granted to those with an official need-to-know.

10.4.5 Notice and consent to use private information

No stipulation.

10.4.6 Disclosure pursuant to judicial or administrative process

The ERCA will not disclose private information to any third party, except when:

- authorised by the ERCA Policy [3] and this CPS;
- required to be disclosed by law, European Commission, European and Member State regulations, or court order.

Any requests for disclosure of private information must be signed and delivered to the ERCA.

10.4.7 Other information disclosure circumstances

No stipulation.

10.5 Intellectual property rights

The software developed for the ERCA is the property of the European Commission.

10.6 Representations and warranties

10.6.1 ERCA representations and warranties

The ERCA warrants and promises to:

- provide certification services consistent with the ERCA Policy and this CPS;
- provide key management services including certificate issuance, key distribution, publication, and status information, in accordance with the ERCA policy and this CPS.

The European Commission and its staff make no representations, warranties or conditions, express or implied, other than as expressly stated in identified in the ERCA Policy [3] and this CPS.

10.6.2 RA representations and warranties

The ERCA RA warrants and promises to perform the identification and authentication procedures as set forth in Section 3 of this CPS.

10.6.3 Subscriber representations and warranties

ERCA subscribers and motion sensor key recipients warrant and promise to:

- make true representation at all times to the ERCA regarding information in their certificates and / or key distribution requests, and other identification and authentication information;
- comply with the obligations defined in the ERCA Policy [3] and this CPS.

10.6.4 Relying party representations and warranties

Relying parties warrant and promise to use Annex I(B) public keys, certificates, and motion sensor key distribution messages only for the purposes authorised by the ERCA Policy [3] and this CPS.

10.6.5 Representations and warranties of other participants

No stipulation.

10.7 Disclaimers of 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.

10.8 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 the ERCA Policy [3] and this CPS;
- 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:

- the certificate or its associated public/private key pair used by a subscriber or relying party;
- the motion sensor master key distribution message used by a recipient 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 digital tachograph key management system.

Requesters 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 the ERCA Policy and this CPS.

10.9 Indemnities

No stipulation.

10.10 Term and termination

10.10.1 Term

ERCA Policy [3] and CPS become effective from the date of approval, and remain in force until amended, according to the amendment procedure of Section 10.12, or terminated.

The maximum term for the ERCA Policy [3] and CPS corresponds to the lifetime of the European root keys, defined in [3].

Service agreements become effective from the date of signature by the two parties to the agreements, and remain in force for the duration defined in the agreement, unless amended according to the procedure defined in the agreement itself.

The duration of a service agreement corresponds to the validity period of the public key certificates issued to the subscriber, as defined in [3].

10.10.2 Termination

No stipulation.

10.10.3 Effect of termination and survival

No stipulation.

10.11 Individual notices and communications with participants

Official notices and communications with participants in the digital 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, the ERCA Policy [3] and this CPS may require modification as well. Changes to the operations will occur consistent with the administrative requirements stipulated in Section 10.12 of this CPS.

10.12 Amendments

This CPS shall be reviewed in its entirety every year. Errors, updates, or suggested changes to this document shall be communicated to the ERCA OA.

10.12.1 Procedure for amendment

1. Requests for changes to the CPS shall be directed to the ERCA. Such communication must include a description of the change, a rationale, and contact information for the person requesting the change.
2. Notification of change requests will be posted on the ERCA web site. The notification shall include the change request; the final date for receipt of comments; and the proposed effective date of change.
3. Comments shall be directed to the ERCA. Such communication must include contact information for the person submitting the comments.
4. The ERCA shall accept, accept with modifications, or reject the proposed change after completion of the comment period. ERCA disposition of proposed changes are reviewed with the EA. Decisions with respect to the proposed changes are at the discretion of the ERCA and the EA.
5. Change decisions will be posted to the ERCA web-site. The decision shall include the effective date of change.

10.12.2 Notification mechanism and period

The only changes that may be made to this CPS with no change to the document version number and no notification to the MSAs or the EA are editorial or typographical corrections.

The ERCA may change the contact information in section 1.4. with notification to the NAs but without change to the document version number.

All other changes to this CPS shall be made according to the amendment procedure.

10.12.3 Circumstances under which OID must be changed

Not applicable.

10.13 Dispute resolution provisions

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.

10.14 Governing law

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

10.15 Compliance with applicable law

No stipulation.

10.16 Miscellaneous provisions

10.16.1 Entire agreement

11 REFERENCES

[1] Council Regulation (EC) No 2135/98 of 24th September 1998; Official Journal of the European Communities L274, 09.10.98.

[2] Commission Regulation (EC) No 1360/2002 of 13th June 2002; Official Journal of the European Communities L207, 05.08.2002.

[3] Commission Regulation (EC) No 432/2004 of 5th March 2004; Official Journal of the European Communities L71, 10.03.2004.

[4] Digital Tachograph System – European Root Policy; European Commission Special Publication S.P.I.04.131 ; http://dtc.jrc.it.

[5] Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Request for Comments No.3647); http://www.ietf.org/rfc/rfc3647.txt

[6] Commission Regulation (EC) No 1360/2002, Annex I(B) Appendix 11 - Common security mechanisms

[7] ISO / IEC 16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

[8] Commission Decision No.2001/844/EC, ECSC, Euratom of 29th Nov. 2001Commission Provisions on Security; Official Journal of the European Communities L 317 of 03.12.2001.