EUROPEAN COMMISSION
DIRECTORATE-GENERAL
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.04.131

Digital Tachograph System
European Root Policy

Version 2.0

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.04.131

Blank page

Table of Contents

Blank page

Blank page

1 INTRODUCTION

The digital tachograph system has been introduced by Council Regulation 3821/85 as amended by Council Regulation 2135/98 [1] and Commission Regulation 1360/2002 [2].

Commission Regulation 1360/2002 [2] includes in Annex I(B) - *Requirements for construction, testing, installation, and inspection* - the technical description of the digital tachograph system. Increasingly detailed technical information is contained in a series of eleven appendices to Annex I (B).

With regard to the key management issues addressed by the Annex I(B); Appendix 11 requirement CSM_007 [6] states:

> *At European level, a single European key pair (EUR.SK and EUR.PK) shall be generated. The European private key shall be used to certify the Member States public keys. Records of all certified keys shall be kept. These tasks shall be handled by a European certification authority, under the authority and responsibility of the European Commission.*

Annex I(B) Appendix 11 requirement CSM_008 states:

> *At Member State level, a Member State key pair (MS.SK and MS.PK) shall be generated. Member States public keys shall be certified by the European Certification Authority. The Member State private key shall be used to certify public keys to be inserted in equipment (vehicle unit or tachograph card). Records of all certified public keys shall be kept with the identification of the equipment to which it is intended. These tasks shall be handled by a Member State certification authority. A Member State may regularly change its key pair.*

Annex I(B) Appendix 11 requirement CSM_009 states:

> *At equipment level, one single key pair (EQT.SK and EQT.PK) shall be generated and inserted in each equipment. Equipment public keys shall be certified by a Member State certification authority. These tasks may be handled by equipment manufacturers, equipment personalisers or Member State authorities. This key pair is used for authentication, digital signature and encipherement services*

An overview of the security measures required by the digital tachograph system is contained in the *Common Security Guidelines* [3].

Information and guidance on the processes to be implemented at the Member State level are provided by the *Guideline and Template National CA Policy for the Digital Tachograph System* [4].

This policy is developed according to the guidelines presented in Section 8 *Framework for the definition of other certificate policies* of the ETSI standard TS 102 042 *Policy requirements for certification authorities issuing public key certificates* [5].

The ETSI TS 102 042 standard was chosen for its concise and comprehensive description of current best practices in the implementation of a PKI. The ETSI standard does not provide solutions to all of the requirements of the Regulation, and so complete conformity to ETSI TS 102 042 is not required.

2 ROLES AND RESPONSIBILITIES

2.1. The European Commission service responsible for the ERCA policy is referred to hereinafter as the *European Authority*.

2.2. The contact address of the European Authority is:

European Commission
Directorate General for Transport and Energy
Unit E4 – Satellite Navigation System (Galileo); Intelligent Transport
Rue de Mot, 28
B-1040 Bruxelles

2.3. The European Commission service responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States is referred to hereinafter as the ERCA.

2.4. The contact address of the ERCA is:

Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)

2.5. The European Authority appoints the organisation which implements the ERCA policy and provides key certification services to the Member States.

2.6. The European Authority shall ensure that the ERCA has the resources required to operate in conformity with this policy.

2.7. Complaints from Member State Authorities about the services provided by the ERCA shall be addressed to the European Authority to be dealt .

2.8. The European Authority shall manage the ERCA policy change procedure described in Chapter 8.

2.9. The ERCA shall document its implementation of the ERCA policy in a Certification Practices Statement.

2.10. The ERCA shall make the contents of its CPS available to Member State Authorities and / or Member State Certification Authorities on a “need to know” basis.

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

2.12. This ERCA policy was approved by the European Authority on 9th July 2004

2.13. Information on the structure of the European Commission is publicly available on the Internet (see for example http://europa.eu.int/comm).

3 ERCA POLICY MANAGEMENT AND SCOPE

3.1. The policy of the ERCA applies only to the cryptographic keys and key certificates used in the mutual authentication, secure messaging and digital signature mechanisms of the digital tachograph system described in Annex I(B) [6] and ISO/CD 16844-3 [7].

3.2. Public key certificates issued by the ERCA are intended for purposes as mandated by the Regulation only.

3.3. Subscribers to the ERCA are restricted to the Member State authorities according to Annex I (B) Appendix 11 requirement CSM_008 [6].

3.4. Business and security requirements for the ERCA are described in Chapter 4 of this document.

3.5. The ERCA policy is available in electronic form from the web site http://dtc.jrc.it

3.6. ERCA documents shall be drafted in English. Translations may be available, but only the English version is authoritative.

3.7. Official communications between the ERCA and Member State Authorities shall use registered mail.

4 ERCA BUSINESS AND SECURITY REQUIREMENTS

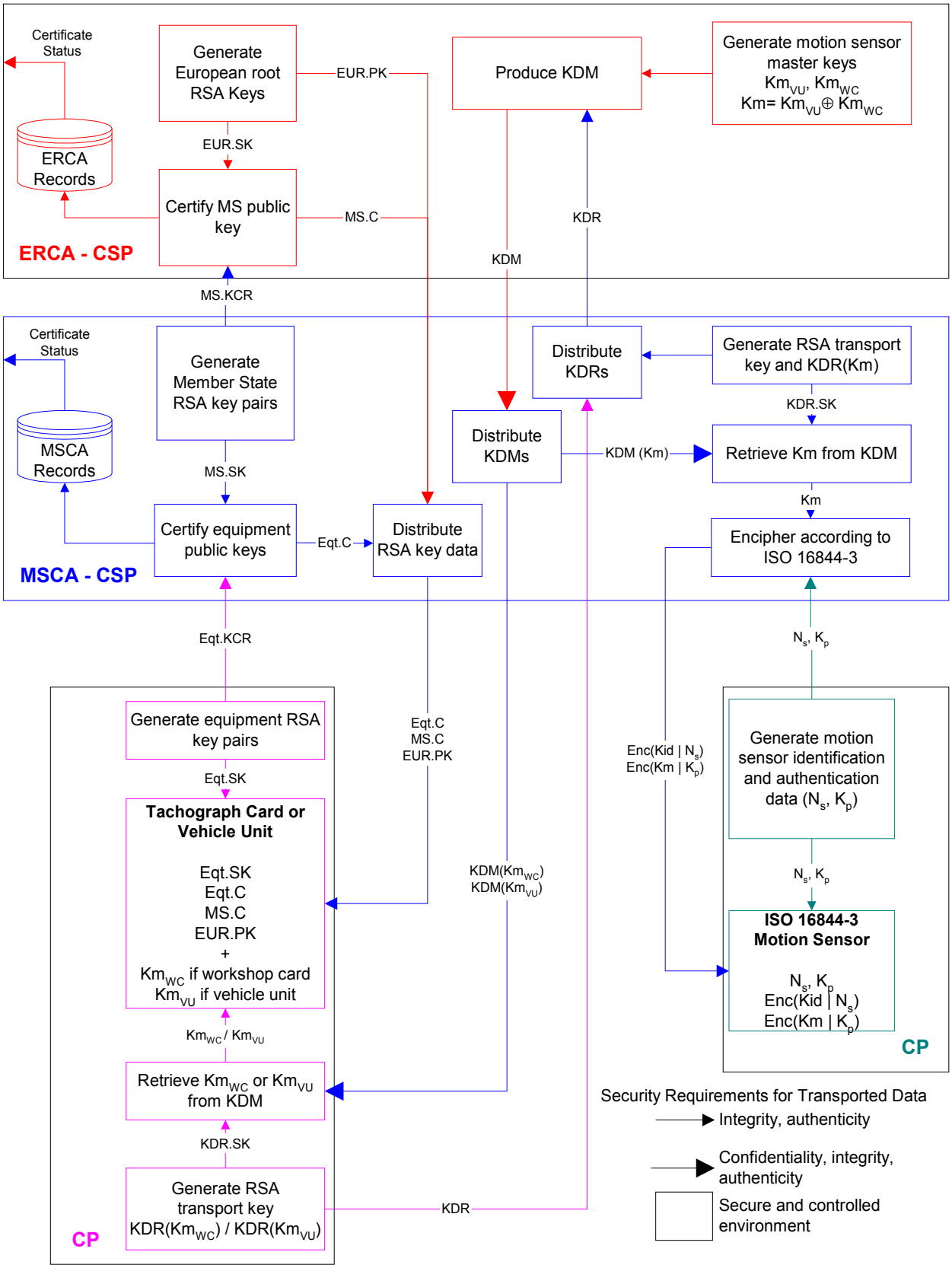

Figure 1 Description of Annex I(B) key management

The key and certificate management in the digital tachograph system is depicted in Figure 1. Four entities are depicted: the ERCA certification service provider (CSP); an MSCA CSP; and the two types of component personaliser (CP): tachograph card or vehicle unit manufacturing; and motion sensor manufacturing.

The ERCA and MSCA CSPs in Figure 1 create and maintain appropriate secret encryption keys and use them to validate digital tachograph security data, only after verifying that the data to encrypt are complete, correct, and duly authorised.

The card, vehicle unit or motion sensor CPs in Figure 1 insert validated security data into digital tachograph equipment by appropriately secured means.

Abbreviations in Figure 1 are as defined in Annex I(B) Appendix 11 [6], ISO / IEC 16844-3 *Motion sensor interface* [7] or Chapter 11 of this document.

4.1 Security Requirements

4.1.1 The ERCA implementation shall conform with the best practices described in ISO 17799 – *Information technology – Code of practice for information security management* [8].

4.1.2 The ERCA shall maintain the confidentiality of the root RSA private key and of the copies it keeps of the motion sensor master keys.

4.1.3 The ERCA shall maintain the integrity and availability for the purposes designated in the Regulation, of the root RSA key pair; and of the motion sensor master keys.

4.1.4 The ERCA shall verify the authenticity, integrity, and uniqueness in the domain of the Regulation of every MSCA public key modulus and key identifier submitted for certification.

4.1.5 The authenticity and integrity of the ERCA public key and MSCA RSA public key certificates shall be maintained during the entire lifetime of the keys.

4.1.6 The confidentiality, integrity, and authenticity of the motion sensor master keys shall be maintained.

4.1.7 The ERCA shall not generate RSA keys for a MSCA.

4.1.8 The ERCA shall distribute the motion sensor master keys and MSCA public key certificates on a "need to know" basis.

4.1.9 The ERCA shall maintain the integrity and availability of the MSCA public key certificate records.

4.1.10 The ERCA shall make available the ERCA RSA public key; and shall publish MSCA public key certificate revocation status.

4.1.11 The ERCA shall distribute test keys and maintain the integrity of test keys and certificates generated according to the Regulation for interoperability purposes.

4.2 Business Requirements

4.2.1 The MSCA RSA keys may be changed regularly. It is anticipated that each Member State will need only a small number of keys per year.

4.2.2 Key certification service from the ERCA shall depend on timely receipt of the MSA audit reports demonstrating that the Member State is continuing to fulfill its obligations as laid down in the approved MSA policy.

4.2.3 The time required for the ERCA to supply a MSCA public key certificate must be determined solely by the time required for correct execution of the ERCA procedures.

4.2.4 The ERCA will impose no limit on the number of MSCA keys that it will certify. However, if MSCA keys are distinguished only by the keySerialNumber field in a CertificationAuthorityKID (Annex I(B) Appendix 1 – *Data Dictionary* Section 2.36), the number of unique keys traceable to a MSCA will be limited to a maximum of 256.

4.2.5 The ERCA services (key certification and distribution) require low availability. Integrity and authenticity during transport will be assured by procedural means (e.g. trusted courier). Turnaround time of one month is guaranteed.

4.2.6 The required lifetime of the ERCA keys is not defined in Commission Regulation 1360/2002 [2]. The ERCA shall therefore maintain the RSA root key pair and the motion sensor master keys for a period of thirty years. Maintenance shall mean: confidentiality, integrity, and availability of the RSA private key, the motion sensor master keys; and integrity and availability of the RSA public key.

4.2.7 The ERCA assumes that technological progress over the next thirty years will render its IT systems obsolete. Measures to manage obsolescence are defined in the CPS.

4.3 Approval of MSA Policy

4.3.1 The objective of the approval process is to assure comparable levels of security in each Member State.

4.3.2 The ERCA shall review the MSA policy for conformity with the requirements defined in Section 5.3 Requirements of this document.

4.3.3 The ERCA shall provide key certification services to a MSA only if the outcome of the policy review provides sufficient grounds to judge that the requirements in Section 5.3 of this document will be met.

4.3.4 The ERCA shall archive the policy review report and the MSA policy for reference purposes.

4.4 ERCA Asset Classification

In Table 1, the column titles *C*, *I,* and *A* denote the security requirements of Confidentiality, Integrity, and Availability. The possible security levels are: X (very high); H (high); M (low to medium), according to the following definitions:

X (very high): breaking this security asset leads to a complete breakdown of the overall security and / or functionality of the digital tachograph system. It is very difficult or even impossible to overcome the damage caused.

H (high): breaking this security asset leads to severe security or functionality problems (at least temporarily) in the digital tachograph system. It will be difficult and / or time consuming to overcome the damage caused.

M (low to medium): breaking this security asset leads to (at most) limited security or functionality problems in the digital tachograph system. It is likely that these problems will be quickly recognised and / or can be easily cured.

The column Security Classification contains the security classification assigned to each asset and defined as follows:

High: the asset shall never leave a secure and controlled environment.

Medium: the asset shall not be disclosed to a third party without specific authorisation.

Low: the asset may be published.

Asset	C	I	A	Security Classification	Remarks
ERCA.SK	X	H	M	High	
ERCA.SK Backup	X	H	M	High	Two backups, one off-site.
ERCA.PK		H	M	Low	Recipient (MSCA) requires proof of origin (ERCA).
KmVU, KmWC, Km	X	H	M	High	Recipient (MSCA) requires proof of origin (ERCA).
Backups of KmVU, KmWC, and Km	X	H	M	High	Two backups, one off-site
Test keys		H		Low	Test key identifiers shall be included in MS.C Records.
ERCA Key Generator		X	M	High	Used only once. Requirements apply to key generator software before use.
ERCA Certificate Signing System		X	M	High	Physical access controls required. Requirements do not apply to software.
MS.KR	M	X	M	Low	Recipient (ERCA) requires proof of origin (MSCA). ERCA requires proof of knowledge of corresponding private key. ERCA must establish uniqueness in the domain of the Regulation of MSCA key.
MS.C		M	M	Low	Recipient (MSCA) requires proof of origin (ERCA).
MS.C Status Information	M	H	H	Low	Online certificate status information.
MS.C Records	M	H	M	Medium	Record of certificates issued by the ERCA becomes only proof of validity of a MS.C in case of ERCA.SK compromise.
ERCA CPS	H	M	M	Medium	
MSA policy		M	M	Low	
MSA Evaluation Report	H	M	M	Medium	

Table 1: ERCA asset classification

5 MSA OBLIGATIONS

5.1 Responsibilities

5.1.1 The MSA shall produce and maintain a MSA policy covering the following processes, where applicable:

a) issuing of tachograph cards, including keys and certificates;

b) issuing of vehicle unit keys and certificates;

c) issuing of motion sensor keys;

d) management of the Member State keys.

5.1.2 The operation and management practices related to these processes shall be documented in practices statements approved by the MSA.

5.1.3 The MSA shall be responsible for the provision of English versions of the MSA policies to the ERCA.

5.1.4 The MSA policy may consist of a collection of documents, as appropriate to the organisation of its component services.

5.1.5 Requirements on the content of the MSA policy are laid down in Section 5.3 of this document.

5.2 Submission of MSA Policy to ERCA

5.2.1 The objective of the submission of each MSA policy to the ERCA is to demonstrate comparable levels of security in each Member State.

5.2.2 The MSA shall submit the MSA policy in a formal communication to the ERCA.

5.2.3 The MSA policy shall be accompanied by a rationale addressing each requirement of Section 5.3.

5.3 Requirements

Formal Requirements

5.3.1 The MSA policy shall identify the entities in charge of operations.

Member State Key Pair Generation (RSA)

5.3.2 Member State Key Pairs for equipment key certification and for motion sensor master key distribution shall be generated and stored within a device which either:

a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9];

b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10];

c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.

d) is demonstrated to provide an equivalent level of security.

5.3.3 Member State Key Pair generation shall take place in a physically secured environment by

personnel in trusted roles under, at least dual control.

5.3.4 The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.

5.3.5 The generation of new Member State Key Pairs shall take into account the one month turn-around time required for certification by the ERCA (see Section 4.2.5).

ERCA Key Certification Requests and Motion Sensor Key Distribution Requests

5.3.6 The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.

5.3.7 The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.

5.3.8 The MSA shall recognise the ERCA public key in the distribution format described in Annex B.

5.3.9 The MSA shall use the physical media for key and certificate transport described in Annex C.

5.3.10 The MSA shall ensure that the Key Identifier (KID) and modulus (n) of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of the MSCA.

Member State Key Pair End of Life

5.3.11 The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either:

destroyed so that the private key cannot be recovered;

or

retained in a manner preventing its use.

Equipment RSA Keys

5.3.12 The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall

- ensure that any relevant prescription mandated by security certification of the equipment is met.
- ensure that both generation and insertion (if not onboard) takes place in a physically secured environment;
- unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used;

The last two of these requirements on generation shall be met by generating equipment keys within a device which either:

a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9];

b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10];

c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.

d) is demonstrated to provide an equivalent level of security.

RSA Key General

5.3.13 The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA policy.

5.3.14 The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA policy.

5.3.15 The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.

5.3.16 Key certification requests that rely on transportation of private keys are not allowed.

5.3.17 Key escrow is strictly forbidden (see definition 12.1).

Symmetric (TDES) Keys

5.3.18 The MSA shall prevent unauthorised use of its motion sensor keys.

5.3.19 The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO / IEC 16844-3 standard [7].

5.3.20 The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.

5.3.21 The MSA shall forward the workshop card motion sensor key (Km_{WC}) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.

5.3.22 The MSA shall forward the vehicle unit motion sensor key (Km_{VU}) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.

5.3.23 The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.

5.3.24 The MSA shall ensure that its motion sensor key copies are stored within a device which either:

a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9];

b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.

Certificate Generation

5.3.25 The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.

5.3.26 The MSA shall ensure availability of its equipment public key certification service.

5.3.27 The MSA shall only use the Member State Private Keys for:

a) the production of Annex I(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in Annex I(B) Appendix 11 *Common Security Mechanisms* [6];

b) production of the ERCA key certification request as described in Annex A.

c) issuing Certificate Revocation Lists if this method is used for providing certificate status information (see 5.3.31).

5.3.28 The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).

5.3.29 Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B) [6].

5.3.30 Unless key generation and certification is performed in the same physically secured environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.

Certificate Status Information

5.3.31 The MSA shall maintain and make certificate status information available.

Component Personalisation

5.3.32 The validity of a tachograph card certificate shall equal the validity of the tachograph card.

5.3.33 The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.

5.3.34 The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.

User Registration

5.3.35 The MSA shall ensure that users of cards are identified at some stage of the card issuing process.

Disaster Recovery

5.3.36 The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.

5.3.37 The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.

General Security Requirements

5.3.38 The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.

5.3.39 The MSA shall ensure that the policies address personnel training, clearance and roles.

5.3.40 The MSA shall ensure that appropriate records of certification operations are maintained.

5.3.41 The MSA shall include provisions for MSCA termination in the MSA policy.

5.3.42 The MSA policy shall include change procedures.

Audit

5.3.43 The MSA audit shall establish whether the Requirements of this Section are being maintained.

5.3.44 The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.

5.3.45 The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit

report, in English, to the ERCA.

5.3.46 The audit report shall define any corrective actions, including an implementation schedule, required to fulfill the MSA obligations.

6 ERCA PRACTICE

The ERCA shall provide the following services to the MSCAs:

a) Registration;

b) Certificate Generation;

c) Distribution;

d) Revocation;

e) Revocation status.

6.1 Certification Practices Statement

6.1.1 The ERCA CPS is the ERCA's procedural document, which details how the ERCA policy is enforced in day-to-day management. The document is developed by the ERCA. The ERCA CPS is owned by the ERCA.

6.1.2 The ERCA CPS shall be treated as restricted information.

6.1.3 The ERCA shall provide its complete CPS to the MSCAs and provide any information needed by the MSCAs.

6.1.4 The ERCA CPS shall be managed, reviewed, and modified following document control procedures.

6.2 ERCA Key Generation

6.2.1 The ERCA RSA keys shall be generated in accordance with Annex I(B) Appendix 11 CSM_014 [6].

6.2.2 Generation of the ERCA RSA keys, the motion sensor master keys, and their backup copies is undertaken in a physically secured environment by personnel in trusted roles under at least dual control. The key generation ceremony is described in the ERCA CPS.

6.2.3 The ERCA shall not generate RSA key pairs for its Subscribers (MSCAs).

6.2.4 A suite of test RSA and motion sensor keys, including MSCA keys, equipment keys, public key certificates, and source code, is available on request to the ERCA for the purposes of interoperability testing.

6.3 ERCA Key Storage, Backup and Recovery

6.3.1 The ERCA shall maintain the confidentiality, integrity, and availability of the root RSA private key and the motion sensor master keys.

6.3.2 The ERCA shall maintain only the following parameters of the root RSA key: the modulus (n), the public exponent (e), the private exponent (d).

6.3.3 The ERCA RSA private key and the motion sensor master keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual control in a physically secured environment.

6.3.4 Backup copies of the ERCA RSA private key and the motion sensor master keys shall be subject to the same level of security controls as the keys in use. One backup copy of the ERCA RSA private key and the motion sensor master keys shall be maintained off-site.

6.4 ERCA Key Distribution

6.4.1 The procedures for assuring confidentiality, integrity and authenticity during distribution are described in the ERCA CPS.

6.4.2 The ERCA shall distribute motion sensor master keys in a secure fashion on a "need to know" basis:

a) Km to MSCAs supporting motion sensor manufacturers;

b) Km_{VU} to MSCAs supporting vehicle unit manufacturers;

c) Km_{WC} to MSCAs supporting workshop card personalisers.

6.5 Key escrow

Key escrow is strictly forbidden. (see definition 12.1).

6.6 ERCA Key Usage

6.6.1 The ERCA RSA private key shall only be used for the production of MSCA public key certificates as described in Annex I(B), Appendix 11, CSM_018 [6].

6.6.2 The ERCA RSA private key shall only be used within a physically secure environment by personnel in trusted roles under at least dual control.

6.6.3 All events of ERCA private key usage shall be logged.

6.6.4 The ERCA shall not use the motion sensor master keys for any purpose.

6.7 End of ERCA Key Life Cycle

At the end of the life cycle, all copies of the ERCA RSA private key shall be destroyed such that the private key cannot be retrieved.

6.8 MSCA Requests

6.8.1 The ERCA shall ensure that MSCA public key certification requests and motion sensor master key distribution requests are complete, accurate, and duly authorised.

6.8.2 The ERCA shall ensure that, within the domain of MSCA public keys received by the ERCA, each MSCA public key has a unique Key Identifier (KID) and modulus (n), and that it has not been previously certified by the ERCA, or used for motion sensor key distribution.

6.8.3 The ERCA shall ensure that the MSCA has possession of the private key associated with the public key presented for certification or motion sensor key distribution.

6.8.4 After successful distribution of a new MSCA certificate, the ERCA shall update the certificate status information.

6.8.5 The ERCA shall keep Member State key certification requests, motion sensor key distribution requests, and public key certificates.

6.9 Certificate Validity

6.9.1 The ERCA will, by default, set the end-of-validity of MSCA public key certificates for tachograph cards to seven years from the date of signature production.

6.9.2 The ERCA will only issue undefined validity certificates when the MSCA specifies that the RSA keys will be used for the production of vehicle unit certificates (see KCR protocol in

Annex A).

6.9.3 The ERCA shall use the end-of-validity specified by the MSCA KCR if it does not exceed the limit defined in clause 6.9.1 above.

6.10 Certificate and Motion Sensor Key Distribution

The procedures by which certificates and motion sensor key distribution messages are made available to MSCAs are described in the ERCA CPS, and communicated to the MSAs.

6.11 Certificate Status Information

6.11.1 The status of MSCA public key certificates may be retrieved on line by any interested party using the public certificate status information from http://dtc.jrc.it.

6.11.2 Published certificate information shall consist of the Certificate Holder Reference, and message digests of the certificate itself.

6.12 Certificate Revocation

6.12.1 The procedures for certificate revocation are described in the CPS.

6.12.2 A MSA can ask for revocation of its own MSCA certificates.

6.12.3 The authenticity and integrity of a certificate revocation request shall be established before a certificate is revoked.

6.12.4 MSCA certificates shall be revoked on reasonable suspicion of compromise of the MSCA secret key.

6.12.5 The ERCA shall maintain the integrity of the certificate revocation status information.

7 ERCA MANAGEMENT AND OPERATION

7.1 Security Management

7.1.1 The ERCA administrative and management procedures, and the information security management system are subjected to periodic audits.

7.1.2 The ERCA retains responsibility for all aspects of the provision of certification services. No ERCA functions are outsourced to subcontractors.

7.1.3 Any changes to the information security infrastructure that will impact on the level of security provided shall be subject to a review.

7.1.4 The operating procedures for ERCA facilities, systems and information assets providing the certification services are subjected to revision control procedures defined in the ERCA CPS.

7.1.5 Security incidents are reported to the European Authority without unreasonable delay and at least within 8-hours of their detection.

7.2 Asset Classification

7.2.1 The ERCA information assets are listed in an inventory and assigned a level of protection consistent with the business and security requirements of Chapter 4.

7.2.2 ERCA information assets shall be assigned a security classification according to the need, priorities and degree of protection.

7.3 Personnel Security

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

7.3.2 Personnel training is managed according to a training plan described in the ERCA CPS.

7.3.3 Personnel appointment to trusted roles shall be managed in accordance with an established screening process.

7.3.4 Security roles and responsibilities are documented in job descriptions described in the ERCA CPS. Trusted roles, on which the security of the ERCA's operation is dependent, are clearly identified.

7.3.5 ERCA personnel job descriptions are defined from the viewpoint of separation of duties and least privilege.

7.3.6 The following trusted roles are defined:

a) Officer: Responsible for authenticating MSCA key certification requests. Authorised to produce RSA public key certificates for MSCAs;

b) Administrator: Responsible for generating ERCA RSA key pair and motion sensor master keys. Authorised to install, configure and maintain the ERCA system for certificate production;

c) Operator: Authorised to perform system backup and recovery;

d) Auditor: Authorised to view and maintain archives and audit logs of the ERCA trustworthy systems.

7.3.7 No single person shall be authorised to perform more than one of the trusted roles defined above.

7.4 Physical and Environmental Security

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

7.5 Records of MSCA Requests

7.5.1 ERCA certificate records shall consist, at minimum, of:

a) Certificate Holder Reference (CHR);

b) certificate end-of-validity (EOV);

c) the modulus (*n*) and exponent (*e*) of the MSCA public key;

d) the MSCA key certification request (KCR);

e) the MSCA certificate.

7.5.2 ERCA motion sensor key distribution records shall consist, at minimum, of:

a) MSCA public key identifier (KID);

b) the modulus (*n*) and exponent (*e*) of the MSCA public key;

c) the MSCA key distribution request (KDR);

d) the motion sensor key distribution message (KDM).

7.5.3 The integrity of key certificate records and of motion sensor key distribution records shall be maintained.

7.5.4 ERCA key and certificate management events shall be time stamped and logged.

7.5.5 The integrity of ERCA system event logs shall be maintained.

7.6 Disaster Recovery

7.6.1 The following incidents are considered to be disasters:

a) compromise or theft of the ERCA root key and / or the motion sensor master keys;

b) loss of the ERCA root key and / or the motion sensor master keys;

c) IT hardware failure.

7.6.2 In the event of compromise or theft of the ERCA root key and / or the motion sensor master keys, the ERCA shall inform immediately the Commission and the MSCAs and the Commission shall take appropriate measures in a reasonable delay.

7.6.3 In the event of loss of the ERCA root key, mutual authentication mechanisms will cease to operate once the validity of the member state public key certificates expires. This incident, from which there is, effectively, no recovery, is prevented by the use of multiple backup copies of the root keys, on a variety of storage media subjected to periodic controls.

7.6.4 In the event of loss of the motion sensor master keys, recovery may be achieved by transferring responsibility for the motion sensor master keys to an MSCA which holds any two of Km, Km_{VU}, and Km_{WC}. Any key can be recovered given knowledge of the other two. Measures to prevent this incident are the use of multiple backup copies of the motion sensor master keys, on a variety of storage media subjected to periodic controls. The way the responsibility transfer will be achieved is outside the scope of this document.

7.6.5 Protection against IT hardware failures is provided by redundancy, i.e. availability of duplicate IT hardware. To protect against hardware obsolescence, the ERCA systems will be reimplemented on new types of hardware, so that, at any moment, at least two systems capable of performing certification operations will be available.

7.7 ERCA Continuation

7.7.1 In the event of termination of the ERCA activity by the appointed organisation, the European Authority shall appoint a new organisation responsible for implementation of this policy and for the provision of key certification services to the Member States.

7.7.2 The ERCA shall transfer its assets (see Section 4.4) to the European Authority ensuring that confidentiality and integrity are maintained.

8 ERCA POLICY CHANGE PROCEDURES

8.1. The only changes that may be made to this policy without notification are editorial or typographical corrections.

8.2. Changes which the ERCA may make to this policy with notification to the MSAs but without comments from the MSAs are changes to the contact details.

8.3. All other changes to the ERCA policy shall be made only after notification to, and the receipt of comments from, the ERCA and the MSAs, according to the following procedure:

a) The MSAs or the ERCA shall submit proposals for change to the ERCA policy to the European Authority.

b) The European Authority shall distribute proposals to change the ERCA policy to the MSAs and to the ERCA.

c) The European Authority shall set an appropriate period for comments.

d) The MSAs and the ERCA may comment on the proposed changes within the defined period for comments.

e) The European Authority shall consider the comments and shall decide which, if any, of the notified changes to implement.

f) The European Authority shall notify the MSAs and the ERCA about its decision, and shall set an appropriate period for the changes to be implemented.

9 ISSUES OF STANDARDS CONFORMANCE

9.1. ETSI TS 102 042 contains no provisions for the management of symmetric encryption keys such as those used in the motion sensor (see ISO / IEC 16844-3 *Motion sensor interface* [7]).

9.2. ETSI TS 102 042 explicitly references ISO / IEC 9794-8 | ITU-T Recommendation X.509 *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks* [13].

9.3. X.509 certificates, were not adopted by the designers of the digital tachograph system.

9.4. A proprietary public key certificate structure based on the standard ISO / IEC 9796-2 *Information Technology – Security Techniques – Digital signature schemes giving message recovery* [14], and incompatible with X.509, was developed for the purposes of the Regulation (see Annex I(B) Appendix 11 [6]).

9.5. The signature minimisation step - described in Annex A, Section A.4 of the ISO / IEC 9796-2: 1997 standard - shall not be performed during the production of Annex I(B) public key certificates.

10 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] Common Security Guidelines, v1.0; Card Issuing Group SWG3; available from: http://www.urba2000.com/chrono/public/public.htm

[4] Guideline and Template National CA Policy for the Digital Tachograph System, v1.0; Card Issuing Group SWG3; available from http://www.urba2000.com/chrono/public/public.htm

[5] ETSI TS 102 042 V1.1.1 (2002-04) *Policy requirements for certification authorities issuing public key certificates*

[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] ISO / IEC 17799:2000 *Information technology – Code of practice for information security management*

[9] FIPS PUB 140-2 *Security Requirements for Cryptographic Modules* NIST, 2001

[10] CEN Workshop Agreement 14167-2: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)*

[11] ISO / IEC 15408 (Parts 1 to 3) *Information technology – Security techniques – Evaluation criteria for IT security*.

[12] ITSEC *Information Technology Security Evaluation Criteria* 1991 v1.2

[13] ISO / IEC 9794-8 | ITU-T Recommendation X.509 *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[14] ISO / IEC 9796-2 (1997-09-01) *Information Technology – Security Techniques – Digital signature schemes giving message recovery*

[15] PKCS#1 v2.0: *RSA Cryptography Standard*, RSA Laboratories, October 1, 1998.

11 ABBREVIATIONS

CP	Component Personaliser
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Services Provider
EA	European Authority
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request (for motion sensor master keys)
KDM	Key Distribution Message (encrypted motion sensor master key)
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
MSA	Member State Authority
MSCA	Member State Certification Authority
PK	RSA public key
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SK	RSA secret key

12 DEFINITIONS

12.1. 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.

ANNEX A: KEY CERTIFICATE REQUESTS

A.1 MSCA Key Certification Request

A.1.1 The following MSCA public key certificate request format and protocol shall be used by the ERCA. This format is based solely on security mechanisms already defined in the Regulation. The protocol demonstrates that the entity (E) submitting the certification request possesses the private RSA key (E.SK) associated with the public RSA key (E.PK) whose certification by the ERCA is required.

A.1.2 The entity (E) submitting the key certification request is identified by procedural means defined in the ERCA CPS.

A.1.3 The MSCA shall create the CertificateContent (164 bytes) according to the following rules:

CPI	Certificate Profile Identifier. The value for this field is 01h (1 byte)
CAR	Certification Authority Reference. 8 byte octet string identifying the ERCA, as defined in Annex I(B), Appendix 1, Section 2.36. This field shall be the octet string: ‘FDh’ NationNumeric: European Community ‘45h’ ‘43h’ ‘20h’ NationAlpha: ‘EC ’ ‘00h’ keySerialNumber ‘FFh’ ‘FFh’ additionalInfo ‘01h’ caIdentifier Test key requests shall contain the values ‘54h’, ‘4Bh’ (‘TK’) in the additionalInfo field.
CHA	Certificate Holder Authorization. 7 byte octet string as defined in Annex I(B) Appendix 1, Section 2.34 having the value: ‘FFh’, ‘54h’, ‘41h’, ‘43h’, ‘48h’, ‘4Fh’ EquipmentType: 1 byte as defined in Annex I(B) Appendix 1, Section 2.52 The MSCA shall specify the EquipmentType 6 (vehicle unit) when requesting an undefined validity certificate. NB: The ERCA shall set the EquipmentType to 0 (used to identify CA key certificates) during signature production.
EOV	End Of Validity. 4 byte integer representing the number of seconds since midnight January 1 1970 GMT, as returned by the Unix time()-function. For undefined, i.e. unlimited, validity shall be ‘FFh’, ‘FFh’, ‘FFh’, ‘FFh’
CHR	Certificate Holder Reference. unique 8-byte octet string identifying the MSCA, as defined in Annex I(B), Appendix 1, Section 2.36.
n	The modulus of the public key of the Certificate Holder; size 128 bytes (1024 bits)
e	The exponent of the public key of the Certificate Holder, size of 8 bytes (64 bits)

A.1.4 With the CertificateContent as defined above, the MSCA key certification request is prepared as follows:

1	Compute the SHA-1 hash of the CertificateContent (164 bytes), yielding *HASH(Cc)* (20 bytes).
2	Format *HASH(Cc)* as a fully recoverable message embedded in a 1024-bit message representative as per ISO/IEC 9796-2:1997 with implicitly identified SHA-1 hash: as follows: '4Bh' | eighty-five times 'BBh' | 'BAh' | *Hash(Cc)* | *Hash(Hash(Cc))* | 'BCh'
3	Sign the above message representative using E.SK, by applying the RSASP1 signature primitive defined in PKCS#1, yielding signature SKR (128 bytes).
4	Concatenate *Cc* and *SCc* to give the key certification request (292 bytes)

A.1.5 The key certification request is processed by the ERCA as follows:

1	Extract E.PK from the *Cc* field of the key certification request.
2	Open the *SCc* field of the key certification request using E.PK.
3	Verify the contents of the ISO 9796-2 signature, yielding the recovered message *Mr'* (20 bytes)
4	Compute the SHA-1 hash of the *Cc* field of the key certification request, yielding *HASH (Cc)* (20 bytes)
5	Reject the key certification request if *Mr'* does not equal *HASH(Cc)*

A.1.6 If the key certification request is accepted, the ERCA shall proceed with additional checks on the certificate content. These checks are described in the following sections.

A.1.7 The ERCA shall communicate with the MSA via an alternate channel to establish that the key certification request is duly authorised.

A.1.8 During this communication, the ERCA shall check that the SHA-1 hash of the key certification request is known by the MSA.

A.2 Checks on the Value and Identity of RSA Keys

A.2.1 The ERCA shall apply the following checks to each RSA public key, including test keys, submitted for certification.

A.2.2 The modulus (n) shall be an odd integer, falling within the range:

$$2^{1023}+1 \le n \le 2^{1024}-1$$

A.2.3 The modulus (n) shall be checked for uniqueness against the records of keys signed by the ERCA.

A.2.4 The public exponent (e) shall be an odd integer, falling within the range:

$$3 \le e \le 2^{64}-1$$

A.2.5 The Certificate Holder Reference (CHR) shall be checked for uniqueness against the records of keys signed by the ERCA.

A.2.6 The ERCA shall reject MSCA key certification requests if any of the requirements above are not satisfied.

A.3 Checks on End of Validity and Equipment Type

A.3.1 The regulation identifies seven types of equipment (see Regulation 1360/2002 Annex I(B), Appendix 1, Section 2.52 [2]).

A.3.2 Member State public key certificates inserted into four equipment types (driver, workshop, control, and company cards) shall have a limited validity.

A.3.3 Member State public key certificates inserted into one equipment type (vehicle unit) shall have an undefined end-of-validity.

A.3.4 Public key certificates are not applicable to manufacturer cards and motion sensors.

A.3.5 The ERCA shall check the equipment type specified in the 7th byte of the CHA field of the CertificateContent, and shall set undefined EOV only if this byte has the value 6, identifying the vehicle unit equipment type.

A.3.6 During signature production, the ERCA shall set the EquipmentType value to 0 (as required to identify a CA certificate).

ANNEX B: ERCA PUBLIC KEY DISTRIBUTION FORMAT

B.1 The ERCA public key shall be distributed to Subscribers in the following format:

CHR	Certificate Holder 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 public key of the Certificate Holder; size 128 bytes (1024 bits)
e	The exponent of the public key of the Certificate Holder, size of 8 bytes (64 bits)

B.2 The ERCA public key shall be provided directly to Subscribers by trusted courier. The use of a trusted courier establishes the authenticity and integrity of the public key.

ANNEX C: KEY DISTRIBUTION

The physical media used to transport MSCA key certification requests, MSCA certificates, the ERCA public key, and the motion sensor master keys are described below.

C.1 Transport Media

C.1.1 For official and for testing purposes, the ERCA shall accept key certification requests and motion sensor key distribution requests, and distribute the ERCA public key, the MSCA key certificates and the motion sensor master key distribution messages on CD-R media.

C.1.2 The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

C.1.3 Filenames shall be in 8.3 format. Filename extensions shall be:
txt for files containing hexadecimal ASCII data;
pem for files containing Base64 encoded data;
bin for files containing binary data.

C.1.4 Official key certification requests, key certificates, and motion sensor key distribution requests shall be accompanied by a paper copy of the data formatted according to a template defined by the ERCA.

C.1.5 For testing purposes only, the ERCA shall accept and dispatch key certification requests, example certificates, and example keys on 3.5 inch DOS floppy disks, or as e-mail attachments.

C.2 Transport Procedures

C.2.1 Official MSCA key certification requests, MSCA key certificates, the ERCA public key, motion sensor master key distribution requests, and motion sensor master key distribution messages shall be carried by a trusted courier appointed by the MSA.

C.2.2 The MSA contact person shall communicate the identification data of the trusted courier to the ERCA in useful time (typically 5 working days) for preparation of the permits required to enter EU Commission premises.

ANNEX D: MOTION SENSOR MASTER KEY DISTRIBUTION

D.1 Motion Sensor Master Key Request

D.1.1 The following key request format and protocol shall be used to transfer one of the motion sensor master keys (Km, KmWC, and KmVU) from the ERCA to a MSCA. The protocol is based on the key certification request protocol.

D.1.2 The protocol uses one RSA key pair generated by the MSCA for the sole purpose of ensuring the confidentiality of one of the Km, KmVU, or KmWC motion sensor master keys during transport between the ERCA and the MSCA.

D.1.3 The motion sensor key distribution procedure uses the ERCA KCR protocol to demonstrate that the entity (E) submitting the request possesses the private RSA key (E.SK) associated with the public RSA key (E.PK) provided for encryption of the motion sensor master key.

D.1.4 The entity (E) submitting the key certification request is identified by procedural means defined in the ERCA CPS.

D.1.5 The MSCA shall create the motion sensor master key distribution request (KDR - 164 bytes) according to the following rules:

CPI	Certificate Profile Identifier. The value for this field is 01h (1 byte)
CAR	Certification Authority Reference. 8 byte octet string identifying the ERCA, as defined in Annex I(B), Appendix 1, Section 2.36. This field shall be the octet string: ‘FDh’ NationNumeric: European Community ‘45h’ ‘43h’ ‘20h’ NationAlpha: ‘EC ’ ‘00h’ keySerialNumber ‘FFh’ ‘FFh’ additionalInfo ‘01h’ caIdentifier Test key requests shall contain the values ‘54h’, ‘4Bh’ (‘TK’) in the additionalInfo field.
MRA	Message Recipient Authorization. 7 byte octet string having the value formed by concatenating: ‘FFh’, ‘54h’, ‘41h’, ‘43h’, ‘48h’, ‘4Fh’ with the motion sensor master key type: 1 byte as defined below: ‘07h’: Km, motion sensor master key; ‘27h’: KmWC, motion sensor master key inserted in workshop cards; ‘67h’: KmVU, motion sensor master key inserted in vehicle units; NB: These codes are based on the EquipmentType codes defined in Annex I(B) Appendix 1, Section 2.52.
EOV	End Of Validity. 4 byte octet string having the value: ‘FFh’, ‘FFh’, ‘FFh’, ‘FFh’

KID	Key Identifier: unique 8-byte octet string identifying a public key of a MSCA, as defined in Annex I(B), Appendix 1, Section 2.36, with the following modifications: NationNumeric: as appropriate for the MSCA NationAlpha: as appropriate for the MSCA keySerialNumber: '00h' .. 'FFh' progressive counter of KDRs from the national CA additionalInfo: '4Bh' '52h' ('KR'for Key Request) master key type: 1 byte as defined below: '07h': Km, motion sensor master key; '27h': KmWC, motion sensor master key inserted in workshop cards; '67h': KmVU, motion sensor master key inserted in vehicle units
n	The modulus of E.PK used for motion sensor master key encryption; size 128 bytes (1024 bits)
e	The exponent of E.PK used for motion sensor master key encryption, size of 8 bytes (64 bits)

D.1.6 The MSCA processes the key distribution request as follows:

1	Compute the SHA-1 hash of the request (164 bytes), yielding *HASH(KR)* (20 bytes).
2	Format *HASH(KR)* as a fully recoverable message embedded in a 1024-bit message representative as per ISO/IEC 9796-2:1997 with implicitly identified SHA-1 hash: as follows: '4Bh' | eighty-five times 'BBh' | 'BAh' | *Hash(KR)* | *Hash(Hash(KR))* | 'BCh''
3	Sign the above message representative using E.SK, by applying the RSASP1 signature primitive defined in PKCS#1, yielding signature *SKR* (128 bytes).
4	Concatenate *KR* and *SKR* to give the motion sensor master key request (292 bytes)

D.1.7 The motion sensor master key distribution request is processed by the ERCA as follows:

1	Extract E.PK from the *KR* field of the master key request.
2	Open the *SKR* field of the key certification request using E.PK.
3	Verify the contents of the ISO 9796-2 signature, yielding the recovered message *Mr'* (20 bytes)
4	Compute the SHA-1 hash of the *KR* field of the motion sensor master key request, yielding *HASH(KR)* (20 bytes)
5	Reject the master key request if *Mr'* does not equal *HASH(KR)*

D.1.8 If the motion sensor master key request is accepted, the ERCA shall proceed with additional checks on the request content. These checks are described in the following section.

D.1.9 The ERCA shall communicate with the MSA via an alternate channel to establish that the motion sensor master key request is duly authorised.

D.1.10 During this communication, the ERCA shall check that the SHA-1 hash of the motion sensor master key request is known by the MSA.

D.2 Checks on Request Content

D.2.1 The RSA modulus (n) shall be an odd integer, falling within the range:

$$2^{1023}+1 \leq n \leq 2^{1024}-1$$

D.2.2 The RSA modulus (n) shall be checked for uniqueness against the records of MSCA RSA public keys received by the ERCA.

D.2.3 The RSA public exponent (e) shall be an odd integer, falling within the range:

$$3 \leq e \leq 2^{64}-1$$

D.2.4 The policy of the MSCA identified by the Key Identifier (KID) shall be checked to justify the type of motion sensor master requested.

D.2.5 The ERCA shall reject motion sensor master key requests if any of the requirements above are not satisfied.

D.3 Encryption of the Motion Sensor Key

D.3.1 The ERCA shall construct the 24-byte labelled motion sensor key (LKM) according to the following rules:

KID	Key Identifier. Unique 8 byte octet string identifying the MSCA as defined in Annex I (B), Appendix 1, Section 2.36, with the following modifications to identify the requested motion sensor master key: NationNumeric: as appropriate for the MSCA NationAlpha: as appropriate for the MSCA keySerialNumber: '00h' .. 'FFh' progressive counter of KDRs from the national CA additionalInfo '44h', '4Bh' ('DK' for DES Key) master key type: 1 byte as defined below: '07h': Km, motion sensor master key; '27h': KmWC, motion sensor master key inserted in workshop cards; '67h': KmVU, motion sensor master key inserted in vehicle units.
KM	Motion sensor master key (16 bytes).

D.3.2 The ERCA shall encrypt the 24-byte LKM with the public key provided by the MSCA according to RSA encryption scheme RSAES-PKCS1-v1_5-ENCRYPT [15] to produce the 128-byte encrypted DES key (EDK).

D.3.3 The ERCA shall distribute the encrypted motion sensor master key to the requesting MSCA in the following 136-byte key distribution message (KDM) format:

KID	Key Identifier: same value as defined in D.3.1.
EDK	Encrypted DES key. The motion sensor master key encrypted according to RSA encryption scheme RSAES-PKCS1-v1_5-ENCRYPT [15]; size of 128 bytes (1024 bits).

D.4 Decryption of the Motion Sensor Key

D.4.1 The MSCA shall decrypt an EDK with the private key used to produce the motion sensor master key distribution request, according to the RSA decryption scheme RSAES-PKCS1-V1_5-DECRYPT.

D.4.2 Only if this decryption succeeds and outputs a message of size 24 bytes, in which the first 8 bytes are equal to the first 8 bytes of the KDM, shall the last 16 bytes of the message be used as the motion sensor master key of the type defined by the KID field of the KDM.