MINISTRY OF INFRASTRUCTURE

Member State Authority Policy - Poland

Warsaw, 14th of March 2019 – ver. 01.02

Document approval

	Name	Organization	Date	Signature

Document version control

Version	Issue date	Description
01.00	18/01/2019	Initial version
01.01	09/03/2019	Updated version based on Mr Michel Chiaramello remarks stated in the document “Review of the Poland policy for the smart tachograph V1.0”, ref. Ares(2019)1520724, dated 6th March 2019. All proposed changes in the mentioned above document have been adapted.
01.02	14/03/2019	Updated version based on Mr Michel Chiaramello remarks stated in the document “Review of the Poland policy for the smart tachograph V1.01”, ref. Ares(2019)1688796, dated 14th March 2019. All proposed changes in the mentioned above document have been adapted.

List of contents

1. Introduction

This document establishes the Polish Member State Authority (MSA) Certificate Policy, referred to hereinafter in brief as "the PL-MSA Policy". The PL-MSA Policy will be followed in the operation of the Smart Tachograph.

The goal of the Smart Tachograph is to improve the safety of road transport through a more comprehensive control of drivers' working time and increase the possibility of control. That is to be achieved by replacing the first-generation cards with the second generation one. The new cards are compatible backwards with the previous generation of cards. It applies to cards used by drivers, workshops, companies and control bodies.

A Member State Authority Policy is a document that contains requirements for secure management of keys, certificates and associated equipment used within the Smart Tachograph.

1.1 Overview

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

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

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

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

Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realise this for the second-generation tachograph system.

A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic systems rely on master keys that have to be delivered to the relevant actors. An infrastructure consisting of three layers has been set up. At the European level, the European Root Certification Authority (ERCA) is responsible for the generation and management of root public-private key pairs, with the respective certificates, and symmetric master keys. The ERCA issues certificates to Member State Certification Authorities (MSCAs) and distributes symmetric master keys to the MSCAs. At the national level, the MSCAs are responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment.

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

This document forms the Certificate Policy (CP) for the PKI at the MSCA level in Poland. It lays down the policy at MSCA level for key generation, key management and certificate signing for the Smart Tachograph system. The PL-MSCA shall comply with requirements laid down in the ERCA Certificate Policy (CP) [6].

The PL-MSA Policy applies only the Smart Tachograph System in Poland.

This document follows the framework for CPs described in RFC 3647 [4]. The Symmetric Key Infrastructure policy has been added to this document, preserving the lay-out of RFC 3647. How the PL-MSCA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the PL-MSCA Certification Practice Statement (CPS).

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119 [5].

1.2 Document Name and Identification

This document is named Member State Authority Certificate Policy – Poland. This Certificate Policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the certificates used in the Smart Tachograph system do not contain a reference to this policy.

The current version is 01.02.

PL-MSA Policy is approved by:

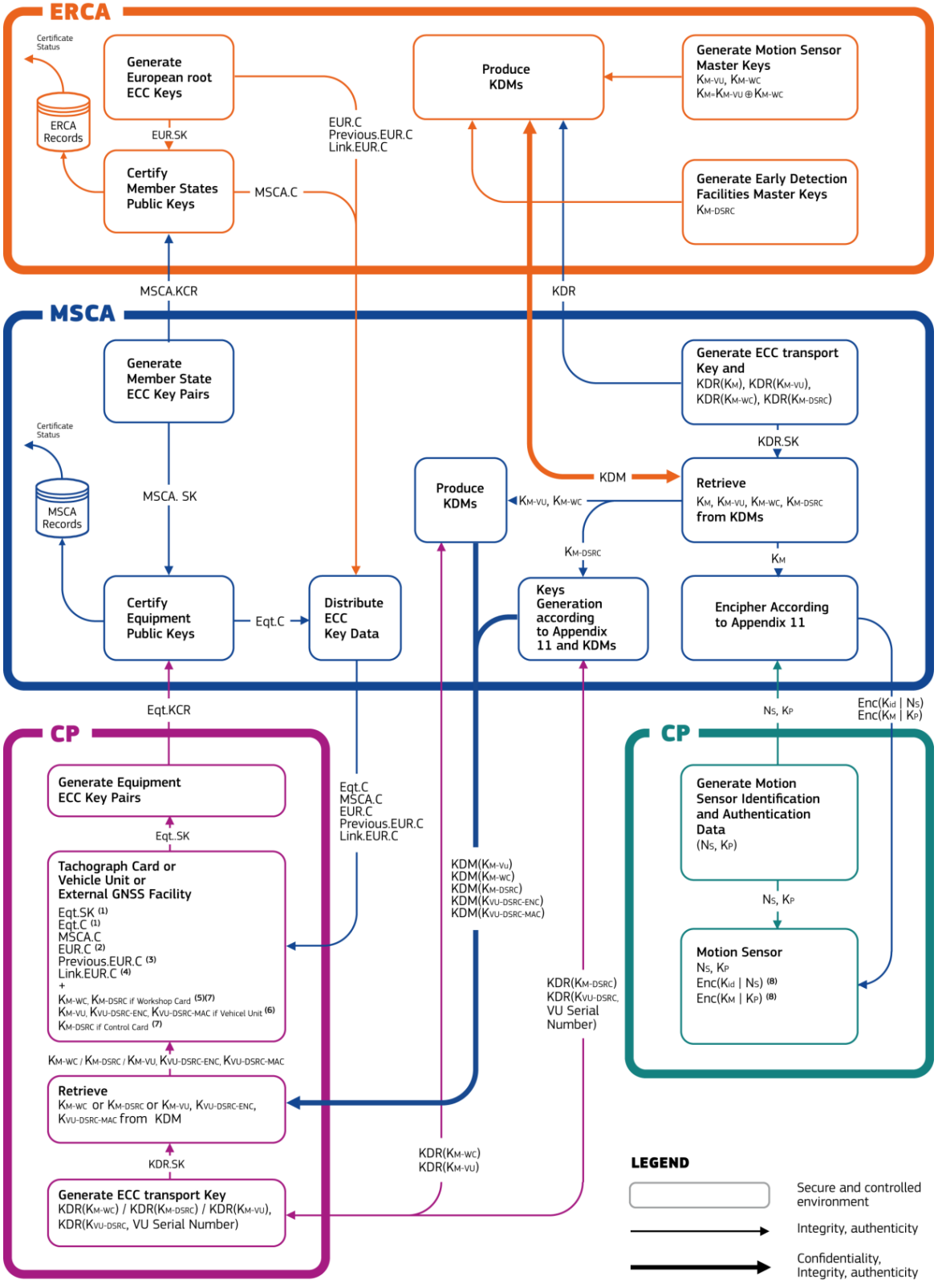
Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
DG JRC - Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

at *Member State Authority Policy - Poland ver. 01.02* under the No D Ares(2019)1715946 - 15/03/2019

After approval the PL-MSA Policy will be publicly available at:
https://www.gov.pl/infrastruktura/polityka-organu-panstwa-czlonkowskiego-polska

1.3 Participants

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



NOTES

1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Figure 1 Participants in the Smart Tachograph PKI and symmetric key infrastructure

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

1.3.1 Certification Authorities

The Member State Certificate Authority in Poland (PL-MSCA) operates as sub-CA under the ERCA. It signs public key certificates for equipment. For this, it operates a registration service, certificate generation service and dissemination service.

The PL-MSCA receives the certificate requests from component personalisers and disseminates the certificates to these parties. There is one type of PL-MSCA key pair and corresponding PL-MSCA certificate for the issuance of Card certificates, called a PL-MSCA_Card key pair. The PL-MSCA may request from the ERCA mentioned type of PL-MSCA certificate, according to its responsibilities regarding the issuance of equipment. The PL-MSCA responsible for the issuance of tachograph card certificates is indicated in this document as an PL-MSCA_Card.

The PL-MSCA is also the entities requesting symmetric master keys from the ERCA, again depending on their responsibilities. The PL-MSCA distributes $K_{M\text{-}WC}$ and K_{DSRC} to card personalisers. The PL-MSCA may also use the Motion Sensor Master Key (K_M) to encrypt motion sensor pairing keys (K_P) on request of a motion sensor manufacturer and derive the motion sensor Identification Key (K_{ID}) from K_M, which it then subsequently uses to encrypt motion sensor serial numbers on request of a motion sensor manufacturer.

1.3.2 Registration Authorities

The registration authority for the PL-MSCA is the PL-CIA. The following functions are carried out by the PL-CIA:

- Application approval registration and processing related to issuing, renewing, replacing of lost, stolen and damaged cards for drivers, companies, workshops and control bodies;
- Card issuing. The PL-CIA shall ensure that issuing of new, replaced and exchanged cards is conducted in compliance with the PL-MSA Policy and that the specified deadlines can be observed;
- Exchange information with others Member States;
- Data storage and status info for registered cards.

1.3.3 Subscribers

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

- Motion Sensors (MoSs);
- Tachograph Cards (TC): four different types of tachograph cards exist: driver cards, company cards, workshop cards and control cards.

This equipment contains cryptographic keys and the TCs also contain certificates as below:

- The MoSs contain a pairing key K_p, the encrypted pairing key and the encrypted MoS serial number.
- The driver cards and workshop cards have two key pairs and corresponding certificates issued by an PL-MSCA_Card, namely
    - a key pair and certificate for mutual authentication, called Card_MA;
    - a key pair and certificate for signing, called Card_Sign.

  The workshop cards also contain $K_{M\text{-}WC}$ and K_{DSRC}.

- The company and control cards have a key pair and corresponding certificate issued by an PL-MSCA_Card for mutual authentication.

  The control cards also contain K_{DSRC}.

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

- A MoS manufacturer
  - generates the MoS serial number;
  - generates the pairing key K_P required to pair a MoS to a VU;
  - requests the encryption of the pairing key with the MoS master key, K_M, and the encryption of the MoS serial number with the identification key K_{ID} from the PL-MSCA;
  - ensures the MoS serial number and pairing key are placed in plain and in encrypted form in the MoS.
- A card personaliser (PL-CP) for driver and workshop cards
  - ensures generation of the two card key pairs, for mutual authentication and signing;
  - performs the certificate application process with the PL-MSCA_Card;
  - performs the application for $K_{M\text{-}WC}$ and K_{DSRC} (workshop cards only);
  - ensures availability in the card of keys and certificates for mutual authentication and signing, MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only).
- A card personaliser (PL-CP) for company and control cards
  - ensures generation of the card key pair for mutual authentication;
  - performs the certificate application process with the PL-MSCA_Card;
  - performs the application of K_{DSRC} (control cards only);
  - ensures availability in the card of keys and certificates for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only).

1.3.4 Relying parties

Parties relying on the PL-MSCA public key certification service are primarily the national authorities tasked with enforcing the rules and regulations regarding driving times and rest periods. Indicated institutions use the PL-MSCA certificates to validate the authenticity of equipment certificates, which in turn are used to validate the authenticity of data downloaded from Vehicle Units and driver cards.

Other relying parties are drivers, companies and workshops.

1.4 Key and Certificate Usage

The PL-MSA and PKI participants (see section 1.3) shall recognise the ERCA public key certificates, provided they are published by the ERCA.

The PL-MSCA shall use its Member State private keys only for:

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

The PL-MSCA shall use the symmetric master keys solely to encrypt motion-sensor related data as specified in Annex IC Appendix 11 [2].

The PL-MSCA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to component personalisers by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11 [2].

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

The Card_MA certificates shall be used for mutual authentication and session key agreement between Card and VU.

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

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

$K_{M\text{-}WC}$ shall be provided to component personalisers for their installation in Workshop Cards.

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

The cards, keys and certificates issued by the PL-MSCA or PL-CP are only for the use within the Smart Tachograph system.

1.5 Policy Administration

1.5.1 National Authority (PL-MSA)

The organization responsible for this policy in Poland will be Ministerstwo Infrastruktury (Ministry of Infrastructure) hereinafter, in conformity with international usage, be referred to as the PL-MSA. The official contact is:

Ministerstwo Infrastruktury (Ministry of Infrastructure)
ul. Chałubińskiego 4/6,
00-928 Warszawa
Poland
Telephone: (+48-22) 630-10-00
https://www.gov.pl/infrastruktura

After approval the PL-MSA Policy will be publicly available at
https://www.gov.pl/infrastruktura/polityka-organu-panstwa-czlonkowskiego-polska

Questions concerning this PL-MSA Policy should be addressed to:
Ministerstwo Infrastruktury (Ministry of Infrastructure)
Departament Transportu Drogowego (Road Transport Department)
ul. Chałubińskiego 4/6,
00-928 Warszawa
Poland
Telephone: (+48-22) 630-12-51
Fax: (+48-22) 630-12-02
e-mail: anna.kowalczyk@mi.gov.pl

The PL-MSA shall:

- Lay down, document and maintain an PL-MSA Policy in conformance with all applicable requirements in the ERCA Certificate Policy [6];
- Appoint the organisation which implements this policy at national level (the PL-MSCA) and provides key certification and key distribution services to the Component Personalizers;
- Ensure that appointed PL-MSCA has the resources required to operate in conformity with this policy;
- Appoint the Card Issuing Authority (the PL-CIA);
- Appoint the Card Personaliser (the PL-CP);
- Determine whether the PL-MSCA CPS complies with this policy;
- Audit the appointed PL-MSCA, PL-CIA and Card Personaliser (PL-CP);
- Audit other component personalisers and the other external service providers, if necessary;
- Approve the Practice Statement (PS) of the PL-MSCA, PS of component personalisers and the PS of other external service providers, if necessary;
- Inform the appointed parties about the PL-MSA Policy;
- Let the PL-MSA Policy be approved by the ERCA;
- Monitor PL-MSCA security. The PL-MSA shall have suitable monitoring procedures and means of enforcement in place to ensure that the certificates generated by the PL-MSCA and the cryptographic keys provided are only, in conformity with their intended purpose that meet the requirements of the PL-MSA Policy;
- Supervise of the quality of processes at Smart Tachograph in Poland;
- Deal with complaints from Component Personalisers and other external service providers about the services provided by the PL-MSCA.

1.5.2 Member State Certification Authority (PL-MSCA)

The authority appointed on the basis of Tachographs Act of 5 July 2018 (Journal of Laws of 2018, item 1480) [8] as the Member State Certification Authority in Poland (be referred to as the PL-MSCA), shall be:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30,
02-871 Warszawa
Poland
Telephone: (+48-22) 332-92-90
Fax: (+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

The appointed PL-MSCA shall:

- Follow the PL-MSA Policy;
- Develop and publish the PL-MSCA CPS that complies with the PL-MSA Policy;
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy in particular to bear the risk of liability damages;
- Check and claim that is able to satisfy the Common Criteria requirements defined in ISO/IEC 15408 [9] regarding the scope of his tasks and services provided;

- Ensure that all requirements on the PL-MSCA, as detailed in PL-MSA Policy, are implemented;
- Conduct functional tests to prove compliance with the PL-MSA Policy;
- Maintain records of its operations as appropriate to demonstrate conformity with this policy and make these records available to the PL-MSA on demand.

The PL-MSCA CPS is owned by the PL-MSCA. The PL-MSCA CPS shall be treated as restricted information. The PL-MSCA shall make the contents of its PS available to the PL-MSA, the PL-CIA and the component personalisers on a need-to-know basis. The PL-MSCA CPS shall be managed, reviewed, and modified following document control procedures.

The PL-MSCA has the responsibility for conformance with the procedures prescribed in the PL-MSA Policy, even when the PL-MSCA's functionality is undertaken by subcontractors. The PL-MSCA is responsible for ensuring that any subcontractor provides all its services consistent with PL-MSCA CPS and the PL-MSA Policy.

1.5.3 Card Issuing Authority (PL-CIA)

The authority appointed on the basis of Tachographs Act of 5 July 2018 (Journal of Laws of 2018, item 1480) [8] as the Card Issuing Authority in Poland (be referred to as the PL-CIA), shall be:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30,
02-871 Warszawa
Poland
Telephone: (+48-22) 332-92-90
Fax:(+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

The appointed PL-CIA shall:

- Follow the PL-MSA Policy;
- Ensure that correct and relevant user information from the application process is passed to the PL-CP;
- Inform the users of the requirements in the PL-MSA Policy related to the use of the Smart Tachograph (or Digital Tachograph System, when necessary);
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy.

The PL-CIA may subcontract parts of its processes to subcontractors. The use of subcontractors in no way diminishes the PL-CIA's overall responsibilities for these processes.

1.5.4 Card Personalization centre (PL-CP)

The Card Personalization centre in Poland (be referred to as the PL-CP) shall be:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30,
02-871 Warszawa
Poland

Telephone: (+48-22) 332-92-90
Fax: (+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

The appointed PL-CP must:

- Follow the PL-MSA Policy;
- Draw up a PS, in which at least the method of implementation of the PL-MSA Policy, Root Policy and legal provisions is explained,
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy, in particular to bear the risk of liability damages;
- Check and claim that is able to satisfy the Common Criteria defined in ISO/IEC 15408 [9] requirements concerning the personalisation of Smart Tachograph cards.
- Check and claim that is able to satisfy the Common Criteria Protection Profile (Digital Tachograph – Tachograph Card) [10] requirements concerning the personalisation of Smart Tachograph cards.

The PL-CP shall ensure that all requirements on it, as detailed in the PL-MSA Policy, are implemented.

The PL-CP has the responsibility for conformance with the requirements prescribed in the PL-MSA Policy, even when the PL-CP functionality is undertaken by subcontractors. The PL-CP may subcontract parts of its processes to subcontractors. The use of subcontractors in no way diminishes the PL-CP's overall responsibilities for these processes.

1.5.5 Other component personalisers

The manufacturer of Motion Sensors (MoSs) in Poland shall be:

BOGART Sp. z o.o.
ul. Nowa Wieś Mała 40,
11-040 Dobre Miasto
Poland
Telephone: (+48-89) 615-17-17
Fax: (+48-89) 615-17-18
e-mail: bogart@bogart.pro
http://www.bogart.pro

Manufacturers of Motion Sensors (MoSs) have to especially ensure that they:

- Observe the requirements, which are relevant to them - i.e. [1], [2], [6], [7], [9] and all other laws and decrees relevant in this regard, especially of this PL-MSA Policy, to the best of their knowledge and according to the respective current technological developments,
    - that the integrated keys and certificates or those to be integrated in the equipment manufactured by them can be used only for proper purposes within the scope of [1], [2], [6], [7], [9],
    - take measures to ensure the confidentiality of the private as well as secret keys during the complete production process and during the total service period of the

equipment;

- Check and claim that is able to satisfy the Common Criteria defined in ISO/IEC 15408 [9] requirements concerning the production process of motion sensors (MoS).
- Check and claim that is able to satisfy the Common Criteria Protection Profile (Digital Tachograph – Motion Sensor) [11] requirements concerning the production process of motion sensors (MoS).
- Provide the PL-MSA with names of all external service providers subcontracted with the responsibility of production and personalisation of their equipment at all required times and make it obligatory for them to adhere to the corresponding requirements. If the manufacturer passes on his tasks to a third party, his rights and duties remain unaffected by the same;
- Draw up a PS, in which at least the method of implementation of the PL-MSA Policy, Root Policy and legal provisions is explained;
- Immediately inform the PL-MSA or one of its authorised agencies about all security relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them;
- Permit the PL-MSA or one of its authorised agencies to evaluate the practical execution of their duties.

1.5.6 Cardholders and users of Motion Sensors (MoSs)

The PL-CIA shall require the cardholder or the organization which represents the cardholder fulfils the obligations arising from the terms and conditions regarding the use of the card.

The organizations or users of motion sensors (MoSs) shall fulfils the obligations arising from the terms and conditions regarding the use of these equipment.

1.6 Definitions and Acronyms

1.6.1 Definitions

Name	Definition
MSA Policy	A named set of rules that indicates the applicability of keys, certificates and equipment to a particular community and/or class of application with common security requirements.
Card	Integrated Circuit equipped card, in the PL-MSA Policy this is equivalent to the use of the terms “IC-Card” and “Smart Card”.
Cardholder	A person or an organization that is a holder and user of a card. Included are drivers, road transport companies, approved workshops and their fitters workers, control bodies and their staff.
Certificate	In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.
Certification Authority	An organization in which certificates are issued by signing user data with a private key to which the certification center signs.
Equipment	In the Smart Tachograph system the following equipment exists: cards, vehicle units

	(VUs), external GNSS facilities (EGFs), motion sensors (MoSs).
Manufacturer/ Equipment manufacturer	Manufacturers of the equipment.
Motion sensor key	A symmetric key used for the motion sensor and the vehicle unit to ensure the mutual recognition.
Practice Statement/ Certification Practice Statement	A statement of the security practices employed in the Smart Tachograph processes. A PS/CPS is comparable to the standard PKI document CPS.
Private key	The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages.
Public key	The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
AES Key	A symmetric key suitable for encrypting / decrypting information in accordance with the AES algorithm.
ECC Keys	A pair of asymmetric keys suitable for encrypting / decrypting information according to the ECC algorithm.
Type of cards	Four types of tachograph cards used in Smart Tachograph: driver card, company card, workshop card, control card.

Table 1 List of definitions

1.6.2 Abbreviations

Acronym	**Definition**
AES	Advanced Encryption Standard
CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Component Personaliser, Card Personalisation Centre
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
DSRC	Dedicated Short Range Communications

EA	European Authority
EC	Elliptic Curve
EC	European Commission
ECC	Elliptic Curve Cryptography, an encryption algorithm based on elliptic curves.
EF	Elementary File. File stored on the tachograph card.
EGF	External GNSS Facility
ERCA	European Root Certification Authority
EU	European Union
EUR.PK	ERCA Public Key
EUR.SK	ERCA Secret Key
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISSO	Information System Security Officer (Inspector of IT Security)
ITSEC	Information Technology Security Evaluation Criteria
JRC	Joint Research Centre
KDM	Key Distribution Message
KDR	Key Distribution Request
KG	Key Generation
$\mathbf{K_{DSRC}}$	DSRC Master Key
$\mathbf{K_{ID}}$	Motion Sensor Identification Key
$\mathbf{K_{M}}$	Motion Sensor Master Key
$\mathbf{K_{M\text{-}VU}}$	Motion Sensor Master Key (Vehicle Unit part)
$\mathbf{K_{M\text{-}WC}}$	Motion Sensor Master Key (Workshop Card part)
$\mathbf{K_{P}}$	Motion Sensor Pairing Key
MA	Mutual Authentication
MoS	Motion Sensor
MS	Member State
MSA	Member State Authority

MSCA	Member State Certification Authority
MSCA.PK	MSCA Public Key
MSCA.SK	MSCA Secret Key
NCP	Normalised Certificate Policy
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
PL-CIA	Polish Card Issuing Authority
PL-CP	Polish Card Personalisation Centre
PL-MSCA	Polish Member State Certification Authority
PL-MSA	Policy Polish Member State Authority Policy
PL-MSA Policy	Polish Member State Authority Policy
PS	Practice Statement
RFC	Request for Comment
SA	System Administrator
SK	Secret Key
TC	Tachograph Card (Driver Card, Company Card, Workshop Card, Control Card)
VU	Vehicle Unit (Smart Tachograph)
WC	Workshop Card

Table 2 List of abbreviations

Further definitions may be found in the documents referenced by this PL-MSA Policy; see the section References towards the end of this document.

2. Publication and Repository Responsibilities

2.1 Repositories

The PL-MSA shall be responsible for the public website https://www.gov.pl/infrastruktura/ , which shall be the repository for PL-MSA documents.

The PL-MSCA shall be responsible for the public website https://www.info-car.pl/infocar/tachograf/ , which shall be the repository for PL-MSCA documents.
The certificates signed by the PL-MSCA shall be maintained in a stand-alone database. The PL-MSCA shall be responsible for storing all issued equipment certificates in a repository. This repository shall not be public.

2.2 Publication of Certification Information

The PL-MSA shall publish the following information on its website - Member State Authority Certification Policy (this document).

The PL-MSCA Certification Practices Statement, the PL-CP Practices Statement and the Practice Statement of component personalisers or other external service providers shall not be public but shall be communicated on request to the relevant parties.

2.3 Time or Frequency of Publication

Information relating to changes in this policy shall be published according to the schedule defined by the change (amendment) procedures laid down in section 9.11 of this document.

Information relating to the changes in the PL-MSA Policy and the PL-MSCA CPS shall be published according to the schedules defined by the change (amendment) procedures laid down in the PL-MSA Policy and the PL-MSCA CPS, respectively.

Changes to the PL-MSCA CPS and the PL-CP PS and the PS of component personalisers or other external service providers shall not be public but shall only be communicated to the relevant parties.

Distribution policies for changes to the PL-MSA Policy and the PL-MSCA CPS shall be determined in the relevant documents.

2.4 Access Controls on Repositories

All information available via the websites mentioned in 2.1 shall have read-only access.

Each of the entities (the PL-MSA, the PL-MSCA, the component personalisers) shall designate staff having rights to write or to modify access to the information to the relevant document.

All information published on the PL-MSA website shall be available via a secure Internet connection.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of name

3.1.1.1 Certificate subject and issuer

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

Entity	**Identifier**	**Construction**
ERCA	Certification Authority Key Identifier (KID)	Nation numeric (‘FD’) Nation alpha (EC) Key serial number Additional info CA identifier (‘01’)
PL-MSCA	Certification Authority Key Identifier (KID)	Nation numeric Nation alpha Key serial number Additional info CA identifier

Table 3 Identifiers for certificate issuers and subjects

3.1.1.2 Key Distribution Requests and Key Distribution Messages

Key Distribution Requests and Key Distribution Messages are identified by the key identifier of the ephemeral public key generated by the PL-MSCA, see section 4.2.1 of the ERCA Certificate Policy [6]. The key identifier value is determined according to section 3.1.1.1 with the following modifications:

- NationNumeric: (‘28’)
- NationAlpha: (PL)
- keySerialNumber: unique for PL-MSCA
- additionalInfo: ‘4B 52’ (“KR”, for Key Request)
- CA identifier: ‘01’.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

PL-MSCA submitting certificate signing requests (CSRs) shall prove possession of the corresponding private key via an internal signature, as specified in section 4.1.1 in the ERCA Certificate Policy [6]. CSRs may also have an outer signature proving the authenticity of the message. The outer signature shall be produced by an already certified private key referenced in the CSR.

3.2.2 Authentication of Organisation Identity

The PL-MSCA shall define a procedure for the registration of a subscriber and authentication of its identity in the PL-MSCA CPS.

3.2.3 Authentication of Individual Identity

The PL-MSCA shall define a procedure for the authentication of individual identities. For the

PL-MSCA, this procedure is available in the PL-MSCA CPS.

3.2.4 Validation of Authority

The PL-MSCA shall define a procedure for the validation of authority in the PL-MSCA CPS.

3.2.5 Criteria for interoperation

The PL-MSCA shall not rely on any external certificate authority for the certificate signing and key distribution services it provides to the Smart Tachograph.

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

3.3 I&A for Re-key Requests

The Identification and Authentication procedures for re-key requests shall be the same as those described in section 3.2.

3.4 I&A for Revocation Requests

If equipment certificate revocation is allowed, the PL-MSCA shall describe in its' CPS how revocation requests for equipment certificates will be validated.

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

The message formats, cryptographic mechanisms and procedures for the application and distribution of PL-MSCA certificates and symmetric master keys between the ERCA and the MSCA (PL-MSCA) are described in detail in sections 4.1 and 4.2 of the ERCA Certificate Policy [6].

In the Certification Practices Statement, the PL-MSCA shall describe in detail the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates and symmetric keys for cards and for the application and distribution of encrypted data for motion sensors between the PL-MSCA and the component personalisers.

4.1 MSCA Public Key Certificate Application and Issuance

4.1.1 Certificate Signing Requests

Certificate signing requests (CSR) can only be submitted by the PL-MSCA recognised by the PL-MSA via a compliance statement. The European Authority is responsible for recognising the PL-MSA.

A CSR shall be in TLV-format. Table 4 shows the CSR encoding, including all tags. For the lengths, the DER encoding rules specified in [19] shall be used. The values are specified in the remainder of this section.

Data Object	**Req**	**Tag**
Authentication	c	'67'
ECC (CV) Certificate	m	'7F 21'
Certificate Body	m	'7F 4E'
Certificate Profile Identifier	m	'5F 29'
Certification Authority Reference	m	'42'
Certificate Holder Authorisation	m	'5F 4C'
Public Key	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'
Certificate Holder Reference	m	'5F 20'
Certificate Effective Date	m	'5F 25'
Certificate Expiry Date	m	'5F 24'
Inner Signature	m	'5F 37'
Certification Authority Reference of Outer Signature Signatory	c	'42'

Outer Signature	c	'5F 37'

Table 4 Certificate signing request format

m: required
c: conditional

The **Authentication** data object shall only be present in case the Outer Signature data object is present.

The version of the profile is identified by the **Certificate Profile Identifier**. Version 1, specified in section 7.1, shall be identified by a value of '00'.

The **Certification Authority Reference** shall be used to inform the ERCA about the ERCA private key that the PL-MSCA expects to be used for signing the certificate. For Certification Authority Reference values see section 3.1. At any given time, the key identifier of the ERCA root key available for signing will be indicated on the ERCA website.

The **Certificate Holder Authorisation** shall be used to identify the type of certificate. It consists of the six most significant bytes of the Tachograph Application ID ('FF 53 4D 52 44 54'), concatenated with the type of equipment for which the certificate is intended (Annex 1C, Appendix 11, CSM_141). For the PL-MSCA certificates, the equipment type shall be set to '0E' (14 decimal).

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

- The **Domain Parameters** data object shall reference the standardised domain parameters to be used with the public key in the certificate. It shall contain one of the object identifiers specified in Table 1 of Appendix 11, Annex 1C.
- The **Public Point** data object shall contain the public point. Elliptic curve public points shall be converted to octet strings as specified in [20]. The uncompressed encoding format shall be used (Annex 1C, Appendix 11, CSM_143).

The **Certificate Holder Reference** is used to identify the public key contained in the request and in the resulting certificate. The Certificate Holder Reference shall be unique. It can be used to reference this public key in equipment-level certificates (Annex 1C, Appendix 11, CSM_144). For Certificate Holder Reference values see section 3.1.

The **Certificate Effective Date** shall indicate the starting date and time of the validity period of the certificate. The **Certificate Expiration Date** shall indicate the end date and time of the validity period. Both data elements shall be of data type `TimeReal`, specified in Appendix 1. Note that the validity period defined by these two data elements shall be 7 years and 1 month (for MSCA_Card certificates).

The certificate body shall be self-signed via an **Inner Signature** that shall be verifiable with the public key contained in the certificate request. The signature shall be created over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, as specified in [14], using the hashing algorithm linked to the size of the public key in the CSR, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain, as specified in [20].

The **Certification Authority Reference** of Outer Signature Signatory shall indicate the PL-MSCA and the respective key that placed the outer signature. It shall only be present in case an outer signature is present. For possible values, see section 3.1.

The **Outer Signature** shall be absent if the PL-MSCA applies for its initial certificate. The outer signature shall be required if the PL-MSCA applies for a successive certificate. In this case, the Certificate Signing Request shall be additionally signed via an outer signature by the MSCA, using (one of) its current valid PL-MSCA private key(s). The outer signature authenticates the request. In case an PL-MSCA is subscribed to receive MSCA_Card certificate, the outer signature shall be placed using a private key linked to a certificate of the same type.

The Outer Signature shall be created over the encoded ECC (CV) Certificate (including the certificate's tag '7F 21' and its length) and the Certification Authority Reference of Outer Signature Signatory field (including the certificate's tag '42' and its length). The signature algorithm shall be ECDSA, as specified in [14], using the hashing algorithm linked to the size of the PL-MSCA key used for signing, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain, as specified in [20].

The PL-MSCA shall calculate and store a hash over the complete CSR, using the hashing algorithm linked to the key size of the signing authority, as specified in Annex 1C, Appendix 11, CSM_50. This hash will be used by the ERCA to verify the authenticity of the CSR.

4.1.2 Certificates

The format of the PL-MSCA public key certificates can be found in section 7.1.

4.1.3 Exchange of Requests and Responses

For transportation of certificate signing requests and certificates, CD-R media should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

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

Each certificate signing request and certificate shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS [7]. Another paper copy of the data shall be held by the ERCA or the PL-MSCA, respectively.

4.1.4 Certificate Acceptance

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

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the certificate complies with Table 8 in section 7.1;
- all certificate field values match the values requested in the CSR;
- the certificate signature can be verified using the ERCA public root key indicated in the CAR field.

If any of these checks fail, the PL-MSCA shall abort the process and contact the ERCA. Certificate rejection is managed according to the certificate revocation procedure (see section 4.1.9).

4.1.5 Key Pair and Certificate Usage

The PL-MSCA shall use any key pair and the corresponding certificate in accordance to section 6.2.

4.1.6 Certificate Renewal

Certificate renewal, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.1.7 Certificate Re-key

Certificate re-key means the signing of a new PL-MSCA certificate, in replacement of an existing certificate. Certificate re-key shall take place either:

- when the PL-MSCA is nearing the end of the usage period of (one of) its private key(s). In this case, re-key shall be done in a timely manner to ensure that the PL-MSCA can continue operations after the end of this period;
- following certificate revocation.

Certificate application, processing, issuance, acceptance and publication is the same as for the initial key pair.

The PL-MSCA key pair(s) may be changed regularly. There are no limits on the number of PL-MSCA certificates that it will sign. The PL-MSCA shall be allowed to request multiple PL-MSCA certificates of the same type, if justified for its activity, with overlapping validity periods.

4.1.8 Certificate Modification

Certificate modification is not allowed.

4.1.9 Certificate Revocation and Suspension

4.1.9.1 Circumstances for certificate revocation

The PL-MSCA certificates shall be revoked in the following circumstances:

- rejection on receipt of a newly issued certificate (see section 4.1.4);
- compromise or suspected compromise of the PL-MSCA private key;
- loss of the PL-MSCA private key;
- the PL-MSCA termination;
- The PL-MSA or the PL-MSCA failure to meet obligations under the Regulation and the ERCA Certificate Policy [6].

4.1.9.2 Who can request revocation

The European Authority is authorised to request revocation of the PL-MSCA certificate.

An PL-MSA is authorised to request revocation for certificates issued to the PL-MSCA pointed in the PL-MSA Policy.

The PL-MSCA is authorised to request revocation for certificates issued to itself.

4.1.9.3 Procedure for revocation request

The certificate revocation procedure is described in the ERCA CPS [7].

4.1.9.4 Special requirements concerning key compromise

Requirements concerning key compromise are described in section 4.5.2.6.

4.1.9.5 Certificate suspension

Certificate suspension is not allowed.

4.1.10 End of Subscription

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

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

4.2 Master Key Application and Distribution

4.2.1 Key Distribution Requests

Key distribution requests (KDR) can only be submitted by PL-MSCA recognised by the PL-MSA via a compliance statement. The European Authority is responsible for recognising the PL-MSA.

A KDR shall be in TLV-format. Table 5 shows the KDR encoding, including all tags. For the lengths, the DER encoding rules specified in [19] shall be used. The values are specified in the remainder of this section.

Data Object	**Req**	**Tag**
Key Distribution Request	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorisation	m	'83'
Key Identifier	m	'84'
Public Key (for ECDH key agreement)	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'

Table 5 Key distribution request format

m: required
c: conditional

The version of the profile is identified by the **Request Profile Identifier**. Version 1, specified in Table 5, shall be identified by a value of '00'.

The **Message Recipient Authorisation** shall be used to identify the symmetric key that is requested. It consists of the concatenation of

- the six most significant bytes of the Tachograph Application ID ('FF 53 4D 52 44 54'),
- the type of key that is requested (see below, 1 byte),
- the version number of the requested master key (1 byte).

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

- '07': KM, motion sensor master key
- '27': KM-WC, motion sensor master key workshop part
- '67': KM-VU, motion sensor master key VU part
- '09': KDSRC, DSRC master key

The **Key Identifier** is a unique 8-byte octet string identifying the public key presented in the KDR for ECDH key exchange, see section 4.2.3 of the ERCA Policy [6]. Its value is determined according to section 3.1.1.2. Since the PL-MSCA shall use a different ephemeral key pair for every key distribution request, the PL-MSCA may use the key identifier to keep track of the ephemeral private key to be used for the decryption of a particular key distribution message, once it arrives at the PL-MSCA. For that reason, the ERCA copies the key identifier in the key distribution message, see Table 6.

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

- The data element Public Point shall contain the public point of the ephemeral PL-MSCA key pair to be used for key agreement. The PL-MSCA shall convert the public point to an octet string as specified in [20], using the uncompressed encoding format.
- The data element Domain Parameters shall contain the object identifier of the set of standardised domain parameters to be used in conjunction with the public point. For more information, see section 4.2.3 of the ERCA Policy [6].

The PL-MSCA shall calculate and store a hash over the complete KDR, using the hashing algorithm linked to the key size of the requested master key, as specified in Annex 1C, Appendix 11, CSM_50. This hash will be used by the ERCA to verify the authenticity of the KDR.

4.2.2 Key Distribution Messages

A key distribution message (KDM) is constructed by the ERCA as shown in Table 6. For the lengths, the DER encoding rules specified in [19] shall be used. The values are specified in the remainder of this section.

Data Object	**Req**	**Tag**
Key Distribution	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorisation	m	'83'
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	m	'84'
Public Point of the ERCA for ECDH key agreement	m	'86'
Encrypted symmetric key	m	'87'
MAC	m	'88'

Table 6 Key distribution message format

m: required
c: conditional

The version of the profile is identified by the **Request Profile Identifier**. Version 1, specified in Table 6, shall be identified by a value of '00'.

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

The **Public Point** shall contain the public point of the ephemeral ERCA key pair used for key agreement, see section 4.2.3 of the ERCA Policy [6]. The public point is converted to an octet string as specified in [20], using the uncompressed encoding format.

The **Encrypted symmetric key** data element shall contain the output of step 4 in section 4.2.3 of the ERCA Policy [6].

The **MAC** data element shall contain the output of step 5 in section 4.2.3 of the ERCA Policy [6].

After successful generation of the key distribution message, the ephemeral private key for key agreement is securely destroyed in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

The key distribution message shall be returned to the PL-MSCA that issued the KDR.

4.2.3 Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages, CD-R media should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

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

Each KDR and KDM shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA CPS [7]. Another paper copy of the data shall be held by the ERCA or the PL-MSCA, respectively.

4.2.4 Master Key Acceptance

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

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with Table 6;
- the message is genuine. The PL-MSCA shall do this by contacting the ERCA as described in the ERCA CPS [7] and verifying that the MAC in the received KDM matches the MAC in the KDM sent by the ERCA;
- the master key type and version in the message matches the requested type and version;
- the public point specified in the message is on the curve specified by the key distribution request sent by the PL-MSCA to the ERCA.

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

If all of these checks succeed, the MSCA shall:

- use the ECKA-DH algorithm to derive a shared point (K_x, K_y), as described in step 3 in section 4.2.3 of the ERCA Policy [6], using the PL-MSCA's ephemeral private key indicated by the key identifier in the message and the ERCA's ephemeral public key. The PL-MSCA shall verify that the shared point is not the infinity point; if it is, the PL-MSCA shall abort the process and contact the ERCA. Else, the PL-MSCA shall form the shared secret K by converting K_x to an octet string as specified in [20] (Conversion between Field Elements and Octet Strings);
- derive the keys KENC and KMAC as described in step 4 in section 4.2.3 of the ERCA Policy [6];
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3 of the ERCA Policy [6]. If this verification fails, the PL-MSCA shall abort the process and contact the ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3 of the ERCA Policy [6]. The PL-MSCA shall verify that the padding of the decrypted key, if any, is correct. If this verification fails, the PL-MSCA shall abort the process and contact the ERCA.

Any operations with the ephemeral private key, with the shared secret and with the derived keys K_{ENC} and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2. After successful recovery of the master key, or when the key distribution process is aborted and no KDM renewal (see section 4.2.6) is initiated, the PL-MSCA shall securely destroy its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

4.2.5 Master Key Usage

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

4.2.6 KDM Renewal

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

KDM renewal may take place only if the original transport media received at the PL-MSCA are damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the PL-MSA and the ERCA. Subsequent to this report, the PL-MSCA may send a KDM renewal request to the ERCA, referring to the original key distribution request. This procedure is described in the ERCA CPS [7] and in the PL-MSCA CPS.

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

4.2.7 Symmetric Key Compromise Notification

Requirements concerning key compromise are described in section 4.5.3.6.

4.2.8 End of Subscription

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

national policy.

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

4.3 Equipment management

According to PL-MSA Policy the equipment in the Smart Tachograph is defined as:

- Tachograph cards hereinafter referred as "cards";
- Motion sensors (MoS).

The equipment is handled or managed by:

- PL-MSA;
- PL-CIA;
- PL-MSCA;
- PL-CP;
- Manufacturers of motion sensors.

4.4 Cards

4.4.1 Quality control

The PL-CP shall ensure that only type approved cards according to [2] are personalized and issued for use.

4.4.2 Application for card

Applicant for a card shall deliver an application form to the PL-CIA in a format which has been determined by the PL-MSA. The application with appropriate attachments shall include the data needed to ensure the correct identification of the applicant.

The PL-CIA shall inform the applicant of the terms and conditions regarding use of the card. This information shall be available in Polish and, where required, also in English.

The applicant shall, by applying for a card and accepting delivery of the card, accept the associated terms and conditions specified in [1], [2], [6] and [7].

4.4.2.1 Agreements

The applicant shall, by making an application for a card and accepting delivery of a card, make an agreement with the PL-CIA stating the following:

- The applicant agrees to the terms and conditions regarding the use and handling of the card specified in [1], [2], [6] and [7];
- The applicant agrees to and certifies that:
    a. from the time of card acceptance and throughout the operational period of the card will not allow illicit access to or use of the card;
    b. at time of application all information given by the applicant to the PL-CIA is true.

4.4.2.2 The PL-CIA terms of approval - Driver card specific

Driver cards shall be issued to individuals subject to the provisions of Regulation (EEC) No 561/2006 [18] and normally resident on the territory of Poland.

The PL-CIA shall make reasonable endeavours to check that the applicant does not have any other valid driver card issued in Poland or in another Member State.

The PL-CIA shall make reasonable endeavours to check that the applicant for a driver card has a

valid driving license of appropriate class (Category B or above).

4.4.3 Validity period of cards

Driver cards shall be valid for no more than **five years** from commencement of validity.

Workshop cards shall be valid for no more than **one year** from commencement of validity.

Company cards shall be valid for no more than **five years** from commencement of validity.

Control cards are valid for no longer than **two years** from commencement of validity.

Temporary cards, non-renewable, are valid for no longer than **185 days** from commencement of validity.

4.4.4 Card renewal - handled by the PL-CIA

4.4.4.1 Card expiry date

Provided application is made for card renewal at least 15 days prior to any card's expiration the PL-CIA will issue a new card before the current card validity expires.

The PL-CIA shall establish routines to remind cardholders of the impending expiration of their cards.

An application for card renewal shall follow the same procedure as an application for a new card.

4.4.4.2 Modification of personal and administrative data

The change of any data crucial for the identification of the cardholder justify the need to exchange an existing card to modify administrative data. PL-CIA shall follow the rules of the renewal if previous card was issued within the same Member State (Poland).

4.4.5 Card exchange - handled by the PL-CIA

4.4.5.1 Change a country of residence

A cardholder who changes country of residence in the territory of the European Union may apply for a driver card or request to have his/her driver card exchanged for a new card under the condition that he/she will proof his/her permanent stay in Poland during at least 185 days in a year.

If the current card was issued by other Member State of the European Union, the cardholder shall show proof of the Polish residence to have the application for exchange accepted.

The PL-CIA shall upon delivery of the new card take possession of the previous card and send it to MSA of origin.

Card exchange due to the change country of residence shall otherwise follow the rules for new card issuing.

4.4.6 Replacement of lost, stolen, damaged and malfunctioning cards - handled by the PL-CIA

4.4.6.1 Replacement of stolen cards

If a card is stolen, its cardholder shall notify this to the authorised control body performing road transport checks or to the local Police in the country where the theft occurred and receive a copy of the notification.

Theft of the card must be reported also to the PL-CIA. The PL-CIA shall register the report of the stolen card.

When a cardholder of stolen card submits an application for the card replacement to the PL-CIA, he or she shall attach to an application the notification from Police.

Stolen card number shall be put on a blacklist available to the appropriate authorities in all Member States.

4.4.6.2 Replacement of the loss of card

The loss of the card must be reported to the PL-CIA. PL-CIA shall register the report of the loss of the card.

A cardholder of lost card submits an application for card replacement to the PL-CIA.

The lost card number shall be put on a blacklist available to authorities in all Member States.

4.4.6.3 Replacement of damaged and malfunctioning card

Damaged and malfunctioning cards shall be delivered to the PL-CIA. If damaged or malfunctioning cards are returned to the PL-CIA their numbers shall be put on a blacklist, visually and electronically cancelled, and subsequently destroyed.

If the card is lost, stolen, damaged or malfunctioning, the cardholder shall apply for a replacement within 7 calendar days.

Provided the cardholder follows the above requirements and the application is considered to be completed correctly and accepted, the PL-CIA shall issue a replacement card with new keys and certificate within 8 working days (Regulation [1]) from receiving a completed application.

The replacement card shall inherit the time of validity from the original card. If the replaced card has less than 2 months remaining valid, the PL-CIA shall renew the card instead of replacing it.

If a workshop card is lost, stolen, damaged or malfunctioning, the PL-CIA shall issue a replacement card with new keys and certificate within 5 working days (Regulation [1]) from receiving a completed application.

4.4.7 Application approval registration

The PL-CIA shall register all applications in a database and shall use this information as input to the certificate generation and card personalization subsystems.

4.4.8 Card personalisation

The PL-CP shall personalize cards both visually and electronically.

4.4.8.1 Visual Personalisation

Cards shall be visually personalized according to Regulation [2] (requirements 227 - 237), specifically:

- A photograph of the applicant must appear on a driver card;
- A photograph of the fitter may appear on a workshop card;
- A photograph of the traffic controller may appear on a control card;
- Company cards are not required to bear the photograph.

4.4.8.2 Applicant data entry

The data on the card should be arranged according to the structure defined in Regulation [2] in Annex 1 C, in Appendix No. 2, chapter 4 "TACHOGRAPH CARD STRUCTURE" - rules

TCS_140 - TCS_179, depending on the type of card.

4.4.8.3 Key entry

The private key shall be inserted in the card without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection. It is intended, where possible, that keys are generated on card or inside HSM.

4.4.8.4 Certificate entry

The card certificate shall be inserted into the card before distribution to the applicant.

4.4.8.5 Quality control

Documented routing shall exist to ensure that the visual information on the card and the electronic information in issued cards matches each other and matches the validated cardholder. The routines shall be described in the PL-CP PS.

4.4.8.6 Cancellation and destruction of non-delivered cards

All cards that are damaged (or for other reasons are not finalized and non-delivered) during personalization shall be destroyed. Accurate records of the destroyed cards shall be kept by the PL-CIA.

4.4.8.7 Cancellation and destruction of returned cards

All cards that are returned to the Pl-CIA except the cards that were issued by other Member State shall be destroyed. Accurate records of the destroyed cards shall be kept by the PL-CIA.

In the event when the card which has been issued in other Member State, is return to the PL-CIA, the PL-CIA shall return the card to the issuing authority.

4.4.9 Card registration and data storage - handled by the PL-CP and the PL- CIA

The PL-CP is responsible for keeping track of which card and card number is given to which applicant.

Necessary data from card applications that are transferred from the PL-CIA to the PL-CP for card personalization are removed from the PL-CP resources after this operation.

The PL-CIA shall maintain up-to-date register of card statuses as well.

The PL-CIA shall keep the register of cards issued, renewed, exchanged, replaced, stolen, lost and defective for a period at least equivalent to their period of administrative validity.

4.4.10 Card distribution to the applicant

The PL-CIA is responsible for the distribution of cards to cardholders. The PL-CIA shall ensure that:

- The personalization shall be scheduled to minimize the time that the personalized card requires safekeeping before delivery to the applicant. Outside of office hours, cards require safekeeping in a controlled environment. Documented routines shall exist for exception handling, including disturbances in the production process, failure of delivery and loss or card damage.
- Personalized cards shall be transferred to the place from where they are to be delivered or distributed to the applicant.

The PL-CP shall always keep personalized cards and non-personalized cards separately.

4.4.11 Authentication codes (PIN)

The PL-CP is responsible for the production of the Personal Identity Number (PIN) corresponding to each workshop card.

4.4.11.1 PIN generation

PIN codes are generated in a secure system and sent safely to the applicants of workshop cards. Their length does not exceed 8 bytes, while in the case of using PIN codes, shorter than 8 bytes, the right side should be complemented with "FF" to full 8 bytes (Regulation [2] in Annex 1 C, in addition to number 1, chapter 2, point 238).

The PIN generation system shall meet the requirements of ITSEC E3, EAL 4 in accordance with Common Criteria defined in ISO/IEC 15408 [9] or equivalent security criteria.

4.4.11.2 PIN distribution

PIN codes and workshop cards shall not be distributed in the same physical envelope.

The PL-CP will distribute PIN codes to the fitters by post in secure way, with acknowledgment of receipt.

The workshop cards will be distributed to the applicants of workshop cards by post, with acknowledgment of receipt.

4.4.12 Card deactivation

If cards are returned to the PL-CIA, this information will be supplied to other Member States on a "need to know" basis.

In the event when the card which has been issued in the other Member State, is returned to the PL-CIA, the PL-CIA shall return the card to that issuing authority with the appropriate information of the reason for returning it.

4.5 Keys management

This chapter contains provisions regarding the management of the keys listed below:

- European Root key (the ERCA public key - EUR.PK);
- Member State keys, i.e. the Member State signing key pair(s) (MS.SK, MS.PK);
- Symmetric master keys, i.e. the Motion Sensor Master Key (K_M), the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC)}$ and the DSRC Master Key (K_{DSRC}).
- The transport keys.

The ERCA public key is used for verifying the PL-MSCA certificates. The ERCA private key is not dealt with here since it never leaves the ERCA.

The Member State keys are the keys used by to sign certificates for tachograph cards.

The symmetric keys are placed in the workshop card and the vehicle unit. The PL-MSCA receives the symmetric keys from the ERCA, stores them and distributes them to PL-CP. Apart from that symmetric keys are used to encrypt information placed in the motion sensor.

The transport keys are used for securely exchanging information between the ERCA and the PL-MSCA and between PL-MSCA and manufacturers of motion sensor.

If the PL-MSCA has need for other cryptographic keys than the above, these shall not be considered part of the Smart Tachograph and is not dealt with in the PL-MSA Policy.

4.5.1 The ERCA public key

The PL-CP and the PL-MSCA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times. The PL-CP shall ensure that EUR.PK with its certificate are inserted in all cards.

4.5.2 The PL-MSCA keys

The keys of the Member State (the PL-MSCA keys) are used to sign certificates issued for

second generation devices. For these devices, the PL-MSCA has the following type of key pairs and related certificates:

- MSCA_Card - used to sign certificates for tachograph cards.

The PL-MSCA public keys are always generated by the PL-MSCA itself and have to be certified by the ERCA.

The Member State keys must not be used for any other purposes than signing tachograph equipment certificates and generating CSR (Certificate Signing Requests).

4.5.2.1 The PL-MSCA keys generation

The PL-MSCA key pair(s) shall be generated and used in a trustworthy dedicated device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

The actual device used, and requirements met shall be stated in the PL-MSCA CPS.

The generation of member state key pair(s) shall occur in a physically secured environment. The PL-MSCA key-pair generation shall require the active participation of at least two separate individuals performing trusted roles.

Keys for the first generation of Digital Tachograph system must be generated using the RSA algorithm and the key length should be 1024 bits.

Keys for the second generation of Digital Tachograph system must be generated using an algorithm based on elliptic curves (ECC), and the key length should be 256 bits or 384 bits or 512/521 bits.

The PL-MSCA shall have at the same time an adequate number of PL-MSCA key pairs, with proper certificates for electronic signatures, to ensure an appropriate level of continuity of the certification process, assuming that the ERCA cannot issue replacement Member State certificates rapidly.

4.5.2.2 The PL-MSCA keys period of validity

The period of validity of the PL-MSCA private key cannot be longer than 2 years from the date of its certificate being issued by the ERCA. After this period, the private key cannot be used.

The appropriate public key is valid in the period of validity of the proper certificate.

Certificates issued by the ERCA are valid:

- MSCA_Card - 7 years and 1 month.

4.5.2.3 The PL-MSCA private keys storage

The PL-MSCA key pair(s) shall be contained in and operated from inside a specific tamper resistant device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or

- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

4.5.2.4 The PL-MSCA private keys backup

The PL-MSCA private keys can be backed up using an archiving procedure that requires the presence of at least two people performing trusted roles in an environment with a high level of physical security. The archiving procedure used shall be stated in the PL-MSCA CPS.

Any copies of PL-MSCA private keys are subject to the same level of security controls as keys in use.

The PL-MSCA private keys can only be imported or exported for backup or recovery purposes.

4.5.2.5 The PL-MSCA keys escrow

The PL-MSCA private signing keys shall not be escrowed.

4.5.2.6 The PL-MSCA keys compromise

A written instruction shall exist, included in the PL-MSCA CPS, which states the measures to be taken by persons responsible for security at the PL-MSCA when the PL-MSCA private keys have become exposed, or is otherwise considered or suspected to be compromised.

In this case, the PL-MSCA must promptly, within no more than 8 hours of detection, inform the PL-MSA and the ERCA, initiate the necessary investigation and implement the actions indicated by the PL-MSA. The results of the investigation should be forwarded to the ERCA.

If the key is compromised or if it cannot be excluded, all private keys as well as their copies should be destroyed such that the private keys cannot be retrieved.

If it is possible, for the destruction of private keys shall be used the dedicated function of the HSM device.

4.5.2.7 The PL-MSCA keys end of life

The PL-MSCA shall implement processes guaranteeing continuous availability of valid, certified by the ERCA pairs of PL-MSCA keys.

Upon termination of use of the PL-MSCA signing key pairs, the public keys shall be archived, and the private keys shall be destroyed such that the private key cannot be retrieved.

If it is possible, for the destruction of private keys shall be used the dedicated function of the HSM device.

4.5.3 Symmetric master keys

Within the Smart Tachograph there are symmetric master keys, which are used for pairing of vehicle units (VUs) and motion sensors (MoS), mutual authentication between VUs and MoS as well as encryption of communication between VUs and MoS.

The PL-MSCA:

- distributes in a safe manner key $K_{M\text{-}WC}$ to PL-CP to place it in workshop cards,
- distributes in a safe manner key K_{DSRC} to PL-CP to place it in workshop and control cards,
- uses the Motion Sensor Master Key (K_M) to encrypt motion sensor pairing keys (K_P) on request of a motion sensor manufacturers,
- derives the Motion Sensor Identification Key (K_{ID}) from K_M, which it then subsequently

uses to encrypt motion sensor serial numbers on request of a motion sensor manufacturers.

The PL-CP:

- shall ensure that the workshop key K_{M-WC} is stored on all issued workshop cards (Annex IC, Appendix 11, Chapter 9, point 9.2 to Regulation [2]),
- shall ensure that the workshop key K_{DSRC} is stored on all issued workshop and control cards (Annex IC, Appendix 11, Chapter 9, point 9.2 to Regulation [2]).

The Symmetric Master Keys must not be used for any other purposes than mentioned in this PL-MSA Policy.

4.5.3.1 Symmetric master keys generation

The symmetric master keys are always generated and distributed by the ERCA. The PL-MSCA shall, as needed, request symmetric master keys K_M, K_{M-WC} from the ERCA (Regulation [6], Regulation [2]).

Keys for the first generation of Digital Tachograph system must be generated using the TDES algorithm and the effective key length should be 112 bits (total length of 128 bits).

Keys for the second generation of Digital Tachograph system must be generated using the AES algorithm and the key length should be 128 bits or 192 bits or 256 bits.

The PL-MCSA shall have at the same time an adequate number of symmetric master keys, to ensure an appropriate level of continuity of the services it provide regard to the validity period of the keys.

4.5.3.2 Symmetric master keys period of validity

The period of validity of the symmetric master keys cannot be longer than 17 years from the date of being issued by the ERCA. After this period, the private key cannot be used.

4.5.3.3 Symmetric master keys storage

The PL-MSCA and the PL-CP protects the symmetric master keys with the use of effective logic and physical protection. The keys shall be contained in and operated from inside a specific tamper resistant device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

4.5.3.4 Symmetric master keys backup

The symmetric master keys can be backed up using an archiving procedure that requires the presence of at least two people performing trusted roles in an environment with a high level of physical security. The archiving procedure used shall be stated in the PL-MSCA CPS.

Any copies of symmetric master keys are subject to the same level of security controls as keys in use.

The export of K_{M-WC} and K_{DSRC} keys (K_VUDSRC_ENC, K_VUDSRC_MAC - DSR-specific VU keys) is only allowed in encrypted form in response to a key distribution request sent by the PL-CP to the PL-MSCA.

Apart from aforementioned cases the symmetric master keys can only be imported or exported for backup or recovery purposes.

The export procedure in both above-mentioned keys requires the presence of at least two persons performing trusted roles.

4.5.3.5 Symmetric master keys escrow

The symmetric master keys shall not be escrowed.

4.5.3.6 Symmetric master keys compromise

A written instruction shall exist, included in the PL-MSCA CPS, which states the measures to be taken by persons responsible for security at the PL-MSCA when the symmetric master keys have become exposed, or is otherwise considered or suspected to be compromised.

In this case, the PL-MSCA must promptly, within no more than 8 hours of detection, inform the PL-MSA and the ERCA, initiate the necessary investigation and implement the actions indicated by the PL-MSA. The results of the investigation should be forwarded to the ERCA.

If the key is compromised or if it cannot be excluded, all symmetric master keys as well as their copies should be destroyed such that keys cannot be retrieved.

If it is possible, for the destruction of symmetric master keys shall be used the dedicated function of the HSM device.

4.5.3.7 Symmetric master keys end of life

The PL-MSCA shall implement processes guaranteeing continuous availability of valid symmetric master keys distributed by the ERCA.

Upon termination of use of the symmetric master keys, the keys shall be destroyed such that the private key cannot be retrieved.

If it is possible, for the destruction of symmetric master keys shall be used the dedicated function of the HSM device.

4.5.4 Transport keys

For secure communication between the ERCA and the PL-MSCA an Elliptic Curve Integrated Encryption Scheme (ECIES) must be used (chapter 4.2.3 of the ERCA Policy [6]).

Transport of keys between the PL-MSCA and the ERCA shall use means, media and protocols defined by the ERCA Root Policy [6]. If physical media is used for key transportation, the PL-MSA will appoint the authorized person to carry the media.

For key certification the PL-MSCA shall use CSR specified in the ERCA Policy [6].

The PL-MSCA shall accept the ERCA Public Key in distribution format described in the ERCA Policy [6].

The PL-MSCA shall request symmetric master key from the ERCA using KDR specified in the ERCA Policy [6]. The PL-MSCA receives the symmetric master key in KDM in accordance with the ERCA Policy [6].

For secure communication between the PL-MSCA and the PL-CP or component personalisers the cryptographic strength of the security mechanisms shall be at least as strong as the strength of the transported keys and encrypted data. Algorithms that are used in those cases are described in the PL-MSCA CPS and appropriate PS.

4.5.4.1 Transport keys generation

The PL-MSCA transport keys shall be generated and used in a trustworthy dedicated device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

The actual device used, and requirements met shall be stated in the PL-MSCA CPS.

4.5.4.2 Transport keys period of validity

The period of validity of the transport keys shall be suitable for the requirements of task that is performed with their use. After this period, the transport keys cannot be used.

4.5.4.3 Transport keys storage

The PL-MSCA protects the transport keys with the use of effective logic and physical protection. The keys shall be contained in and operated from inside a specific tamper resistant device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

4.5.4.4 Transport keys backup

The transport keys can be backed up using an archiving procedure that requires the presence of at least two people performing trusted roles in an environment with a high level of physical security. The archiving procedure used shall be stated in the PL-MSCA CPS.

Any copies of transport keys are subject to the same level of security controls as keys in use.

4.5.4.5 Transport keys escrow

The transport private keys shall not be escrowed.

4.5.4.6 Transport keys compromise

A written instruction shall exist, included in the PL-MSCA CPS, which states the measures to be taken by persons responsible for security at the PL-MSCA when the transport keys have become exposed, or is otherwise considered or suspected to be compromised.

In this case, the PL-MSCA must promptly, within no more than 8 hours of detection, inform an institution for which the transport keys were generated and the PL-MSA and the ERCA, initiate the necessary investigation and implement the actions indicated by the PL-MSA. The results of the investigation should be forwarded to the ERCA.

If the key is compromised or if it cannot be excluded, transport keys as well as their copies should be destroyed such that keys cannot be retrieved.

If it is possible, for the destruction of transport key shall be used the dedicated function of the HSM device.

4.5.4.7 Transport keys end of life

Upon termination of use of the transport keys, the keys shall be destroyed such that the private key cannot be retrieved.

If it is possible, for the destruction of transport key shall be used the dedicated function of the HSM device.

4.5.5 Equipment keys

The equipment's keys are symmetric or asymmetric keys generated or derived from other keys by the device manufacturer or the PL-MSCA or the PL-CP. Asymmetric keys are certified by the PL-MSCA. The table below presents the devices and types of keys that are stored on them.

Device / Key	**Symmetric**	**Asymmetric**
Tachograph card (driver card)	---	Card_MA, Card_Sign
Tachograph card (company card)	---	Card_MA
Tachograph card (control card)	K_{DSRC}	Card_MA
Tachograph card (workshop card)	K_{M-WC}, K_{DSRC}	Card_MA, Card_Sign
Motion sensors (MoS)	K_P	---

Table 7 Equipment keys

In order to preserve backward compatibility, the keys that are required for first generation equipment are also stored in the second generation equipment.

4.5.5.1 General aspects

Card and other equipment initialization, key loading and personalization shall be performed in a physically secure and controlled environment. Entry to this area shall be strictly regulated, controllable at the individual level, and requiring a minimum of two persons to be present to operate the system. A log shall be kept of the entries and the actions in the system.

No sensitive information contained in the key generation systems may leave the system in a way that violates the PL-MSA Policy.

No sensitive information in the card personalization system may leave the system in a way that violates the PL-MSA Policy.

The log of the personalization system shall contain a reference to the order and list the corresponding equipment numbers and certificates. The PL-MSA shall have access to the logs on request.

4.5.5.2 Equipment key generation

Keys may be generated either by the equipment manufacturer, the PL-MSCA or the PL-CP. The entity that performs the key generation shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

Key generation shall be carried out within the equipment (card) or within a trustworthy dedicated device HSM (Hardware Security Module) which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or

- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

If private or symmetric keys generation is carried out within the equipment, this activity shall be covered by the security certification of the equipment, ensuring that publicly specified and appropriate cryptographic key generation algorithms are used. The equipment type used for private or symmetric keys generation shall be stated in suitable documents - CPS or PS.

Symmetric keys are generated using the AES algorithm, and asymmetric keys are generated using the ECC algorithm in accordance with the ERCA Certificate Policy [6].

The generation procedure and storage of the private key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been inserted in the device.

It is the responsibility of the key generation entity to undertake adequate measures to ensure that the public key is unique within its domain before certificate binding takes place. This is presumably done by making sure that the key generation system is random at its nature and therefore the probability of generating non-unique keys is insignificant.

4.5.5.3 Batch key generation

Cryptographic key generation may be performed by batch processing in advance of certificate request, or in direct connection with certificate request.

Batch processing must be performed in stand-alone equipment. Key integrity must be protected until certificate issuing is performed.

4.5.5.4 Equipment key validity

4.5.5.4.1 Keys on cards

Usage of an equipment private key in connection with certificates issued under the PL-MSA Policy shall never exceed the end of validity of the corresponding certificate.

4.5.5.5 Equipment private key protection and storage

The PL-CP and the PL-CIA, and the equipment manufactures shall ensure that the card private key is protected by, and restricted to, a card that has been delivered to the cardholder according to the procedures stated in the PL-MSA Policy.

Copies of the private key are not to be kept anywhere except in the card, unless required during key generation and device personalization.

In no case may the card private key be exposed or stored outside the appropriate card.

4.5.5.6 Equipment private key escrow and archival

Equipment private keys shall be neither escrowed nor archived.

4.5.5.7 Equipment public key archival

All certified public keys shall be archived by the PL-MSCA for the time defined in CPS of PL-MSCA.

4.5.5.8 Equipment keys end of life

Upon termination of use of a card, the public key shall be archived, and the private key shall be destroyed such that the private key cannot be retrieved.

4.6 Equipment certificates management

This section describes the certificate life cycle, containing registration function, certificate

issuing, distribution, use, renewal, revocation (if applicable) and end of life.

The PL-MSCA CPS and the PL-CP PS shall describe the complete procedures of application for certificates of equipment.

4.6.1 Cards

4.6.1.1 Data input

Cardholders do not apply for certificates. Certification issuing is based on the information contained in the application for a card.

The PL-CP shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique. The PL-MSCA shall verify that each CHR is unique within its domain.

4.6.1.2 Card certificates issuing

Driver, workshop, control and company card certificates are only issued after the PL-CIA approval of the application for a card.

4.6.1.3 Card certificate time of validity

The driver card will contain certificates with the following validity periods:

- certificate Card_Ma – 5 years,
- certificate Card_Sign – 5 years + 1 month.

The workshop card will contain certificates with the following validity periods:

- certificate Card_Ma – 1 year,
- certificate Card_Sign – 1 year + 1 month.

The company card will contain certificates with the following validity periods:

- certificate Card_Ma – 5 years.

The control card will contain certificates with the following validity periods:

- certificate Card_Ma – 2 years.

The date of entry into force of the Card_Ma and the Card_Sign certificates must be equal to the begin of the validity of the tachograph card itself, as encoded in the EF_Identification file stored on the card.

The period of validity of certificates cannot be longer than the period of validity of the device.

The date of entry into force of the Card_Ma and Card_Sign certificate pairs of the relevant driver card or workshop card must be the same.

In order to preserve backward compatibility on second generation cards are stored certificates that are required for first generation cards.

4.6.1.4 Card certificate issuing

The PL-MSCA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by the ERCA Certificate Policy [6] and Regulation [2] (Annex 1C, Appendix 11 and 1).

The PL-MSCA and the PL-CP shall therefore validate proof of origin and integrity of the certificate requests. Proof of origin and integrity check mechanisms may not rely on techniques that would cause private keys to be revealed.

4.6.1.5 Card certificate renewal and update

See equipment management section. Since certificates and cards have the same time of validity, they are dealt with together.

4.6.1.6 Dissemination of card certificates information

The PL-CIA shall ensure that information about certificates is made available as necessary to cardholder and relying parties.

4.6.1.7 Card certificate use

The card certificates are only for use within the Smart Tachograph.

4.6.1.8 Card certificate revocation

The PL-MSA Policy makes no provision for the revocation of card certificates, however, the PL-CIA will record the details of cards that have been lost, declared stolen, returned, destroyed or otherwise no longer in use. Information from this record will be made available to relying parties and other Member States on request.

5. Facility, Management, and Operational Control

This section describes the Information Security measures imposed by the PL-MSA Policy.

5.1 Physical Security Controls

The key and certificate generation services shall be housed in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorised access, damage, and interference.
Storage media used to store confidential information, such as hard disks, smart cards and HSMs, shall be protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
Procedures for the disposal of waste shall be implemented in order to avoid unauthorised use, access, or disclosure of confidential data.
An off-site backup facility for the PL-MSCA critical data shall be implemented.

5.1.1 Asset classification and management of the PL-MSCA and component personalisers

The PL-MSCA and component personalisers shall ensure that its assets and information receive an appropriate level of protection. In particular:

- The PL-MSCA and component personalisers shall conduct a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures;
- The PL-MSCA and component personalisers shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

5.1.2 System security controls of the PL-MSCA and component personalisers

The PL-MSCA and component personalisers shall ensure that the systems are secure and correctly operated, with minimal risk of failure. In particular:

- The integrity of systems and information shall be protected against viruses, malicious and unauthorized software;
- Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.

5.1.3 Physical security control of the PL-MSCA and component personalisers

Physical security controls shall be implemented to control access to the PL-MSCA or component personalisers hardware and software. This includes the workstations and other parts of the PL-MSCA and personalization hardware and any external cryptographic hardware module or card.

The PL-MSCA keys for signing certificates shall be kept physically and logically protected as described in the PS.

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

5.1.3.1 Physical access

Access to the PL-MSCA and component personalisers facilities shall be limited to those personnel performing one of roles the described in 5.3. Access may be controlled through the use of an access control list to the room housing the systems.

5.2 Procedural Controls

Procedural controls shall be implemented to ensure secure operations. Separation of duties shall be enforced by implementing multiple-person control for critical tasks.
Access to the systems of PL-MSCA and component personalisers shall be limited to individuals who are properly authorised and, on a need to know basis. In particular, the following access control measures shall be in place:

- Confidential data[1] shall be protected to safeguard data integrity and confidentiality when stored;
- Confidential data shall be protected to safeguard data integrity and confidentiality when exchanged over unsecure networks;
- Confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data.
- The systems of PL-MSCA and component personalisers shall ensure effective user administration and access management;
- The systems of PL-MSCA and component personalisers shall ensure that access to information and application system functions is restricted to authorised staff and provide sufficient computer security controls for the separation of trusted roles. Particularly, the use of system utility programs shall be restricted and tightly controlled. Access shall be restricted, only allowing access to resources as necessary for carrying out the role(s) allocated to a user;
- PL-MSCA and component personalisers personnel shall be identified and authenticated before using the systems;
- PL-MSCA and component personalisers personnel shall be accountable for their activities, which shall be logged in event logs as described in section 5.4;

The PL-MSCA and component personalisers shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. The PL-MSCA and component personalisers shall ensure that the ISMS policies address personnel training, clearances and roles. The PL-MSCA and component personalisers ISMS implementations should conform with the requirements described in ISO/IEC 27001 [14].

The PL-MSCA and component personalisers shall retain responsibility for all aspects of the provision of key certification services, even if some functions are outsourced. Responsibilities of third parties shall be clearly defined by the PL-MSCA and component personalisers and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the PL-MSCA and component personalisers. The PL-MSCA and component personalisers shall retain responsibility for the disclosure of relevant practices of all parties.

The information security infrastructure necessary to manage the security within the PL- MSCA and component personalisers shall be maintained always. Any changes that will impact on the level of security provided shall be approved by the PL-MSA.

5.3 Personnel Controls

The PL-MSCA and the component personalisers, supporting the PL-MSA Policy, should recognize three distinct roles, as outlined below. Trusted roles, on which the security of the

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

operation is dependent, shall be clearly identified and described in detail in the respective PL-MSCA CPS or component personalisers PS. These roles and the associated responsibilities shall be documented in job descriptions. These job descriptions shall be defined from the viewpoint of separation of duties and least privilege. No single person shall be authorised to simultaneously perform more than one of the trusted roles.

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

The roles are:

- Certification Authority Administrator or Personalization Administrator;
- System Administrator;
- IT Security Inspector.

For the PL-MSCA and component personalisers, different individuals shall fill each of the three roles described above and at least one individual shall be appointed per task.

All personnel involved with the PL-MSCA or component personalisers shall be properly trained and shall possess the expert knowledge, experience and qualifications necessary for the services offered and appropriate to the job function.

Personnel training shall be managed according to a training plan described in the PL-MSCA CPS and in the component personaliser PS.

Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the PL-MSCA CPS and in the component personaliser PS.

5.4 Audit Logging Procedures

The security audit procedures in this section are valid for all computers and system components which are related to keys, certificates and equipment issuing processes.

All significant security events in the PL-MSCA and component personaliser software shall be automatically timestamped and recorded in the system log files. These include at least the following:

- Successful and failed attempts to create, update, remove or retrieve status information about accounts of PL-MSCA or component personaliser personnel, or to set or revoke the privileges of an account;
- Successful and failed attempts to set or change an authentication method (e.g. password, biometric, cryptographic certificate) associated to a personal account;
- Successful and failed attempts to log-in and log-out on an account;
- Successful and failed attempts to change the software configuration;
- Software starts and stops;
- Software updates;
- System start-up and shut-down;
- Successful and failed attempts to add or remove an entity from the register of subscribers to which the PL-MSCA currently provide key certification services, or to change any details for any of the subscribers, or to retrieve information from the register;

- Successful and failed attempts to process a certificate signing request or a key distribution request;
- Successful and failed attempts to sign a certificate;
- Successful and failed interactions with the database(s) containing data on (the status of) issued certificates, including connection attempts and read, write and update or removal operations;
- Successful and failed attempts to connect to or disconnect from an HSM;
- Successful and failed attempts to authenticate a user to an HSM;
- Successful and failed attempts to generate or destroy a key pair or a symmetric key inside an HSM;
- Successful and failed attempts to import or export a key to or from an HSM;
- Successful and failed attempts to change the life cycle state of any key pair or symmetric key;
- Successful and failed attempts to use a private key or symmetric key inside an HSM for any purpose.

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

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

5.5 Records Archival

An overview of the events which shall be archived shall be described in internal procedures and shall be in accordance with relevant rules and regulations. The PL-MSCA shall implement appropriate record archival procedures. Procedures shall be in place to ensure integrity, authenticity and confidentiality of the records.

For all archived information, archival periods shall be indefinite.

Measures shall be taken to assure that the record archive is stored in such a way that loss is reasonably excluded.

The events mentioned in section 5.4 shall be inspected periodically for integrity. These inspections shall take place at least annually. Apart from that audit logs shall be consolidated at least annually.

Two copies of the consolidated log shall be made and stored in separate physically secured locations. The audit log shall be stored in a way that makes it possible to examine the log during its retention period.

5.6 Key Changeover

The PL-MSCA shall generate new PL-MSCA key pairs as needed. After the PL-MSCA has generated a new key pair, it shall submit a certificate re-key request.

The PL-MSCA shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in the ERCA Certificate Policy [6].

5.7 Compromise and Disaster Recovery

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

The PL-MSCA and the PL-CP shall maintain a Business Continuity Plan (BCP) detailing how they will maintain their services in the event of an incident that affects normal operations. On detection of an incident, operations shall be suspended until the level of compromise has been established. The PL-MSCA and PL-CP shall furthermore assume that technological progress will render their IT systems obsolete over time and shall define measures to manage obsolescence.

Back-up and recovery procedures for all relevant data shall be described in a Back-up and Recovery Plan.

The following incidents are considered to be disasters:

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

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

c) IT hardware failure.

The PL-MSCA CPS and the PL-CP PS shall describe appropriate disaster recovery mechanisms and state all measures and routines taken to prevent disasters in future. The disaster recovery mechanisms shall not depend on the ERCA response times.

In the event of compromise or theft of an PL-MSCA private key and / or a symmetric master key, the PL-MSCA shall immediately inform the PL-MSA and the ERCA. The PL-MSA shall take appropriate measures within a reasonable time period.

There is effectively no recovery from a loss of the PL-MSCA keys or of the symmetric master keys. Loss shall therefore be prevented using multiple backup copies of the root keys and master keys, subjected to periodic controls.

Protection against IT hardware failures shall be provided by redundancy, i.e. availability of duplicate IT hardware.

5.8 CA or RA Termination

In the event of termination of PL-MSCA activity by the appointed organisation, the PL-MSA shall notify the European Authority and the ERCA of this and optionally inform the European Authority and ERCA about the newly appointed PL-MSCA.
The PL-MSA shall ensure that at least one PL-MSCA is operational in its jurisdiction at all times.

5.8.1 Final termination of the PL-MSCA or PL-CP

Termination of the PL-MSCA or PL-CP takes place when all service associated with a logical entity is terminated permanently. The PL-MSA ensures that the tasks outlined below are carried out:

- Inform all users and parties with whom the PL-MSCA and the PL-CP have agreements or other form of established relations;
- Make publicly available information of its termination at least 6 months prior to termination;
- The PL-MSCA and the PL-CP maintain and provide continuous access to record archives by handing them over to the PL-MSA.

5.8.2 Transfer of the PL-MSCA or the PL-CP responsibility

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

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

The old PL-MSCA shall transfer all root keys to the new PL-MSCA in the manner decided by the PL-MSA.

The old PL-MSCA shall destroy any copies of keys that are not transferred.

6. Technical Security Controls

6.1 Key Pair Generation and Symmetric Key Installation

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

Generation of key pairs and installation of master keys shall be undertaken in a physically secured environment by personnel in trusted roles under (at least) dual person control. The key generation ceremony shall be documented.

The PL-MSCA should have available a Test PL-MSCA system for interoperability test purposes, according to the Regulation. If present, the Test PL-MSCA system shall be a separate system and shall have its own MSCA private keys and symmetric master keys. The Test PL-MSCA system shall be able to request the signing of test certificates and the distribution of symmetric test keys using the processes described in sections 4.1 and 4.2 of the ERCA Certificate Policy [6]. The Test PL-MSCA shall also be able to sign test equipment certificates on request of component personalisers, and to distribute symmetric test keys and encrypted data for motion sensors to component personalisers.

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

The PL-MSCA shall maintain the confidentiality, integrity, and availability of the private keys and the master keys as described in this section.
The private keys shall be generated and used, and/or master keys shall be imported and used in a trustworthy dedicated device which:

- is certified to EAL 4 or higher in accordance with Common Criteria defined in ISO/IEC 15408 [9] using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790 [10] level 3; or
- meets the requirements identified in FIPS PUB 140-2 level 3 [13]; or
- offers an equivalent level of security according to equivalent national or internationally recognised evaluation criteria for IT security.

The most common implementation of such a trustworthy dedicated device for use in a PKI system is a Hardware Security Module (HSM). Other implementations, using different devices, are possible as well, as long as the adopted devices satisfy one of the security requirements listed above. In addition, apart from these security requirements, this MSA Policy contains various functional requirements for the HSMs used in PL-MSCA systems. In case a different device is used in place of an HSM, all such functional requirements must be satisfied as well.

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

The PL-MSCA private keys and symmetric master keys shall only be used within a physically secure environment by personnel in trusted roles under at least dual control. All events of private key usage and symmetric master key usage shall be logged.

The PL-MSCA private keys and the master keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual person control in a physically secured environment.

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

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

Master key import and export is allowed for back-up and recovery purposes. In addition, for the PL-MSCA, export of K_{M-WC} and the VU-specific keys for DSRC is allowed in encrypted form only, and only in response to a valid key distribution request from a component personaliser, by personnel in trusted roles under at least dual person control.

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

At the end of private key usage period of an PL-MSCA private key (as specified in Appendix 11 of Annex IC), the PL-MSCA shall destroy all copies of the key such that it cannot be retrieved. Similarly, at the end of the life cycle of a symmetric master key (as specified in Appendix 11 of Annex IC), the PL-MSCA shall destroy all copies of the key in their possession[2] such that it cannot be retrieved.

All private keys and master keys shall immediately be deactivated (such that they cannot be used) if a compromise is suspected. The PL-MSCA shall investigate the suspected compromise. If a compromise is confirmed or cannot be ruled out, the keys shall be destroyed. Also, all copies of a compromised key shall be destroyed. If a compromise can be ruled out, the keys shall be activated again.

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

6.3 Other Aspects of Key Pair Management

The PL-MSCA public key certificates and hence the public keys shall be archived indefinitely.
The validity periods of all PL-MSCA certificates shall comply with Annex IC Appendix 11 [2].
The private key usage period of PL-MSCA private keys shall be two years. Private key usage periods shall start at the effective date in the corresponding certificate. The PL-MSCA shall not use a private key after the private key usage period is over.

6.4 Activation Data

The PL-MSCA in their CPS shall describe the number of persons in a trusted role that are required in order to activate the system and generate, use or destroy a PL-MSCA private key or to import or use a symmetric master key.

Generating, importing, using or destroying PL-MSCA private keys and/or importing, using or destroying symmetric master keys stored in an HSM shall only be possible if the number of trusted persons specified in the CPS for the specific task have authenticated themselves towards the HSM. Authentication shall take place by using proper means (e.g. passphrases, authentication tokens). The duration of an authentication session shall not be unlimited.

For activation of the PL-MSCA software and the system on which this software is running, user authentication shall take place using proper means (e.g. by a passphrase).

6.5 Computer Security Controls

The PL-MSCA shall specify and approve procedures and specific technical security measures for managing their computer systems. These procedures shall guarantee that the required security level is always being met. The procedures and technical security measures shall be described in internal PL-MSCA documentation. The PL-MSCA computer systems shall be arranged and managed conform these procedures.

[2] Keys K_{M-WC} and K_{DSRC} are also stored on tachograph cards. For instance, the copies of these keys residing on a card will not be destroyed until the moment that specific card is taken out of service.

6.6 Life Cycle Security Controls

The PL-MSCA shall carry out an analysis of security requirements at the design and requirements specifications phase to ensure that security is built into PL-MSCA IT systems.

A separation between Acceptance (or Pre-Production) and Production systems shall be maintained. Change procedures and security management procedures shall guarantee that the required security level is maintained in the Production system.

Change control procedures shall be documented and used for releases, modifications and (emergency) software fixes for any operational software.

6.7 Network Security Controls

The PL-MSCA shall devise and implement their network architecture in such a way that access from the internet to their internal network domain, and from the internal network domain to the Certification Authority systems, can be effectively controlled. In particular, taking the CA signing system completely off-line (‘air gapping’) shall be considered.

6.8 Timestamping

The time and date of an event shall be included in every audit trail entry. The PL-MSCA CPS shall describe how time is synchronised and verified.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

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

Table 8 Certificate profile

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

The options are:

Name	Object Identifier reference	Object identifier value
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
Brainpool P384r1	brainpoolP384r1	1.3.36.3.3.2.8.1.1.11

Brainpool P512r1	brainpoolP512r1	1.3.36.3.3.2.8.1.1.13
NIST P-521	secp521r1	1.3.132.0.35

Table 9 Allowed Standardised Domain Parameters OIDs

7.2 CRL Profile

No CRL shall be published.

7.3 OCSP Profile

No OCSP shall be used.

8. Compliance Audit and Other Assessment

The PL-MSA is responsible for ensuring that audits of the PL-MSCA and the component personalisers and other external service providers, if necessary, take place.

The PL-MSCA and the component personalisers and other external service providers, bears the costs of the audit conducted.

The PL-MSA may consult an external certification or accreditation organization for approval of CPS or PS submitted by the PL-MSCA, the component personalisers or other external service providers in order to increase relying parties' trust in the implementation.

8.1 Frequency or Circumstances of Assessment

A national audit shall establish whether the requirements on the organisation to be audited, as described in the PL-MSA Policy, are being maintained. The PL-MSA shall perform the first audit within 12 months of the start of the operations covered by the PL-MSA Policy. If an audit finds no evidence of non-conformity, the next audit shall be performed within 24 months. If an audit finds evidence of non-conformity, a follow-up audit shall be performed within 12 months to verify that the non-conformities have been solved.

Before the start of the operations covered by the PL-MSA Policy, the PL-MSA shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in the PL-MSA Policy.

8.2 Identity/Qualifications of Assessor

The audit shall be performed by an independent auditor.

Any person selected or proposed to perform an PL-MSCA compliance audit shall first be approved by the Polish Member State Authority.

The names of the auditors which will perform the audits shall be registered. Such auditors shall comply with the following requirements:

- Ethical behaviour: trustworthiness, uniformity, confidentiality regarding their relationship to the organisation to be audited and when handling its information and data;
- Fair presentation – findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit;
- Professional approach – has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in information technologies, PKI and the related technical norms and standards.

The auditor shall possess significant knowledge of, and preferably be accredited for:

- performance of information system security audits;
- PKI and cryptographic technologies;
- the operation of PKI software;
- the relevant European Commission policies and regulations,
- the Polish Member State Authority policy.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The PL-MSA audit shall cover compliance to the PL-MSA Policy, the PL-MSCA CPS and the associated procedures and techniques documented by the organisation to be audited.

The audit shall cover organisations playing a role in the overall equipment issuing process in the country. The audit shall also consider the operations of any subcontractors.

The scope of the compliance audit shall be the implementation of the technical, procedural and personnel practices described in these documents.

Some areas of focus for the audits shall be:

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

By assessment of the audit logs it shall be determined whether weaknesses are present in the security of the systems of the organisation to be audited. Determined (possible) weaknesses shall be mitigated. The assessment and possible weaknesses shall be recorded.

8.5 Actions Taken as a Result of Deficiency

If deficiencies for non–conformity are discovered by the auditor, corrective actions shall be taken immediately by the organisation that was audited. After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.6 Communication of Results

For an audit on national level, the independent auditor shall report the full results of the compliance audit to the organisation that was audited and to the PL-MSA.

The PL-MSA shall send an audit report covering the relevant results of the audit to the ERCA. This shall include at least the number of deviations found and the nature of each deviation.

The audit report shall include the corrective actions with the implementation schedule needed to fulfil requirements in the PL-MSA Policy.

If requested by the ERCA, the PL-MSA shall send the full results of the compliance audit to the ERCA.

9. Other Business and Legal Matters

9.1 Fees

Not applicable.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Business Information

Confidential data shall comprehend at least:

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

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

9.3.2 Information that is not treated as confidential

Certificates are not considered confidential.

Identification information or other information about private persons or enterprises appearing on the cards and in the certificates are not considered confidential unless it is ordered by law or other formal obligations.

9.4 Privacy of Personal Information

The only personal data processed or stored in an PL-MSCA system is those of ERCA, PL-MSCA and component personaliser representatives.

Any personal or corporate information held by the PL-MSCA, the PL-CP or subcontractors that is not appearing on issued cards is considered confidential and shall not be released without the prior consent of the user, nor (where applicable) without prior consent of the user's employer or representative, unless required otherwise by law.

In order to ensure the confidentiality and protection of individuals, the processing of personal data and the transfer of such data shall be limited in accordance with European Union Regulation 2016/679 [16] and Polish Act on the protection of personal data [17].

9.5 Intellectual Property Rights

The PL-MSCA owns the intellectual property rights of the PL-MSCA software.

9.6 Representations and Warranties

The PL-MSCA shall operate according to the ERCA CP and PL-MSA CP and its own CPS.

9.7 Limitations of Liability

The Polish Member State 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 PL-MSCA, and use of certificates beyond the prescribed use defined by this MSA Policy and the PL-MSCA Certification Practice Statement;
- caused by fraudulent or negligent use of certificates and/or certificate status information issued by the PL-MSCA.

The Polish Member State disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon:

- any certificate issued by the PL-MSCA, or its associated public/private key pair, used by a subscriber or relying party;
- any symmetric key distributed by the PL-MSCA, used by a subscriber or relying party.

Issuance of certificates and key distribution messages by the PL-MSCA does not make the Polish Member State or the PL-MSCA an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the Smart Tachograph key management system.

Subscribers and relying parties are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this key management system.

In addition, the PL-MSCA is not an intermediary to transactions between subscribers and relying parties. Claims against the PL-MSCA are limited to showing that it operated in a manner inconsistent with this PL-MSA Policy and the PL-MSCA CPS.

The PL-MSCA and the PL-CP bear the responsibility for proper execution of their tasks, even if some or all the tasks are outsourced to subcontractors. If the PL-MSCA or the PL-CP intends to subcontract to other parties, they shall inform beforehand of such intentions and provide the PL-MSA with all the extra resources necessary for the PL-MSA to meet its obligations.

The PL-MSCA and the PL-CP do not carry liability towards end user, only towards the PL-MSA and the PL-CIA.

Any liability issued towards end users of the Smart Tachograph is the responsibility of the PL-MSA/PL-CIA.

Only certificates signed by the ERCA or the PL-MSCA shall be used within the Smart Tachograph. Other certificates present on cards are in violation of the PL-MSA Policy, and hence neither the PL-MSA, the PL-CIA, the PL-MSCA nor the PL-CP carries any liability in respect to such use.

9.7.1 The PL-MSA and the PL-CIA liability towards the Smart Tachograph users

The PL-MSA and PL-CIA are liable for damages resulting from failures to fulfil these obligations only if they have acted negligently. If the PL-MSA and PL-CIA has acted according to the PL-MSA Policy and any other governing document, it will not be considered to have been negligent.

9.7.2 The PL-MSCA and the PL-CP liability towards the PL-MSA and the PL-CIA

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

9.8 Indemnities

No stipulation.

9.9 Term and Termination

This PL-MSA Policy is valid from the moment it is accepted by the ERCA. It shall be valid until further notice.
The validity of this PL-MSA Policy ends when the PL-MSCA stops operating[3] or when the PL-MSA announces this Policy is no longer valid, e.g. because a new version of the Policy becomes effective.

9.10 Individual Notices and Communications with Participants

Official notices and communications with participants in the Smart Tachograph System in Poland shall be in written form, and subject to the registration procedures for correspondence in force within the Polish Member State.

9.11 Amendments

This Policy is issued under responsibility of the Polish Member State. The PL-MSA, in cooperation with the PL-MSCA, may revise this Policy if it deems this necessary.

It is allowed to make editorial or typographical corrections to this policy without notification to the ERCA and without an increase in version number.

It is allowed to change the contact information in section 1.5 with notification to the ERCA, but without change to the document version number.

For all other changes of this PL-MSA Policy, the procedure for change proposals and approvals shall be as follows:

A. The PL-MSCA, the PL-CIA, the PL-CP and the manufacturers of Motion Sensors (MoSs) from Poland may submit proposals for change to the PL-MSA Policy to the Polish Authority at any time.

B. The Polish Authority shall distribute any proposal to change the PL-MSA Policy to the PL-MSCA, the PL-CIA, the PL-CP and the manufacturers of Motion Sensors (MoSs) from Poland.

C. The Polish Authority shall set an appropriate period for comments. The PL-MSCA, the PL-CIA, the PL-CP and the manufacturers of Motion Sensors (MoSs) from Poland may comment on the proposed changes within the defined period for comments.

D. The Polish Authority shall consider the comments and shall decide which, if any, of the notified changes to implement.

E. When the Polish Authority decide to apply changes in the PL-MSA Policy, should re-submit a new version of the PL-MSA Policy to the ERCA for a new approval.

F. The Polish Authority shall notify the PL-MSCA, the PL-CIA, the PL-CP and the manufacturers of Motion Sensors (MoSs) from Poland about decision made by itself and the European Authority, and shall set an appropriate period for the changes to be implemented.

[3] Section 5.8 covers the situation that the PL-MSCA responsibilities are transferred to a different organization.

G. The Polish Authority shall publish a new version of the PL-MSA Policy including all implemented changes, accompanied by an increase in the version number of the document.

9.11.1 Advance notification

Any item in the PL-MSA Policy may be changed with **90** days' notice.

Changes to items which, in the judgment of the policy responsible organization (the PL- MSA), will not materially impact a substantial number of the users or relying parties using this policy may be changed with **30** days' notice.

9.11.2 Comment period

Impacted users may file comments with the policy administration organization within **15** days of original notice.

9.11.3 Whom to inform

Information about changes in the PL-MSA Policy shall be sent to:

- the ERCA;
- the PL-MSCA, the PL-CIA, the PL-CP,
- the manufacturers of motion sensors.

9.11.4 Period for final change notice

If the proposed change is modified as a result of comments, notice of the modified proposed change shall be given at least **30** days prior to the change taking effect.

9.12 Dispute Resolution Procedures

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

9.13 Governing Law

European regulations and the Polish legislation shall govern the enforceability, construction, interpretation, and validity of this PL-MSA Policy.

Any controversy arising from the interpretation performance of the PL-MSA Policy shall be interpreted according to the law in force in Poland.

9.14 Compliance with Applicable Law

This PL-MSA Policy is in compliance with:

- Regulation (EU) No 165/2014 of the European Parliament and of the Council [1],
- Commission Implementing Regulation (EU) 2016/799 [2],
- Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy version 1.00 [6].

In case discrepancies exist between this PL-MSA Policy and the documents mentioned above, the latter shall prevail.

9.15 Miscellaneous Provisions

No stipulation.

9.16 Other Provisions

No stipulation.

10. References

1. Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014, Official Journal of the European Union L60
2. Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139, including ref. 3
3. Commission Implementing Regulation (EU) 2018/502, amending Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 85
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
6. Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy version 1.0
7. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0
8. Tachographs Act of 5 July 2018 (Journal of Laws of 2018, item 1480, The Parliament of the Polish Republic)
9. Common Criteria. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 – 2014
10. Common Criteria Protection Profile, Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017
11. Common Criteria Protection Profile, Digital Tachograph – Motion Sensor (MS PP), version 1.0, 9 May 2017
12. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15
13. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001
14. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
15. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01
16. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
17. Personal Data Protection Act (Journal of Laws of 2018 item 1000, The Parliament of the Polish Republic)
18. Regulation (EU) No 561/2006 of the European Parliament and of the Council of 15 March 2006, Official Journal of the European Union L102/1
19. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic

Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15

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

11. Conformity to the ERCA Certificate Policy

The requirements for the Polish MSA-Policy are formulated in the European Root Certificate Policy and Symmetric Key Infrastructure Policy [6], especially in point 1.5.3 of that document.

The table below provides the rationale between the requirements as formulated in the ERCA Policy and the requirements in the PL-MSA Policy.

ERCA Policy Version 1.0	**PL-MSA Policy Version 1.01**	**Remarks**
An MSA certificate policy should follow the framework for certificate policies described in RFC 3647 [4]	§1.1	Applies to the entire document.
An MSA certificate policy shall describe the roles and responsibilities involved in the overall equipment issuing process in the country concerned, including at least the MSCA and component personaliser roles. All organisations carrying out one or more of these roles shall be identified.	§1.3, §1.5	
An MSA certificate policy shall require that at least those organisations that generate or manage private or symmetric keys shall be audited regularly. An MSA certificate policy shall describe the scope of each audit, depending on the responsibilities of each organisation, e.g. by pointing out the sections of the MSA certificate policy especially relevant for the given audit.	§8	
An MSA certificate policy shall specify how the MSCA(s) shall register component personalisers who are allowed to send certificate signing requests and key distribution requests.	§1.5.4, §1.5.6, §3.2.2	The component personalisers (PL-CP) are defined in this policy.
An MSA certificate policy shall cover the following processes, where applicable:		
• Issuing of tachograph card keys and certificates;	§4.4, §4.5.5, §4.6.1	
• Issuing of vehicle unit keys and certificates;	---	There is no VU manufactures in Poland. If, at any time in the future, PL-MSA will establish an agreement to provide services to the VU manufactures the PL-MSA Policy will be modified appropriately and re-submitted to the ERCA for approval.
• Issuing of External GNSS facility keys and certificates;	---	There is no External GNSS facilities manufactures in Poland. If, at any time in the future, PL-MSA will establish an agreement to provide services to the External GNSS facilities manufactures the PL-MSA Policy will be modified appropriately and re-submitted to the ERCA for approval.
• Distribution of symmetric keys for cards and VUs and encrypted data for motion sensors to component	§4.5.3	There is no VU manufactures in Poland. Applicable to manufacturers of motion

personalisers;		sensors (MoSs). If, at any time in the future, PL-MSA will establish an agreement to provide services to the VU manufactures the PL-MSA Policy will be modified appropriately and re-submitted to the ERCA for approval.
• Management of the Member State keys.	§4.5.2	
An MSA certificate policy shall require that equipment keys are generated, transported and inserted into the equipment in such a way as to preserve their confidentiality and integrity. For this purpose, the MSA shall:		
• require that any relevant prescription mandated by the Common Criteria security certification of the equipment is met during the complete life cycle of the equipment;	§1.5.2, §1.5.4, §1.5.5, §4.4.8.3, §4.5.2.1, §4.5.2.3, §4.5.3.3, §4.5.4.1, §4.5.4.3, §4.5.5.2, §4.5.5.5, §6.2	
• require that if equipment private key generation is not done on-board the equipment, private key generation takes place within an HSM that complies with the requirements in section 6.2;	§4.4.8.3, §4.5.2.1, §4.5.4.1, §4.5.5.2	
• require that if equipment symmetric key generation is not done on-board the equipment, symmetric key generation takes place within an HSM that complies with the requirements in section 6.2;	§4.5.5.2	
• require that insertion of private keys and symmetric keys into equipment takes place in a physically secured environment;	§4.4.8.3, §4.5.3, §4.5.3.4, §4.5.5.1, §4.5.5.2, §4.5.5.5,	
• require that if equipment is capable of generating private or symmetric keys on-board, key generation shall be covered by the security certification of the equipment, ensuring that publicly specified and appropriate cryptographic key generation algorithms are used.	§4.5.5.2	
An MSA certificate policy shall require that the user of each tachograph card is identified at some stage of the card issuing process.	§4.4.2	
An MSA certificate policy shall require that the ERCA is notified without delay of loss, theft, or potential compromise of any MSCA private key or symmetric master key and shall indicate any follow-up investigation and potential action by the MSA.	§4.5.2.6, §4.5.3.6, §4.5.4.6, §5.7, §6.2	
An MSA certificate policy shall indicate appropriate disaster recovery mechanisms, complying with the requirements in section 5.7.	§5.1, §5.7	
An MSA certificate policy shall require that all subscribers to an MSCA's services shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. The implementation of the ISMS should conform with the requirements described in	§5.2	

ISO 27001 [14].		
An MSA certificate policy shall require that appropriate records of operations involving private or symmetric keys are maintained.	§5.4	
An MSA certificate policy shall include provisions for MSCA termination.	§4.1.10, §5.8, §9.10	
An MSA certificate policy shall include change procedures.	§9.11	
An MSA certificate policy shall require that MSCA shall maintain certificate status information and make this information available to parties having a legitimate interest.	§1.3.2, §4.4.9, §4.6.1.6, §4.6.1.8,	
An MSA certificate policy shall require that the issuance process of tachograph cards ensures that the effective date of the card's certificate(s) is equal to the begin of the validity of the tachograph card itself, as encoded in EF Identification.	§4.6.1.3	
An MSA certificate policy shall forbid key escrow, meaning that MSCA private keys shall not be exported to or stored in any system apart from the systems of the respective MSCA.	§4.5.2.5, §4.5.3.5, §4.5.4.5, §4.5.5.6	

Table 10 The rationale between the requirements in the ERCA Policy and the requirements in the PL-MSA Policy

12. List of Figures

13. List of Tables