MAANTEEAMET

MSA Certificate Policy for the Smart Tachograph in Estonia

Version 1.0
Valid from 02.02.2020

This MSA Certificate Policy is approved by ERCA 13.01.2020.

Table of contents

1. Introduction

This document is the ***MSA Certificate Policy*** for the Smart Tachograph in Estonia.

An ***MSA Certificate Policy*** is required by the ***ERCA Policy*** issued by the ERCA, European Root Certificate Authority.

The current ***ERCA Policy*** is published at https://dtc.jrc.ec.europa.eu/:

- Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy, Version 1.0, June 2018

The second generation of the Digital Tachograph system, called Smart Tachograph, has been introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council. Annex 1C of the Commission Implementing Regulation (EU) 2016/799 lays down the technical requirements for the construction, testing, installation, operation and repair of Smart Tachographs and their components.

1.1 Validity

This ***MSA Certificate Policy*** is valid from the moment it is approved by ERCA. It shall be valid until further notice.

The validity of this ***MSA Certificate Policy*** ends when the MSA stops operating or when the MSA announces this ***MSA Certificate Policy*** is no longer valid, e.g. because a new version of the ***MSA Certificate Policy*** becomes effective.

1.2 Terminology

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.

We mainly use “shall” in this policy.

CP in the ***ERCA Policy*** is abbreviation for Component Personaliser. For Estonia is this the same as Card Personaliser since that is the only component that is produced in charge of MSA in Estonia.

Terminology in this document:

ERCA	European Root Certification Authority	
MSA	Member State Authority	
CIA	Card Issuing Authority	
CP	Card Personaliser (Component Personaliser)	In this ***MSA Certificate Policy*** we have only Card Personaliser

MSCA	Member State Certification Authority	
CPS	Certification Practice Statement	Ref RFC 3647
ERCA Policy	European Root Certificate Policy and Symmetric Key Infrastructure Policy	
Compliance table	Compliance table	A table with all requirements in this policy and how the organisation comply
NA	Not applicable	
VU	Vehicle Unit	The tachograph in a vehicle which are recording drivers' activities, such as driving and rest periods
HSM	Hardware Security Module	A secure computer for storing and handling encryption keys
PKI	Public Key Infrastructure	A method of using encryption keys for encryption, identification and signatures
Incident	Incident and security incident is the same in this document	A security incident is a warning that there may be a threat to tachograph system or that has already occurred

1.3 Exception

There is no CP like tachograph or motion sensor manufacturer connected to Estonian MSA, hence there is no need for regulation in this ***MSA Certificate Policy*** concerning manufacturer.

1.4 Purpose of the MSA Certificate Policy

The purpose of this ***MSA Certificate Policy*** is to address necessary security requirements on the Smart Tachograph in Estonia, i.e. for the issuing and production of tachograph cards. The Smart Tachograph is a control device, used in heavy vehicles, for recording drivers' activities, such as driving and rest periods.

The Smart Tachograph contains personal data and security components that need to be protected. The system is designed so that a security incident in one Member State, such as compromise of certain cryptographic keys, can make serious damage to the entire European system. Therefore, issuing and production of tachograph cards and tachograph equipment must be performed in such a way that necessary security is upheld.

1.5 Which organisation the MSA Certificate Policy concern

This ***MSA Certificate Policy*** concern and put requirements on the following organisations and roles:

Organisation and role	Chapter for information	Chapter with requirements
MSA	1, 2	3, 4, 14, 15
CIA	1, 2, 3	5, 13, 14
CP	1, 2, 3	6, 8, 9 10, 11, 12, 13, 14
MSCA	1, 2, 3	7, 8, 9 10, 11, 12, 13, 14

2. Organisation, roles and responsibilities

The following roles or the Smart Tachograph system are referred to in this ***MSA Certificate Policy***:

ERCA, European Root Certification Authority

CIA, Card Issuing Authority

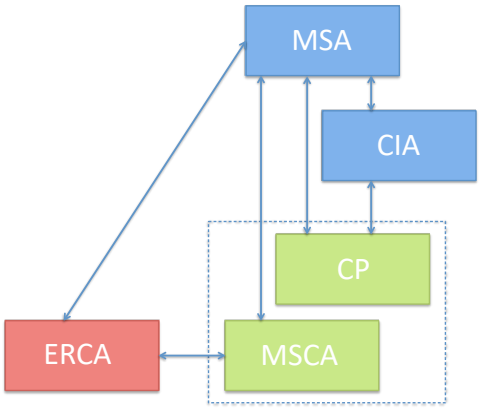
CP, Card Personaliser (Component Personaliser)

MSCA, Member State Certification Authority

With regard to the key management issues addressed by regulation 2016/799 the following two levels of management are described in part B Appendix 11, requirements CSM_53-71:

At 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 Member State 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.) The MSCA is a sub-CA of the ERCA. Overview of roles:



2.1 European roles and responsibilities

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

The contact address of the **European Authority** is:

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

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

The contact address of the **ERCA** is:

European Root Certification Authority
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)

2.2 Entities in charge of operations in Estonia

Responsible for the Smart Tachograph in Estonia, i.e. Member State Authority (**MSA**), is Road Administration (Maanteeamet).

Maanteeamet
Teelise 4
10916, Tallinn
Estonia

https://www.mnt.ee/et

MSA has implemented the following three executive organisations or roles:

- **CIA**
- **CP**
- **MSCA**

CIA:
Responsible for issuing tachograph cards, Card Issuing Authority (**CIA**).

Name and address:

Maanteeamet
Teelise 4
10916 Tallinn
Estonia

https://www.mnt.ee/et

CP:
Responsible for personalisation and distribution of tachograph cards, Card Personaliser (**CP**).

Name and address:

CardPlus Group OY
Koskelontie 23 F
02920 Espoo
Finland

MSCA:
Responsible for certification services, including Member State root key management and motion sensor data encryption, Member State Certification Authority (**MSCA**).

Name and address:

SK ID Solutions AS
Pärnu mnt 141
11314 Tallinn
Estonia

The **CP** and the **MSCA** are outsourced to an external contractor.

3. Member State Authorities, MSA

Each Member State shall set up a Member State Authority (MSA).

3.1 ERCA Policy

The MSA may submit proposals for change to the ***ERCA Policy*** to the European Authority at any time.

3.2 MSA Certificate Policy

Each Member State Authority shall lay down and document an ***MSA Certificate Policy*** in conformance with all applicable requirements in the ***ERCA Policy***.

3.3 MSA Certificate Policy in English to be approved by ERCA

3.3.1 *Approval of the MSA Certificate Policy*

The MSA shall make this ***MSA Certificate Policy*** available to the ERCA.

The ERCA shall review the ***MSA Certificate Policy*** for conformity with the requirements defined in this document. The MSA shall adequately respond to any comment by the ERCA. The objective of the review process is to assure comparable levels of security in each Member State.

The ERCA shall archive the ***MSA Certificate Policy*** and the corresponding review report for reference purposes.

3.3.2 *MSA Certificate Policy to stakeholders*

After approval by the ERCA, the MSA shall make its ***MSA Certificate Policy*** available to all stakeholders, including the MSCA and CP in its country.

3.3.3 *ERCA certification services*

The ERCA shall provide key certification services to the MSCA affiliated to an MSA only if the outcome of the ***MSA Certificate Policy*** review provides sufficient grounds to judge that the requirements in this ***ERCA Policy*** will be met.

Continuation of key certification service from the ERCA to an MSCA shall depend on timely receipt of the MSA audit reports (see section 8.1 in the ***ERCA Policy***) demonstrating that the MSCA is continuing to fulfil its obligations as laid down in the approved ***MSA Certificate Policy***.

3.4 Policy change procedures (MSA)

3.4.1 *Responsibility for change*

MSA is responsible for this policy and the change of this policy.

If the ***ERCA Policy*** is changed this ***MSA Certificate Policy*** may be changed.

3.4.2 *Information about change*

This ***MSA Certificate Policy*** may be changed only in consultation in written form with the roles and organisations concerned, i.e. CIA, CP and MSCA, except for minor editorial changes. A timeframe for when the new ***MSA Certificate Policy*** will come into force shall be stated.

3.4.3 *Forward MSA Certificate Policy to ERCA for approval*

Any changes in this ***MSA Certificate Policy*** must be approved by ERCA. MSA shall forward any updated ***MSA Certificate Policy*** to ERCA for approval.

3.5 Appoint MSCA

MSA shall appoint an organisation which implement the ***MSA Certificate Policy***, it is an MSCA, which provides key certification and key distribution services, to the CP. The MSCA shall act on behalf of the Member State.

3.6 Certificate Revocation

An MSA is authorised to request revocation for certificates issued to the MSCA listed in chapter 2.2 in this ***MSA Certificate Policy***.

3.7 Incident Handling

MSA shall inform ERCA about any incident on expose of keys.

MSA shall do follow-up investigations, identify root causes and corrective actions.

The outcome of the MSA investigations shall be reported to the ERCA.

3.8 Complaints

MSA shall deal with complaints from CIA about the services provided by the CP and MSCA.

MSA shall deal with complaints from CP about the services provided by the MSCA.

MSA shall deal with complaints from CP and MSCA about the services provided by ERCA.

4. Compliance Audit and Approval

4.1 Approval of organisations and roles

MSA may approve CIA before they are allowed to commence operations.

MSA shall approve CP and MSCA before they are allowed to commence operations.

MSA shall approve the CPS of MSCA before MSCA is allowed to commence operations.

MSA shall approve the CPS of CP before CP is allowed to commence operations.

4.1.1 *Approval of the operation (MSCA, CP and CIA)*

Before the start of the operations of the MSCA, CP and CIA the MSA shall carry out a preoperational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in the ***MSA Certificate Policy***, and for the MSCA even the CPS. A Compliance audit shall be performed.

4.1.2 *Approval of MSCA and CP CPS*

The MSA shall ensure whether the MSCA and CP CPS complies with the ***MSA Certificate Policy***.

4.2 Scope and frequency of Compliance audit

MSA may perform a full and formal Compliance audit on the CIA.

MSA shall perform a full and formal Compliance audit on MSCA and CP.

The Compliance audit shall establish whether the requirements on the organisation and role to be audited, as described in the ***MSA Certificate Policy*** and for the MSCA, the CPS, are being maintained.

The MSA shall perform the first Compliance audit within 12 months of the start of the operations of MSCA, CP and CIA.

If a Compliance audit finds no evidence of non-conformity, the next Compliance audit shall be performed within 24 months.

If a Compliance audit finds evidence of non-conformity, a follow-up Compliance audit shall be performed within 12 months to verify that the non-conformities have been solved.

4.3 Identity/Qualifications of Assessor (auditor)

The Compliance audit shall be performed by an independent auditor.

MSA shall appoint and approve the person to perform a Compliance audit.

The names of the auditors which will perform the audits shall be registered by the MSA.

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;
- data protection regulation (privacy);
- PKI and cryptographic technologies;
- the operation of PKI software;
- the relevant European Commission policies and regulations.

4.3.1 *Assessor's Relationship to Assessed Entity*

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

4.4 Topics Covered by Compliance audit

A Compliance audit shall cover compliance to the ***MSA Certificate Policy***. The MSCA CPS and the associated procedures and techniques documented by the organisation shall be audited.

The scope of the Compliance audit shall be the implementation of the technical, procedural and personnel practices described in MSCA CPS and other MSCA and CP documentation, all referenced in a Compliance table.

Some areas of focus for the Compliance audits shall be:

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

The Compliance audit shall assess the system logs/audit logs to be determined whether weaknesses are present in the security of the systems of the organisation to be audited.

Determined (possible) weaknesses shall be mitigated by the Assessed role and organisation.

The Compliance audit including the assessment and possible weaknesses shall be recorded and documented in the audit report.

4.5 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 and role that was audited (MSCA, CP and CIA).

The corrective actions shall be reported to the auditor who will approve them.

After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

4.6 Communication of Results

The auditor shall report the full results of the Compliance audit to the organisation that was audited (MSCA, CP and CIA) and to the MSA.

4.6.1 *Audit report to ERCA*

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

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

5. Issuing of Tachograph cards (CIA)

This chapter contains requirements on CIA.

5.1 Compliance table

The CIA shall have a Compliance table that describe how CIA comply with the requirements in this ***MSA Certificate Policy***, with reference to steering documents.

5.2 Complaints to MSA

Complaints from CIA about the services provided by the CP and MSCA shall be addressed to the MSA to be dealt with.

5.3 Compliance audit CIA

CIA may be audited, see chapter 4.

CIA shall make the premises, personnel, system and documentation etc. available for the Compliance audit.

If deficiencies for non–conformity are discovered by the auditor, CIA shall immediately take corrective actions.

The corrective actions shall be reported to the auditor who will approve them.

5.4 Issuing of Tachograph cards

The CIA shall ensure that users of Driver cards are personally identified on application of a Tachograph card.

The CIA shall identify the responsible party (owner) of all other Tachograph cards. This has to be done by the CIA in the application process.

The CIA shall ensure that the effective date of the card's certificate(s) is equal to the beginning of the validity of the tachograph card itself, as encoded in EF Identification

CIA shall control that the responsible party for the tachograph card has registered the card as stolen or lost before they reissued a tachograph card.

CIA shall make sure that a reissued Tachograph card is not delivered before the existing Tachograph card is delivered to CIA or is registered as stolen or lost.

5.5 Information to the tachograph card applicant

The CIA shall inform the applicant about rules and regulation for ownership and use of Smart Tachograph cards.

5.6 Handling of tachograph cards

CIA shall handle and store tachograph cards in a secure way.

CIA shall have routines for handling of tachograph cards with functional errors.

5.7 Maculation of tachograph cards

CIA shall maculate tachograph cards in a secure way, electronically and physical. The CIA shall destruct tachograph cards in a way that they are sure that the certificate or keys cannot be compromised. (For example, to cut the chip in two.)

5.8 Communication with CP

CIA shall make sure that CP has received the applications of tachograph cards and give a receipt of received tachograph cards.

If the CIA recognises that any tachograph card is lost in transportation between CP and CIA, the CIA shall report card loss, as an incident, to CP. CP will produce a new tachograph card.

5.9 Communication with other parties

The CIA shall make tachograph card information available for relevant parties such as:

- Control authorities (in Estonia and other Member States)
- MSA
- The EU-Commission (ERCA)

CIA shall make necessary information about tachograph cards available for other countries (TACHOnet etc.).

CIA shall make sure integrity and confidentiality of information about tachograph cards that is given to other parties.

CIA shall send delivered (found, withdrawn) driver cards to the CIA that issued the card.

5.10 Logging, data storing and archiving

CIA shall store all necessary data about tachograph cards and minimum

- Tachograph card number, connection to responsible party and status

CIA shall archive information about tachograph cards indefinite.

CIA shall make sure that the archived information is available, and the integrity and confidentiality is kept.

CIA shall make the information available for MSA on request.

5.11 General Security Requirements

The CIA shall have necessary written documentation and routines to secure that the work is performed in compliance with the ***MSA Certificate Policy***.

The CIA shall have defined roles and responsibility. All personnel shall have adequate competence and training. No person may have more than one security critical role with conflict of interests.

Critical systems and data shall be protected from unauthorised access by means of access control systems and with fine granular traceability (to the individual level).

System access and use of critical systems shall be controlled by collecting and analysing relevant information. This information shall be protected against tampering. This information shall be given MSA on request.

6. Card Personaliser (CP)

6.1 Compliance table

The CP shall have a Compliance table that for describe how CP comply with the requirements in this ***MSA Certificate Policy***, with reference to steering documents.

6.2 Responsibility

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

- A card personaliser for driver and workshop cards
  - ensures generation of the two card key pairs, for mutual authentication and signing;
  - performs the certificate application process with the MSCA_Card;
  - performs the application for KM-WC and KDSRC (workshop cards only);
  - ensures availability in the card of keys and certificates for mutual authentication and signing, MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only).
- A card personaliser for company and control cards
  - ensures generation of the card key pair for mutual authentication;
  - performs the certificate application process with the MSCA_Card;
  - performs the application of KDSRC (control cards only);
  - ensures availability in the card of keys and certificates for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only).

6.3 CP Certification Practice Statement

The CP shall document its implementation of the ***MSA Certificate Policy*** in a CPS (Certification Practice Statement). The CP shall make its CPS available to the MSA.

Upon request, the CP shall also make its CPS available to the ERCA.

6.4 Complaints to MSA

Complaints from CP about the services provided by the MSCA shall be addressed to the MSA to be dealt with.

6.5 Compliance audit CP

CP shall be audited, see chapter 4.

CP shall make the premises, personnel, system and documentation etc. available for the Compliance audit.

If deficiencies for non–conformity are discovered by the auditor, corrective actions shall be taken immediately by the organisation that was audited.

The corrective actions shall be reported to the auditor who will approve them.

6.6 Confidentiality of Business Information

CP shall comprehend at least the following as Confidential data:

- Private keys;
- Symmetric master keys.

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

6.7 Card loss

If the CP recognises that a tachograph card is lost before it is sent to Estonia, the tachograph card should be reported as lost to CIA and MSCA and CP will produce a new card.

6.8 Maculation of tachograph cards

CP shall maculate tachograph cards in a secure way, electronically and physical. The CP shall destruct card in a way that they are sure that the certificate or keys cannot be compromised. (For example, to cut the chip in two.)

7. Member State Certification Authority, MSCA

MSCA shall operate according to ERCA CP, the ***MSA Certificate Policy*** and their own CPS.

7.1 Compliance table

The MSCA shall have a Compliance table that for describe how MSCA comply with the requirements in this ***MSA Certificate Policy***, with reference to steering documents.

The Compliance table shall exist is in addition to the CPS.

7.2 MSCA Certification Practice Statement

The MSCA shall document its implementation of the ***MSA Certificate Policy*** in a CPS (Certification Practice Statement). The MSCA shall make its CPS available to the MSA.

The MSCA shall make its CPS available to its subscribers on a need-to-know basis, i.e. the CP.

Upon request, the MSCA shall also make its CPS available to the ERCA.

7.3 Records of operation

The MSCA shall maintain record of its operations as appropriate to demonstrate conformity with the ***MSA Certificate Policy*** and **CPS.**

MSCA shall make these records available to the MSA and/or the ERCA on demand.

7.4 Compliance audit MSCA

MSCA shall be audited, see chapter 4.

MSCA shall make the premises, personnel, system and documentation etc. available for the Compliance audit.

If deficiencies for non–conformity are discovered by the auditor, corrective actions shall be taken immediately by the organisation that was audited.

The corrective actions shall be reported to the auditor who will approve them.

7.5 Publication and Repository Responsibilities

7.5.1 *Certificate repositories*

An MSCA shall be responsible for storing all issued equipment certificates (card certificate) in a repository.

This repository shall not be public.

7.5.2 *Certificate status*

The MSCA shall make certificate information upon request available for relevant parties such as:

- Control authorities (in Estonia and other Member States)
- MSA

- The EU-Commission (ERCA)

7.6 Confidentiality of Business Information

MSCA shall comprehend at least the following as Confidential data:

- Private keys;
- Symmetric master keys;
- Audit logs/System log files; i.e all significant security events in the MSCA software shall be automatically time-stamped and recorded in the system log files;
- Detailed documentation regarding the PKI management.

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

7.7 Revocation of Certificates and Keys

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

7.8 General Security Requirements

MSCA private keys shall not be exported to or stored in any system apart from the systems of the MSCA.

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

Equipment keys shall be generated, transported and inserted into the equipment in such a way as to preserve their confidentiality and integrity. For this purpose, it is required that

- any relevant prescription mandated by the Common Criteria security certification of the equipment is met during the complete life cycle of the equipment;
- 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 of the ERCA Policy;
- 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 of the ERCA Policy;
- insertion of private keys and symmetric keys into equipment takes place in a physically secured environment;
- 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.

7.9 Use of Certificates

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

KM-WC shall be provided to CP for their installation in Workshop Cards.

(KDSRC shall be used by an MSCA to derive VU specific keys to secure the DSRC communication.)

KDSRC 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.

8. Identification and Authentication (ERCA chapter 3)

The MSCA shall follow the requirements in the ***ERCA Policy*** chapter 3.

8.1 Authentication of Organisation Identity

The MSCA shall define a procedure for the authentication of organisation identities in their CPS.

8.2 Authentication of Individual Identity

The MSCA shall define a procedure for the authentication of individual identities in their CPS.

9. Requirements on certification and keys (ERCA chapter 4)

The requirements in chapter 4 in the ***ERCA Policy*** shall be followed by CP and MSCA.

10. Facility, Management, and Operational Controls (ERCA chapter 5)

The requirements in chapter 5 in the ***ERCA Policy*** shall be followed by CP and MSCA.

10.1 CP and MSCA

10.1.1 *Risk management*

CP and MSCA shall have written procedures for risk management. A risk analysis shall be performed and updated minimum every 12 months or before major changes are done.

10.1.2 *Change procedures*

CP and MSCA shall have written change procedures. The change procedures shall include the communication with the MSA.

10.1.3 *Data storage*

MSCA shall store personalisation data as long as it is needed for the personalisation process and until necessary data is transferred to CP.

MSCA shall delete certification request when the personalisation process is ended, and CP has received necessary data.

The only personal data processed or stored in an MSCA system is those of ERCA, MSCA and CP representatives.

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

10.1.4 *Archiving*

MSCA and CP shall identify which data to archived and how long time. MSCA and CP shall give the archived data to MSA upon request.

11. Technical Security Controls (ERCA chapter 6)

The requirements in chapter 6 in the ERCA Policy shall be followed by CP and MSCA.

12. Certificate, CRL, and OCSP Profiles (ERCA chapter 7)

The requirements in chapter 7 in the ERCA Policy shall be followed by CP and MSCA.

13. Business continuity planning and incident handling (CP and MSCA)

13.1 Business continuity plan

The MSCA and the CP shall, to prevent and minimise the effects of incidents and disasters, have a well-documented and established business continuity plan. The plan shall include:

- key compromise
- loss of data (theft, fire, hardware- or software errors, etc)
- other types of system errors.

13.2 Key Compromising

Specifically, the CP and the MSCA shall describe what measures shall be taken in case a MSCA private key or a motion sensor key is compromised or suspected to be compromised.

As a minimum, the CP and the MSCA shall in such cases inform the MSA and the ERCA without delay.

If any card keys are compromised and detected before the card is sent to the user, the card should not be sent to the user.

13.2.1 *Special requirements concerning key compromise*

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

If the MSCA private key is compromised, or suspected to be compromised, the MSCA shall notify the incident to the ERCA and to the MSA without unnecessary delay and at least within **8 hours** of detection.

In their incident report (notification), the MSCA shall indicate the circumstances under which the compromise occurred.

The outcome of the MSCA investigation of the incident shall be reported to the MSA and the ERCA.

13.3 Incident handling

13.3.1 *Incident handling*

All detected incidents (security incidents) shall be

- recorded
- communicated
- classified
- investigated and analysed
- reported
- necessary corrective and preventive action taken

CIA may have a process for incident (security incident) handling, from reporting to recording of incidents to corrective and counter actions.

CP and MSCA shall use written incident reports.

CP and MSCA shall have a written security incident handling procedure.

CP and MSCA shall have a record (list) of all security incidents (incident reports).

Incident handling:
The MCSA and CP shall allocate resources, and appointed responsible, for each incident to perform investigation and analysis, and then, present identified root causes and implement **corrective** actions.

Preventing incidents:
The MSA, MCSA and CP shall record statistics of incidents and have a yearly, documented, management meeting analysing the statistics. The outcome of the meeting should be a list of actions to be implemented to **prevent** future incidents.

14. Termination of the organisations and roles

14.1 MSA

MSA shall ensure that at least one MSCA is operational at all time (Ref ***ERCA Policy*** 5.8).

If the CIA, CP or MSCA are to be terminated, the MSA is responsible for informing the relevant parties and ERCA.

MSA is responsible that CIA, CP and MSCA delivers relevant data and information concerning the Smart Tachograph for archiving or maculates data and information. MSA is responsible of decision on archiving or maculation.

MSA is responsible for the decision to submit a certificate revocation request for any valid MSCA certificates, or to allow all MSCA certificates to expire. (Ref ***ERCA Policy*** 4.1.1.12).

MSA is responsible for that all private MS root keys are maculated, and MS public root keys are archived.

14.2 CIA

The CIA shall cooperate with MSA and other parties to make the termination correct and effective.

14.3 MSCA and CP

The MSCA and CP shall cooperate with MSA and other parties to make the termination correct and effective.

The MSCA and CP shall follow the requirements that MSA will put on the termination and their decision on which data and information to transfer to MSA or to maculate.

The MSCA shall securely destroy all copies of any symmetric master key in its possession. (Ref ***ERCA Policy*** 4.2.12)

15. Change history

Date	Version	Comment	Person
09.01.2019	0.1	For review by MSA	Tiit Poll
17.01.2019	0.1	Reviewed by MSCA	Kai Tooming
17.01.2019	0.2	For second review by MSA	Tiit Poll
18.01.2019	0.2	Reviewed by MSCA	Kai Tooming
29.01.2019	0.2	Final version submitted to ERCA	Tiit Poll
01.03.2019	0.2	ERCA approval received	Michel Chiaramello
10.12.2019	0.3	CP and MSCA contacts updated by MSA	Tiit Poll
12.12.2019	1.0	Final version submitted to ERCA	Tiit Poll
13.01.2020	1.0	ERCA approval received	Michel Chiaramello