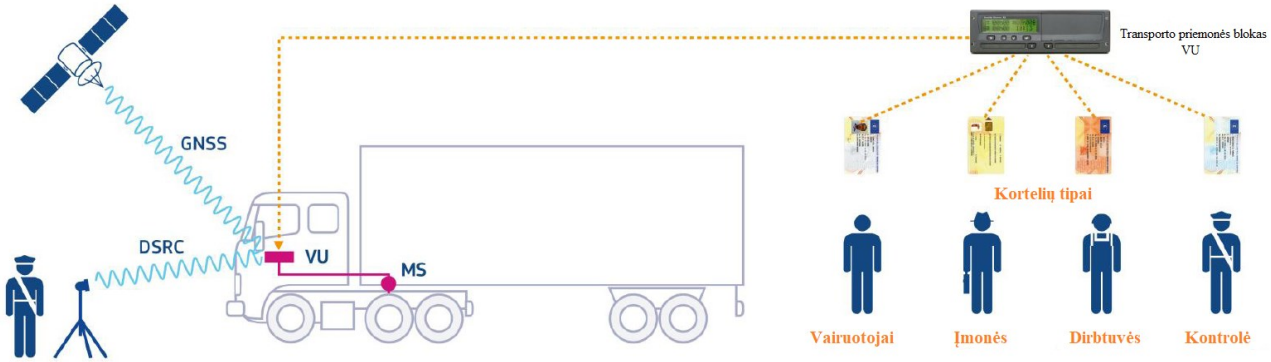
CERTIFICATION POLICY OF LITHUANIA
FOR THE SMART TACHOGRAPHS SYSTEM

According to Regulation (EU) No 165/2014 of the European Parliament and of the Council, as last amended by Regulation (EU) 2020/1054 of the European Parliament and of the Council of 15 July 2020



Metrics

Issued by	Lithuanian transport safety administration Švitrigailos g. 42, LT-03209 Vilnius
Information	Phone: +370 5 278 5602 Fax +370 5 213 2270 e-mail: ltsa@ltsa.lrv.lt
Authors	Virginijus Čiškauskas
Version	Version 1.2
Date	2023-12-21

History of the versions of the Project of Certification Policy of Lithuania

0.1 version	2019-05-09	Draft
0.2 version	2019-05-28	Changes after 1st review of ERCA
0.3 version	2019-05-29	Version sent to ERCA for final approved by ERCA
0.4 version	2019-06-10	Changes after 2nd review of ERCA
0.4 version	2019-06-11	Approved by ERCA, Ares(2019)3717619 – 11/06/2019
1.0 version	2019-07-25	Official version for production
1.1 version	2023-10-16	Changes in points 1.5.3, 9 and 9.11. Editorial changes.
1.2 version	2023-12-21	Editorial changes to items: 1.5.3, 4.2.1, 4.2.2, 4.2.2.1, 4.2.2.2, 4.2.5, 4.2.6, 4.2.8-4.2.13, 4.7, 6.1.1.3

TABLE OF CONTENTS

1. Introduction

1.1. Overview

This document describes the certification policy of the Republic of Lithuania applicable to the smart tachograph system.
The second generation digital tachograph system, known as the advanced tachograph, was introduced by Regulation (EU) No 165/2014 of the European Parliament and of the Council. The requirements for the construction, testing, installation, use and repair of tachographs and their components are set out in Commission Implementing Regulation (EU) 2016/799 (hereinafter referred to as the Regulation).
Public Key Infrastructure (PKI) is designed to support public key systems, and symmetric cryptographic systems are based on key keys to be delivered to stakeholders. Created three-layer infrastructure. At European level, the European Root Certification Authority (hereinafter referred to as ERCA) is responsible for the creation and management of root and public key pairs, relevant certificates and symmetric key keys.
The structure of this document is in line with the Certificate Policy and Certification Practice Guidelines RFC 3647.
The digital tachograph (first generation system) and the smart tachograph (second generation system) are two different systems that must be used in parallel and independently. For this reason, in order to avoid problems, it is necessary to maintain separate MSA policies when the time comes to terminate the digital tachograph and the corresponding ERCA (Gen 1) policy, therefore the Lithuanian National Certification Policy for the Digital Tachograph System remains valid.

1.2. Document Name and Identification

The title of the document is the policy of certification of the Lithuanian smart tachograph system (hereinafter – Policy).
This document does not apply to ASN.1 coding rule. Such an identifier is unnecessary because the certificates used in the smart tachograph system do not refer to the Policy.

1.3. PKI Participants

The participants of the PKI and symmetric key infrastructure of the smart tachograph are described and presented in Figure 1.

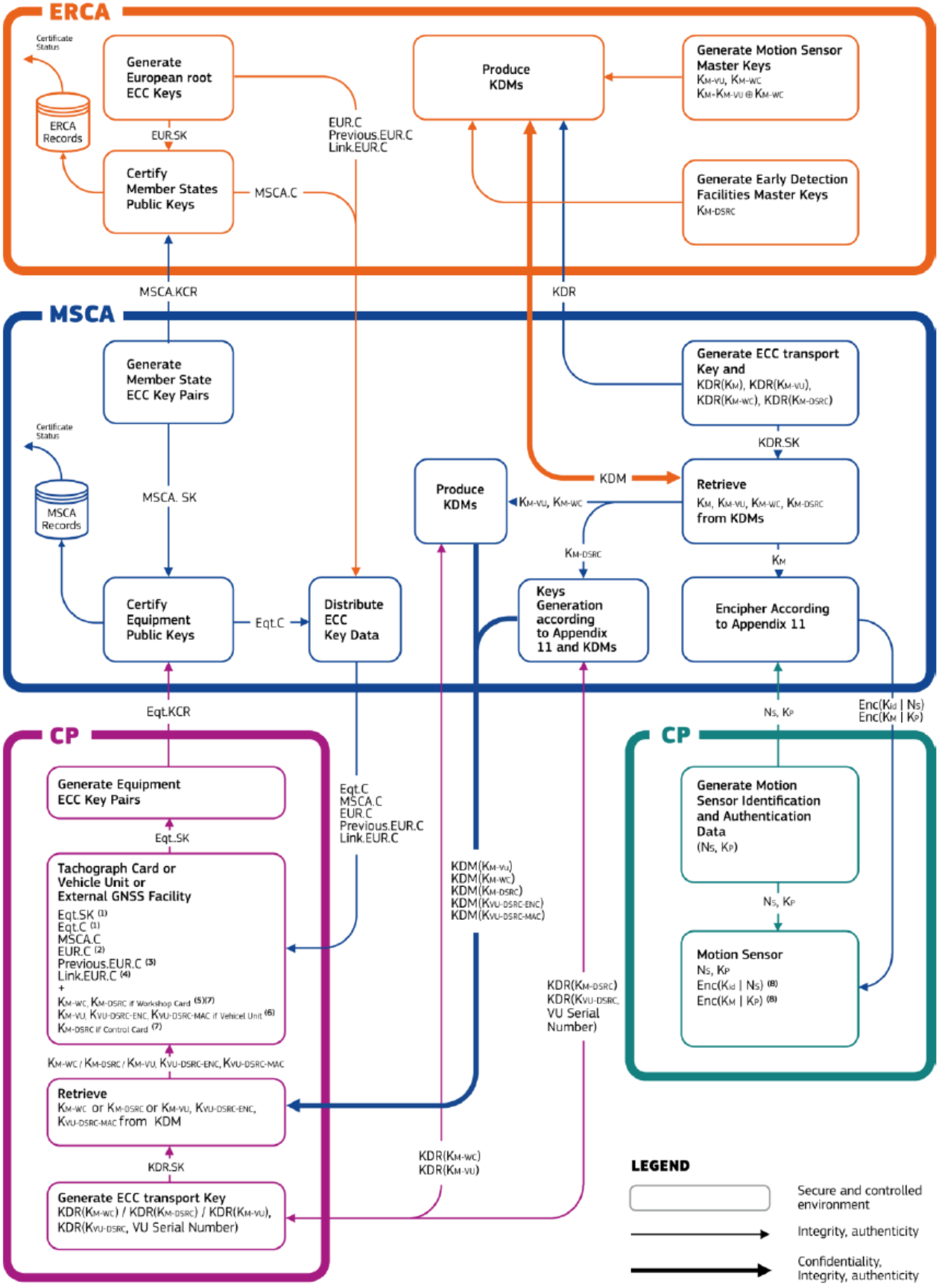


Figure 1 Smart Tachograph PKI and Symmetric Key Infrastructure

For more information on the symmetrical and asymmetric keys mentioned in this section, see Part B of Appendix 11 to Annex 1C of the Regulation.

1.3.1. Certification Authorities

Certification Authorities are listed in section 9.6 and section 9.8 of this Policy.

1.3.1.1. European Root Certification Authority (ERCA)

The ERCA is the Root Certification Authority (CA) that signs public key MSCA certificates. It operates the following component services: registration service, certificate generation service, dissemination service.
The ERCA generates PKI root key pairs and respective certificates, along with link certificates to create a chain of trust between different root certificates.
The ERCA is also the entity generating, managing and distributing on request the symmetric master keys, i.e. the Motion Sensor Master Key–VU part ($K_{M\text{-}VU}$), the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC}$) and the DSRC Master Key (K_{DSRC}).

1.3.1.2. Member State Certificate Authorities (MSCA)

The MSCA operate as sub-CA under the ERCA. They sign public key certificates for equipment. For this, they operate a registration service, certificate generation service and dissemination service. The MSCA receive the certificate requests from component personalisers and disseminate the certificates to these parties. There are two types of MSCA key pair(s) and corresponding MSCA certificate(s): one for the issuance of VU and EGF certificates; and one for the issuance of Card certificates. MSCA may request from the ERCA either or both types of MSCA certificate, depending on their responsibilities regarding the issuance of equipment.
The MSCA are also the entity requesting symmetric master keys from the ERCA. The MSCA distribute $K_{M\text{-}VU}$ to VU manufacturers, and $K_{M\text{-}WC}$ and K_{DSRC} to card personalisers. The 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 they then subsequently use to encrypt motion sensor serial numbers on request of a motion sensor manufacturer. Finally, MSCA may use K_{DSRC} to derive VU-specific keys by request of a VU manufacturer on basis of the VU serial number.

1.3.1.3. Lithuanian Member State Certificate Authority (LT-MSCA)

The Lithuanian MSCA (LT-MSCA) operates as sub-CA under the ERCA as described in the previous chapter. As there are no manufacturers of related equipment in Lithuania, the functionality for the delivery of Smart Tachograph certificates for Vehicle Units (VU), Motion Sensors (MoS) and External GNSS Facilities (EGF) is not implemented.
The LT-MSCA handles the MSCA key pair and corresponding MSCA certificate for the issuance of card certificates, called an LT-MSCA key pair.
The LT-MSCA submits the requests for symmetric master keys K_{DSRC} and $K_{M\text{-}WC}$ towards ERCA and distributes the received keys to the LT-CP, the Lithuanian card personaliser via secured network.
The LT-MSCA receives the certificate requests from the LT-CP and disseminates the certificates to this party. Additionally, for driver cards and workshop cards, the LT-MSCA ensures that Card_MA and Card_Sign certificates have the same Certificate Effective Date.
As a result of their responsibilities, the LT-MSCA disposes of the following cryptographic keys and certificates, at any moment in time:

- the current MSCA_Card key pair and corresponding certificate;
- all previous MSCA_Card certificates to be used for the verification of the certificates of tachograph cards that are still valid;
- the current EUR certificate necessary for the verification of the current MSCA certificate;

- all previous EUR certificates necessary for the verification of all MSCA certificates that are still valid.

1.3.2. Registration Authorities

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

1.3.3. Subscribers

The only subscribers to the ERCA public key certification service are the MSCA.
The only subscribers to the LT-MSCA public key certification service are the component personalisers of the tachograph cards (LT-CP). The component personalisers of the tachograph cards are responsible for the personalisation of the four different types of tachograph cards: driver cards, company cards, workshop cards and control cards.
The tachograph cards contain cryptographic keys and certificates.
The driver cards and workshop cards have two key pairs and corresponding certificates issued by an LT-MSCA, namely:
- a key pair and certificate for mutual authentication, called Card_MA;
- a key pair and certificate for signing, called Card_Sign.

The company and control cards have a key pair and corresponding certificate issued by an LT-MSCA 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.
The 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 LT-MSCA;
- performs the application for K_{M-WC} and K_{DSRC} (workshop cards only);
- ensures availability in the card of keys and certificates for mutual authentication and signing (with identical Certificate Effective Date), MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only).

The card personaliser for company and control cards:
- ensures generation of the card key pair for mutual authentication;
- performs the certificate application process with the LT-MSCA;
- 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).

An overview of the necessary keys on the respective card type can be found in the following table:

Card Type	Card_MA	Card_Sign	K_{M-WC}*	K_{DSRC}*
Driver Card	√	√		
Company Card	√			
Workshop Card	√	√	√	√
Control Card	√			√

** A workshop card respectively a control card has up to three K_{M-WC} keys resp. K_{DSRC} keys and the corresponding version numbers, as they relate to the root keys and their overlapping validity periods.*

1.3.4. Relying Parties

Parties relying on the ERCA public key certification service are primarily the national authorities tasked with enforcing the rules and regulations regarding driving times and rest periods, who use the ERCA certificates to validate the authenticity of MSCA certificates. MSCA certificates are then used

to validate the authenticity of equipment certificates, which in turn are used to validate the authenticity of data downloaded from Vehicle Units and driver cards.

1.3.5. Other relying parties are drivers, companies and workshops. Responsabilities

MSA shall be responsible for:

a) appointment of LT-CIA;
b) appointment of LT-MSCA;
c) appointment of LT-CP.

MSA shall be responsible for the proper enforcement of the Policy. MSA shall ensure card certificates are generated in accordance with the requirements of the Regulation No. 165/2014 and the Policy and the certificates contain all the required information.

LT-CIA shall be responsible for:

a) verification of cardholder's identity;
b) issuing of cards to persons, registration of persons and registration of applications on card issuing;
c) supervision of the status of the card.

LT-MSCA shall be responsible for:

a) generation of member state key pair;
b) management of member state key pair;
c) generation and registration of card certificates;
d) keeping records of issued certificates.

The LT-MSCA has the responsibility for conformance with the procedures prescribed in this Policy, even when the LT-MSCA functionality is undertaken by subcontractors / Service Agencies. The LT-MSCA is responsible for ensuring that any subcontractor / Service Agency performs all its functions consistent with the Policy requirements and PS of the certification process.

LT-CP shall be responsible for:

a) personalization of tachograph cards under request of LT-CIA;
b) transfer of personalized cards to LT-CIA.

Users will be responsible for:

a) timely submission of a card application to LT-CIA where the card is being issued for the first time, renewed or issued to replace a lost or stolen card, correctness of the submitted information;
b) proper use of the card and confidentiality of PIN code;
c) timely notification to LT-CIA that the card has been lost, stolen, is malfunctioning or is potentially compromised.

1.3.6. Obligations

MSA obligations:

a) enforces the requirements fixed in the Policy;
b) appoints LT-CIA, LT-MSCA and LT-CP;
c) organizes audit of the appointed LT-MSCA and LT-CP including the selected subcontractors / Service Agencies;
d) approves PS of LT-MSCA, LT-CP, LT-CIA;
e) informs LT-CIA, LT-MSCA and LT-CP about the Policy;
f) drafts this Policy and submits it to the ERCA for approval.

CIA obligations:

a) follows the requirements set in the Policy;
b) drafts PS of LT-CIA, which shall contain a reference to the present Policy;
c) handles identity data of cardholders (receives applications, checks the submitted data, verifies the applicant's identity);
d) transfers the data required for personalization to LT-CP;

e) ensures that correct and relevant user information submitted by the applicants when applying for a card is transferred to the LT-MSCA and LT-CP;

f) issues personalized Cards;

g) transfers PIN code to workshop cardholders;

h) maintains white and blacklists of cards;

i) informs the users about the rules and procedures of card issuing.

MSCA obligations:

a) follows the requirements set in the Policy;

b) drafts certification PS, which shall contain reference to the present Policy;

c) maintains sufficient organizational and financial resources to operate in conformity with the requirements laid down in this Policy, in particular to bear the risk of liability damages;

d) generates and registers member state keys;

e) generates and registers card certificates;

f) registers European keys and certificates;

g) takes part in presenting member state keys to ERCA for certification.

CP obligations:

a) follows the requirements set in the Policy;

b) publishes PS for personalization activities that includes reference to this Policy;

c) personalizes cards by printing identity data of cardholders on them and by recording data of cardholders, member state and European keys and certificates into them;

d) transfers personalized cards and PINs of workshop cards to LT-CIA;

e) maintains sufficient organizational and financial resources to operate in conformity with the requirements laid down in this Policy, in particular to bear the risk of liability damages;

f) informs LT-CIA about the status of personalization and transfer to LT-CIA of each card;

g) holds the responsibility for conformance with the procedures prescribed in this Policy, even when part of LT-CP functionality is undertaken by subcontractors / Service Agencies;

h) is responsible for the confidentiality of personal data until the card is sent to LT-CIA.

Obligations of subcontractors / Service Agencies:

Subcontractors / Service Agencies (if any) have obligations towards MSA according to contractual agreements prescribing their obligations. Despite the fact, that such agreements have been concluded, MSA has a full liability for the performance of any service, which is being regulated in this Policy.

Obligations of cardholders:

a) to submit accurate and complete information to LT-CIA in accordance with the requirements of this Policy;

b) to ensure the keys and certificates are only used in the digital tachograph system;

c) to ensure the cards are only used in the digital tachograph system;

d) ensure reasonable care is exercised to avoid unauthorized use of the cards and equipment private key;

e) to use only his own cards (Article 27(2) of the Regulation No. 165/2014);

f) to have only one valid driver card (Article 27(2) of the Regulation No. 165/2014);

g) only under very special and duly justified circumstances to have both a workshop card and a company card; workshop and driver cards; a few workshop cards;

h) to not use a malfunctioning or expired card (Article 27(2) of the Regulation No. 165/2014);

i) to notify LT-CIA immediately about any of the following:

- the card or the equipment private key have been lost, stolen, are malfunctioning or are potentially compromised (Article 29(4) of the Regulation No. 165/2014);
- the possibility to operate workshop card has been lost due to compromised PIN code;
- the contents of the certificate are inaccurate.

1.4. Key and Certificate Usage

This section contains provisions that address management.
The ERCA root certificates and ERCA link certificates shall be used to verify MSCA certificates issued by the ERCA.
The ERCA certificates will be the highest trust point for the PKI and shall be placed in VUs, cards and EGFs, as specified in Annex IC Appendix 11 of the Regulation. LT-MSA and PKI participants shall recognise the ERCA public key certificates, provided they are published by the ERCA according to the requirements in the ERCA Policy.
Member State Keys and Transfer Keys are generated in a certified HSM and stored in a physically protected environment with 24/7 security controls, electronic locks, and video control.
Hardware keys are symmetric keys generated during the manufacturing process of equipment that are LT-MSCA certified for the following parts of the digital tachograph system:

- keys to protect the connection between the VU and the motion sensor;
- keys to protect the connection through the DSRC connection between the VU and the remote early detection connection scanner.

The ERCA shall use its ERCA private keys only for signing of ERCA root, ERCA link and MSCA certificates, in accordance with Annex IC Appendix 11 of the Regulation.
The LT-MSCA shall use its Member State private keys only for:

- Signing of equipment certificates, in accordance with Annex IC Appendix 11 of the Regulation;
- Signing of Certificate Signing Requests.

The LT-MSCA tachograph card certificates described in the Policy on hand are never revoked or suspended.
The LT-MSCA certificates shall be used to verify card certificates issued by the LT-MSCA.
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.
$K_{M\text{-}WC}$ and the corresponding version number shall be provided to component personalisers for their installation respectively in workshop cards.
K_{DSRC} and the corresponding version number shall be used by control cards 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 ERCA shall not use the symmetric master keys for any purpose except distribution to the MSCA.
The LT-MSCA as well as the LT-CP shall not use the smart tachograph certificates and keys underlying the Policy on hand for any purpose except the ones described above.
The LT-MSCA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to LT-CP by secured network for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11 of the Regulation.

Note: As there are no manufactures of related equipment in Lithuania, the functionality for the delivery of Smart Tachograph certificates for VU, Motion Sensors and EGF is not implemented (see section 1.3.1.3). Motion sensor manufacturer and vehicle unit manufacturer apply their key request to the responsible MSCA. The LT-CP ensures the availability of the $K_{M\text{-}WC}$ and K_{DSRC} keys to be used within in the control cards and workshop cards.

1.5. Policy Administration

1.5.1. ERCA

The European Commission service responsible for implementing the certification policy at European level and providing core certification and key distribution services to Member States is called the European Root Certification Authority (ERCA).
ERCA contact address is:
Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

1.5.2. MSA

The Responsible Authority (MSA) of the Member State is responsible for the implementation of this Policy.

MSA:
Lithuanian transport safety administration
Švitrigailos str. 42
LT-02309 Vilnius
Lithuania

In this document, Lithuanian Transport Safety Administration is called LTSA.
The functions assigned to the LT-CIA are performed by the LTSA.

1.5.3. LT-MSCA and LT-CP

Member States delegate the functions of the Personalization Center (LT-CP) to:
Thales DIS Finland Oy
Myllynkivenkuja 4, FI-01620 Vantaa, Finland

Member States delegate the functions of the Certification Center (LT-MSCA) to:
CertSing S. A.
Oltenitei Avenue Nr. 107 A, Building C1, ground floor, CP 041303, Sector 4, Bucharest, Romania
The visiting address:
29A Tudor Vladimirescu Blvd., 2nd floor, District 5, Bucharest, Romania
Email: *cards.helpdesk@certsign.ro*

LT-MSCA or LT-CP can not transfer part of the functions to subcontractors / service agencies.

1.6. Definitions and Acronyms

The following abbreviations and definitions are used in the present document:

CA / PA	Certification Authority Administrator / Personalization Administrator
CHR	Certificate Holder Reference
CIA	Authority in charge of issuing cards and handling data related to the issued cards, status, holders thereof and other data related to issuing of cards
LT-CIA	Lithuanian authority in charge of issuing cards and handling data related to the issued cards, status, holders thereof and other data related to issuing of cards

CP	A legal person in charge of personalization of a card, i.e. generation of public and private keys of a card, identification of a cardholder and printing of other required data on the card, providing of this data
LT-CP	A legal person in charge of personalization of a card in Lithuania, i.e. generation of public and private keys of a card, identification of a cardholder and printing of other required data on the card, providing of this data
ERCA	The authority appointed by the European Commission in charge of generation of European electronic keys used in the tachograph system, certification of member state keys and distribution of certificates
EQT	Equipment of a digital tachograph (cards, VU and Motion Sensors)
EQT.C	Equipment Certificate
EQT.PK	Equipment Public Key
EQT.SK	Equipment Private Key
EUR.PK	European Public Key
EUR.SK	European Private Key
ISSP	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
Km	European Master Key (TDES)
KmVU	TDES key recorded in the Vehicle Unit
KmWC	TDES Key recorded in the Workshop Card
MS.C	Member State Certificate
MS.PK	Member State Public Key
MS.SK	Member State Private Key
MSA	The authority in charge of development, functioning of the tachograph system and monitoring of functioning status thereof.
LT-MSCA	Lithuanian Member State Certification Authority
Ns	Extended series number of a motion sensor
PIN	Workshop card authentication code
RSA	Rivest's, Shamir's and Adelmann's asymmetric coding algorithm
SA	Information System Administrator
TDES	Triple DES. A key that is 3 times longer, i.e. 3 simple DES keys used to consistently cipher / decipher the data
VU	Vehicle unit
Audit	Checking of activities in order to establish whether the activities are in line with the requirements set in the Policy and the PS
Blacklist	A list of invalid (withdrawn, lost, stolen, malfunctioning, confiscated) or temporary invalid (suspended) issued cards, card certificates
Ciphering	The process of translating the data (text) into ciphered (coded) form. Ciphered text is not understandable
Confidential information	Information which is not publicly available the unauthorized revealing of which may be harmful to the functioning of the digital tachograph system
Card	A smart card, which is intended to identify a cardholder (or identity group) and store certain data, which is registered by a digital tachograph. There exists driver, control, workshop and company cards
Card personalization	A smart card intended for use with a digital tachograph. From the tachograph cards the digital tachograph may identify a card colder (or identity group); data may be rewritten and stored in the tachograph card

Certificate	A digital certificate whereby information about the subject (such as name, validity date, public key and electronic CA signature whereby the authenticity of a certificate may be verified) is transferred
ERCA public key	Used for verifying the Member State certificates. ERCA private key is not dealt with here, since it never leaves ERCA
Digital tachograph	All equipment intended to automatically or semi-automatically record and store in the vehicles comprehensive information on the activity of the vehicles and certain periods of drivers' work and rest.
Key	A variable, which has a line or a block of symbols assigned thereto by using certain algorithm. A key may be used to cipher a notification or decipher a ciphered notification, The length of a key constitutes the safety criterion of ciphering
Member state keys	The member state signing keys and may also be called member state root keys
Motion sensor keys	The symmetric keys to be placed in the workshop card, VU and motion sensor for mutual recognition. LT-MSCA receives the motion sensor keys from ERCA, stores them and distributes them to manufacturers
Private key	A key to cipher / decipher notifications, which is known to one or all-communicating parties. In the case of Public key infrastructure the private key is used together with the public key
Public key	A key, which is publicly distributed and used for deciphering of notifications and electronic signature. A public key which along with the private key constitutes the mechanism of asymmetric ciphering
Transport keys	RSA key pairs to be used in secure transfer of motion sensor keys between ERCA and LT-MSCA
Relying parties	Organizations or persons that are using certificates and / or the information of the digital tachograph system on the status of certificates
Visual personalization	Printing of information on the card
White-list	A list of valid issued cards, card certificates.
Workshop	A workshop or a company, which is manufacturing or installing tachographs or is manufacturing vehicles and is approved in the Republic of Lithuania under the established procedure. Workers of such company may have workshop cards issued.

2. Publication and Repository Responsibilities

2.1. Repositories

The LT-MSCA is responsible for hosting and storing certificates issued. Access to the repository is not public.

2.2. Publication of Certification Information

Policy are published on the LTSA website: https://www.ltsa.lrv.lt/.

Questions addressed to this policy should be sent to:
Lithuanian transport safety administration
Švitrigailos str. 42
LT-02309 Vilnius
Lithuania

The Practice Statement shall not be public but shall be communicated on re-quest 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 9.12 of of this Policy.

2.4. Access Controls on Repositories

All information available on repositories shall have read-only access.
All information published on on repositories shall be available via a secure Internet connection.
The access to the repositories should be granted at least to LT-MSA and LT-CP.

3. Identification and Authentication

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

3.1. Naming

3.1.1. Types of Names

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 IC.

3.1.1.2. Key Distribution Requests and Key Distribution Messages

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 IC, Appendix 11, CSM_136/CSM_141 and Appendix 1 of the Reglation.

3.2. Initial Identity Validation

3.2.1. Method to prove Possession of Private Key

When LT-LMSCA submitting certificate signing requests (CSRs) to the ERCA, proof of possession of the corresponding private key via an internal signature, as specified in section 4.1.1 of ERCA Policy, is necessary. The 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.

Card personalisation request submitted by the LT-CIA do not contain private keys, but authentication shall be provided using secured network.
LT-CP submitting Card Certificate Signing Requests (Card-CSRs) shall prove possession of the corresponding private key with the LT-CP signature and shall prove the integrity and request authentication with the request signature.

3.2.2. Authentication of Organization Identity

LT-MSCA defines a procedure for authentication of organization identity in its PS.

3.2.3. Authentication of Individual Identity

LT-MSCA defines a procedure for the authentication of individual identities in its Practice Statement.

The LT-CIA authenticates natural persons during card application validation and approval process for driver cards based on the already authenticated entries of the national register of drivers and register of natural persons.

3.2.4. Validation of Authority

LT-MSCA defines a procedure for the validation of authority in its Practice Statement.
The initial determination of permission to act on behalf of an organisation is not part of the card application validation and approval process. Card application for organisations rely on already determined register entries of authorized people.

3.2.5. Criteria for Interoperation

The LT-MSCA shall not rely on any external certification authority except the ERCA for the certificate signing and key distribution services it provides to the smart tachograph system.
If the LT-MSCA must rely on an external PKI for any other service or function, review and approval of the CP and/or CPS of the external certification service provider by the LT-MSA prior to applying for certification services, is required.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

The Identification and Authentication procedures for re-key requests towards ERCA are defined in section 3.3 of the ERCA Policy.
The Identification and Authentication procedures for re-key requests applied by LT-CP towards LT-MSCA shall be the same as those described in section 3.2. Key generation for tachograph cards is done by LT-CP and therefor tachograph card keys are not subject to key requests.

3.4. Identification and Authentication for Revocation Request

The validation of LT-MSCA certificate revocation requests is defined in the section 3.4 of the ERCA Policy.
Card certificate revocation is not allowed. Card revocation is handled within the national register of the tachograph cards using card status.

4. Life-Cycle Operational Requirements for Certificates, symmetric Keys and Encryption Services

4.1. MSCA Public Key Certificate Application and Issuance

Applications for the approval of the keys are assessed, verification, generation, distribution and administration of certificates are conducted in accordance with the ERCA Policy.
The LT-MSCA public key format is described in section 7.1 of the ERCA Policy.
Exchange of inquires and responses to them are carried out in accordance with the ERCA Policy.
Modifications of certificates are strictly prohibited. Certificates shall be revoked based on the grounds provided in the ERCA policy.

4.1.1. Certificate Signing Requests

Certificate Signing Requests (CSR) can only be submitted by LT-MSCA recognised by LT-MSA. The European Authority is responsible for recognising MSA.
The master keys for the tachograph cards shall be handed over from LT-MSCA to LT-CP using the defined and agreed file format and signature rules for master key exchange.
The card personalisation requests data shall send to the LT-CP via secured network.

The Card Certificate Signing Requests shall include the untouched and signed personalisation request data and shall contain the card specific keys signed by the LT-CP. The LT-CP shall sign the overall request and sent it to the LT-MSCA.
The LT-MSCA response to the LT-CP Card Certificate Signing Request shall include the requested certificates as part of an overall signed message file.
Card Personalisation Request can only be submitted by the LT-CIA. Card Certificate Signing Requests (Card-CSRs) can only be submitted by the LT-CP.
A CSR format shall follow the requirements of Section 4.1.1 of ERCA Policy.

4.1.2. Certificate Application Processing

4.1.2.1. Verification of CSR contents

For submitter identification and authentication reasons the LT-MSCA examines every incoming Card Certificate Signing Request concerning:
- the correctness and validity of order data signature of LT-CIA;
- the correctness and validity of certificate signing data signature of LT-CP;
- the completeness of key data corresponding to the card type treated in the request;
- the correct validity data corresponding to the card type treated in the request;
- the absence of error messages.

For submitter identification and authentication reasons the LT-CP examines every incoming Card CSR Response concerning:
- the correctness and validity of the order result (certificates);
- the absence of error messages (status).

4.1.2.2. Certificate generation, distribution and administration

If all checks succeed, the ERCA shall proceed to sign the certificate as described in section 4.1.3 of ERCA Policy.

4.1.3. Certificates

The format of the LT-MSCA public key certificates can be found in section 7.1 of ERCA Policy.
The LT-MSCA validates only once and in general for all requests the validity of the Member State Certificate.
The LT-MSCA validates for every incoming Card Certificate Signing Request:
- the requested card types are valid;
- the Begin of Validity (BOV) and End of Validity (EOV) are corresponding to EU requirements concerning the period of validity per card type;
- the LT-CIA signature is valid and the authorisation of the personalisation data thus is proofed;
- the LT-CP signature is valid and the authorisation of the keys sent is therefore proven;
- the request signature is valid and the integrity of the request is therefore proven;
- the keys to be signed are cryptographically useable and in particular not damaged or corrupted.

4.1.4. Exchange of Requests and Responses

For transportation of certificate signing requests and certificates, CD-R media should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).
Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA shall accept and dispatch CSRs and certificates as e-mail attachments.
The LT-MSCA shall write one to three copies of each certificate signing request to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) or binary (.bin file) format.

The ERCA shall write three copies of each certificate to the transport medium for return to the LT-MSCA. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.
Each certificate signing request and certificate shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA Policy. Another paper copy of the data shall be held by the ERCA or the LT-MSCA, respectively.
For both CSRs and certificates, the transport media and the printouts are handed over between an ERCA employee and the courier in the ERCA controlled area.

4.1.5. Certificate Acceptance

The courier signs for receipt of the LT-MSCA certificate at the ERCA premises. Upon reception of the certificate at the LT-MSCA premises, the LT-MSCA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the certificate complies with Table 5 in section 7.1 of ERCA Policy;
- 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 LT-MSCA shall abort the process and contact the ERCA. Certificate rejection is managed according to the certificate revocation procedure (see Section 4.1.10 of this Policy).
The Card Key Certification is part of the automatically processed reply to the Card Certificate Signing Request. The LT-CP uses the reply deposited on the card information module to finish the card creation process.

4.1.6. Key Pair and Certificate Usage

The Card Certificates as part of the Card Key Certification Reply sent to the LT-CP and used for card personalisation are exclusively intended for the usage on the cards. The Card Certificates are not subject of any publication.
The LT-MSCA shall use any key pair and the corresponding certificate in accordance to Section 6.2 of this Policy.
The LT-MSCA shall ensure that the LT-MSCA private signing keys are only used for the national Card Certificate Signing Requests for use within the Digital Tachograph system. The LT-MSCA shall ensure that, after certification of the national level keys, the LT-MSCA private signing keys are only used for the production of public key certificates for use within the Digital Tachograph system.
The LT-CP shall use any key pair and the corresponding certificate in accordance to Section 6.2 of this Policy.
The LT-CP shall ensure that master keys, tachograph card keys and tachograph card certificates are only used for tachograph card production as described in the document on hand.
Card user ensure proper application of keys and certificates by ensuring correct usage of their tachograph cards.
Card user shall ensure that the tachograph cards are exclusively used as intended. In particular card user acknowledge that tachograph cards are not transferable and any other usage than for tachograph systems is prohibited.

4.1.7. Certificate Renewal

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

4.1.8. Certificate Re-key

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

- when an LT-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 LT-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 LT-MSCA key pair(s) may be changed regularly.
LT-MSCA certificate re-key is described in section 4.1.8 of ERCA Policy.
For Card Key Certification no certificate re-key process is in place. Every Card Certificate Signing Request is treated as a new application.

4.1.9. Certificate Modification

Certificate modification is not allowed.

4.1.10. Certificate Revocation and Suspension

Certificates and keys subject to the Certificate Signing Requests towards ERCA following the revocation process described in section 4.1.10 of ERCA Policy.
Certificates and keys subject to the Card Certificate Signing Request cannot be revoked.
Certificates and keys subject to a compromised or suspected compromised Card Certificate Signing Request shall not be used for card creation and card personalisation.
Provisions in case of key compromise or suspected key compromise following the national compromise procedure as described in Section 5.7 of this Policy, and may result in at least one of the following provisioning steps:

- issuing of a replacement card containing uncompromised keys;
- master key replacement following the ERCA re-key process;
- LT-MSCA Certificate replacement following the ERCA certification revocation process.

Certificate suspension is not allowed.

4.1.10.1. Circumstances for certificate revocation

Not applicable.

4.1.10.2. Who can request revocation

Not applicable.

4.1.10.3. Procedure for revocation request

Not applicable.

4.1.10.4. Revocation request grace period

Not applicable.

4.1.10.5. Time within which ERCA shall process the revocation request

Not applicable.

4.1.10.6. Revocation checking requirements for relying parties

Not applicable.

4.1.10.7. Certificate status issuance frequency

Not applicable.

4.1.10.8. Maximum latency for CRLs

Not applicable.

4.1.10.9. On-line revocation / status checking availability

Not applicable.

4.1.10.10. On-line revocation / status checking requirements

Not applicable.

4.1.10.11. Other forms of revocation advertisements available

Not applicable.

4.1.10.12. Special requirements concerning key compromise

Not applicable.

4.1.10.13. Certificate suspension

Not applicable.

4.1.11. Certificate Status Service

Certificate status information for all issued certificates is maintained by the LT-MSCA. This information shall not be published but will be made available to parties having a legitimate interest upon request.

4.1.12. End of Subscription

End of Subscription regulations for the ERCA's certificate signing services are described in section 4.1.12 of ERCA Policy.
An End of subscription on LT-MSCA level is not envisaged.

4.1.13. Key Escrow and Recovery

Key escrow is strictly prohibited to any participants. This applies to the LT-MSCA and the LT-CP. However, keys are backed up in at least two encrypted backup tokens stored in separate, secure locations off-site. For recovering backup tokens, at least two authorized staff members of the LT-MSCA or respectively of the LT-CP are required.

4.2. Master Key Application and Distribution

Applications for the issuance of the keys are assessed, verification, generation, distribution and administration of the keys are conducted in accordance with the ERCA Policy.
Exchange of inquires and responses to them are carried out in accordance with the ERCA Policy.

4.2.1. Key Distribution Requests

Key Distribution Requests (KDR) can only be submitted by LT-MSCA or LT-CP recognised by LT-MSA. The European Authority is responsible for recognising MSA.
A KDR format shall follow the requirements of Section 4.2.1 of ERCA Policy.

4.2.2. Master Key Application Processing

Key distribution requests (KDR) towards ERCA are following the same preconditions that are defined for CSRs and therefore KDRs can only be submitted by LT-MSCA or LT-CP.

4.2.2.1. Verification of KDR contents

For submitter identification and authentication reasons the LT-MSCA or / and LT-CP examines every incoming Key Distribution Message concerning:

- the correctness of profile, authorisation and key identifier;
- the correctness and validity of the MAC;
- the absence of error messages.

4.2.2.2. KDM generation, distribution and administration

If all checks succeed, the ERCA shall proceed to prepare the key distribution message (KDM) by determining the symmetric key requested by the LT-MSCA or / and LT-CP and following the steps as described in section 4.2.3 of ERCA Policy.

4.2.3. Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys shall be ensured as decribed in section 4.2.3 of ERCA Policy.

4.2.4. Key Distribution Messages

Key distribution message format should follow requirements decribed in section 4.2.4 of ERCA Policy.

4.2.5. Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages, CD-R media should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).
Other transport methods may be used after prior consent of the ERCA. For testing purposes, the ERCA shall accept and dispatch key distribution requests and key distribution messages as e-mail attachments.
The LT-MSCA or / and LT-CP shall write one to three copies of each key distribution request to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) or binary (.bin file) format.
The ERCA shall write three copies of each key distribution message to the transport medium for return to the LT-MSCA or / and LT-CP. These copies shall be in hexadecimal ASCII (.txt file), Base64 (.pem file) and binary (.bin file) format.
Each KDR and KDM shall be accompanied by a paper copy of the data, formatted according to a template defined in the ERCA Policy. Another paper copy of the data shall be held by the ERCA or the LT-MSCA or / and LT-CP, respectively.
For both KDRs and KDMs, the transport media and the printouts shall be handed over between an ERCA employee and the courier in the JRC controlled area.

4.2.6. Master Key Acceptance

The courier signs for receipt of the key distribution message at the ERCA premises. Upon reception of the key distribution message at the LT-MSCA or / and LT-CP premises, the LT-MSCA or / and LT-CP shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with Table 4 in section 4.2.4 of ERCA Policy;
- the message is genuine;
- 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 LT-MSCA to the ERCA.

If any of these checks fail, the LT-MSCA or / and LT-CP shall abort the process and contact the ERCA.
If all these checks succeed, the LT-MSCA or / and LT-CP shall follow the procedures in ERCA Policy.

4.2.7. Master Key Usage

The LT-MSCA shall use any received master key in accordance to section 6.2 of ERCA Policy.

4.2.8. KDM Renewal

KDM renewal means the issuance of a copy of an existing KDM to an LT-MSCA or / and LT-CP 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 LT-MSCA or / and LT-CP are damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported to the LT-MSA or / and LT-CP and the ERCA. After this report, the LT-MSCA may send a KDM renewal request to the ERCA, referring to the original key distribution request.
Note: In case the LT-MSCA or / and LT-CP needs to send a request to redistribute a master key that was already successfully distributed to the LT-MSCA or / and LT-CP, it shall generate a new key distribution request, using a newly generated ephemeral key pair. Such a request may lead the ERCA to initiate an investigation of the possibility of key compromise.

4.2.9. Master Key Re-key

To receive the new version, LT-MSCA or / and LT-CP shall submit a new KDR. Requesting a new master key shall take place in a timely manner so that the key (or derived keys or encrypted data for motion sensors) can be placed in time in newly issued components.
Key application, processing, distribution and acceptance is the same as for the initial key.

4.2.10. Symmetric Key Compromise Notification

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

4.2.11. Master Key Status Service

The LT-MSCA or / and LT-CP do not offer any key status service.
The status can be derived directly from the validity date of the key.

4.2.12. End of Subscription

End of Subscription regulations for the ERCA's certificate signing services are described in section 4.2.12 of ERCA Policy.
An End of subscription on LT-MSCA or / and LT-CP level is not envisaged.
Subscription for the ERCA's key distribution services ends when an LT-MSA decides for MSA termination. Such a change is notified to the ERCA by the LT-MSA as a change to the Policy.
In the case of subscription ending, the LT-MSCA or / and LT-CP shall securely destroy all copies of any symmetric master key in its possession.

4.2.13. Key Escrow and Recovery

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

4.3. Member State keys generating

Member state key pair generation shall be carried out within a HSM.
The actual device used and requirements met shall be stated in the LT-MSCA PS.
LT-MSCA key-pair generation shall require the participation of three separate individuals. At least one of these shall have a role of CAA / PA (certification authority / personalization administrator).

Keys shall be generated using the algorithm with the key lengths in accordance with the Regulation and Annex 1C (1024-bit RSA) of the Regulation.
The key generation device shall be stand-alone.
Key generation shall be performed by authorized staff in a physically secure environment under at least dual control, i.e. when choosing the technical means, it is required that at least two authorized persons are present, one which shall have be the staff of LT-MSCA and the other of LT-MSA.
LT-MSCA shall have more than one certified member state key pair since ERCA cannot issue replacement member state certificates rapidly.

4.4. Member state private key backup

The member state private key may be backed up to ensure key recovery if needed under at least dual control. The backing up procedure used shall be stated in LT-MSCA PS.

4.5. Member state keys compromise

A written instruction shall exist, included in LT-MSCA PS, which states the measures to be taken by LT-MSCA staff in charge of security if the member state private key has become exposed, or is otherwise considered or suspected to be compromised.
In such case the LT-MSCA shall as the minimum:
- inform without delay the MSA, the ERCA and other LT-MSCAs;
- will start disaster recovery actions independent of response delay from ERCA.

4.6. Member state keys end of life

The LT-MSCA shall ensure that it always has a valid certified Member state key pair.
Upon termination of use of a Member State key pair, the public key shall be archived, and the private key shall be destroyed in such a manner that the private key cannot be retrieved.
The procedures of public key backing up and private key destroying shall be stated in LT-MSCA PS.

4.7. Motion sensor keys

The LT-MSCA or / and LT-CP shall, as needed, request motion sensor keys $K_{M\text{-}WC}$ and K_{DSRC} from the ERCA (Appendix 11: 3.1.3, Annex 1C of the Regulation).
If the keys were requested by the LT-MSCA, it shall only forward the workshop key $K_{M\text{-}WC}$ to the LT-CP for insertion into Workshop cards.
LT-MSCA or / and LT-CP will ensure that keys are not used for any purposes and that they will never leave the secure environment of LT-MSCA or / and LT-CP. The LT-CP shall undertake the LT-MSCA's task to ensure that the workshop key $K_{M\text{-}WC}$ is inserted into all issued Workshop cards (Appendix 11: 3.1.3, Annex 1C of the Regulation).
The LT-MSCA and / or LT-CP shall, during storage, use and distribution, protect the motion sensor keys with high assurance physical and logical security controls. The keys should be contained in and operated from a specific tamper resistant device which meets the requirements identified in Section 6.2 of ERCA Policy.

4.8. Card certificates

4.8.1. Driver card certificates

Driver certificates are issued only to successful applicants for a driver card.

4.8.2. Workshop card certificates

Workshop certificates are issued only to successful applicants for a workshop card.

4.8.3. Control card certificates

Control body certificates are issued only to successful applicants for a control card

4.8.4. Company card certificates

Company certificates are issued only to successful applicants for a company card.

4.8.5. VU certificates

Not applicable in Lithuania for the time being.

4.8.6. EGF certificates

Not applicable in Lithuania for the time being.

4.9. Equipment certificate issuing

LT-MSCA shall ensure that it issues certificates so that their authenticity and integrity is maintained. The content of the certificates is defined by Appendix 11 of Annex 1C of the Regulation. Management and storage of certificates shall be stated in LT-MSCA PS.

4.10. Certificate revocation

LT-MSA may ask to revoke certificates issued by LT-MSCA.

4.11. Request and distribution

4.11.1. Data input

4.11.1.1. Tachograph cards

Cardholders do not apply for certificates. Their certificates are issued based on the information given in the application for a card and captured from the LT-CIA register. The public key to be certified is extracted from the key generation process.
LT-CP shall ensure that the input data contains information, which renders the Certificate Holder Reference (CHR) unique. LT-MSCA shall verify the uniqueness of the CHR.
If the equipment key pair is not generated by LT-MSCA, the certificate request process shall ensure that the LT-MSCA has the possibility to verify the connection of the private key and the public key presented for certification.
A digital signature of the card public key certification request produced with the corresponding private key would provide the LT-MSCA with the means to prove:

- integrity and origin of the key certification request, without revealing the private key;
- possession of the private key by the entity which produced the request.

4.11.1.2. VU and EGF

Not applicable in Lithuania for the time being.

4.11.2. Dissemination of equipment certificates and information

LT-CP shall transfer all the data about the certificates entered into the cards to the LT-CIA database. Thereby the certificates, equipment and users are associated with each other.
LT-CIA shall ensure that the certificates, if required, are made available to all parties concerned.

5. Facility, Management, and Operational Controls

The LT-CIA, LT-MSCA and LT-CP shall have PS used to address all the requirements identified in the Policy, which shall be approved by MSA, in particular:

a) the PS shall identify the obligations of all external organizations supporting the LT-CIA, LT-MSCA and LT-CP services including the applicable policies and practices;

b) the PS shall be made available to MSA. LT-CIA, LT-MSCA and LT-CP are not obliged to make all the details of their practices public and available for the users;

c) the management of the LT-CIA, LT-MSCA and LT-CP has responsibility for ensuring that the PS is properly implemented;

d) LT-CIA, LT-MSCA and LT-CP shall define a review process for the PS.

LT-CIA, LT-MSCA and LT-CP shall give due notice to MSA of changes and additions it intends to make in its PS and, following approval, make the revised PS immediately available. Minor revisions may be released without MSA approval.

5.1. Physical Security Controls

Physical security controls shall be implemented to control access to LT-MSCA or LT-CP hardware and software. This includes the workstations and certification and personalization hardware and any external cryptographic hardware module or card. A log shall be kept over all physical entries.

The LT-MSCA shall describe in its PS how it will keep physically and logicaly protected the member state keys for signing certificate.LT-MSCA / LT-CP's facility shall also have a place to store backup of LT-MSCA / LT-CP system in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. These backups shall be kept both for data recovery and for the archival of important information. Backup of LT-MSCA / LT-CP system media shall also be stored at a site different from where LT-MSCA / LT-CP system resides, to permit restoration in the event of a natural disaster to the primary facility.

A security check of the facility housing LT-MSCA / LT-CP's central equipment shall be made at least once every 24 hours. If it is a continuously attended facility, this may be a visual check once per shift to ensure that the systems and any associated cryptographic devices / cards are securely stored if not in use, that the physical security systems (e. g., door locks and alarms) are functioning properly, and that there have been no attempts at forceful entry.

Access to the physical area housing the member state keys and the means for their usage, shall require simultaneous presence of at least two persons which have been individually appointed the right to enter the area.

Access to other LT-MSCA / LT-CP facilities shall be limited to those personnel performing one of the roles described in Section 5.2.2.1 of this Policy. Access may be controlled using an access control list to the room housing the systems. Anyone not on the access control list shall be escorted by a person on the list. If an access control list is not feasible for a particular site, it may be acceptable to make sure that the certification and personalization related material is locked in a secure room or storage area when it is not being used.

The private key shall be contained in and operated from inside a specific tamper resistant device (HSM).

For access to the LT-MSCA private signing keys, dual control is required. This means that no single person shall possess the means required to access the environment where the private key is stored. It does not mean that signing of equipment certificates must be performed under dual control.

Member State private key shall not be made public.

The storage of Member State private key shall be stated in LT-MSCA PS.

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). The secured location is equipped with water detectors connected to the building's surveil-lance centre. The secured location is equipped with smoke and heat detectors connected to the build-ing's surveillance centre.

Personnel shall use the appropriate mechanisms depending on the classification of the data held by media for removal, e.g. magnetic and mechanical shredders.

Procedures for the disposal of waste shall be implemented to avoid unauthorized use, access, or disclosure of confidential data.

5.2. Procedural Controls

Tools of procedural controls are implemented in order to ensure safe operations. In particular, the segregation of duties is carried out during multilateral surveillance of important tasks.
Access to LT-MSCA systems is enabled only to persons who are entrusted and duly authorized to perform the tasks. The LT-MSCA shall implement the access control measures which are referred in point 5.2 of the ERCA policy.
Each of the trusted roles described below is assigned to one person with at least one substitute. All system user rights are restricted according to their role. Role description and role concept are part of nonpublic documents.

5.2.1. Trusted roles

LT-MSCA / LT-CP, supporting this Policy, should recognize at least three distinct roles. The roles have different authorizations assigned.
To ensure that one person acting alone cannot affect safeguards, each person shall have roles and responsibilities assigned. Each user account shall have limited rights commensurate with the role of the account holder.
The recommended roles are:

a) Certification Authority Administrator or Personalization Administrator (CA / PA);
b) Information System Administrator (SA);
c) Information System Security Officer (ISSO).

The role of a Certification Administrator / Personalization Administrator includes:

a) key generation;
b) certificate generation;
c) personalization and secure distribution of equipment.
d) administrative functions associated with maintaining the LT-MSCA / LT-CP database.

The role of the System Administrator includes:

a) performing initial configuration of the system including secure boot start-up and shut down of the system;
b) initial set up of all new accounts;
c) setting the initial network configuration;
d) creating emergency system restart media to recover from system break down and protection of data from loss;
e) performing system backups, software upgrades.

Backups shall be performed at least once per week. The system shall be restarted after a backup is performed, so that the checks of hardware integrity, the changes of IP address and / or name are performed.

a) The role of the Information System Security Officer includes:
b) assigning rights to Certification Administrators / Personalization Administrators;
c) assigning passwords to all new accounts;
d) performing archiving of all required system records;
e) review of the audit log to detect violations by the Certification Administrator’s / Personalization Administrator’s compliance of the security policy. Review of the audit log shall be done at least once per week;
f) personal supervision of the annual inventory of LT-MSCA / LT-CP's records;
g) participating in member state key generation process.

5.2.2. Separation of roles

For each of the role at least one individual shall be appointed. All roles shall be separated.

5.2.3. Identification and authentication for each role

Identification and authentication of the Certification Administrator / Personalization Administrator, System Administrator and Information System Security Officer shall be consistent with the PS and the provisions of this Policy.
LT-MSCA and LT-CP running a tight access rights management and control for identifying and authenticating its personnel handling the certification processes. The access control uses security mechanisms capable of separating the different trusted roles detailed in Section 5.2.1 of this Policy and identifying the specific functions within a role each of the role owners fulfils at any time.

5.2.4. Information security management by MSCA and CP

LT-MSCA / LT-CP shall ensure that administrative and management procedures are applied which are adequate and correspond to the recognized standards.
LT-MSCA / LT-CP shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by LT-MSCA / LT-CP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by LT-MSCA / LT-CP.
The information security infrastructure defined in LT-MSCA / LT-CP PS and needed to manage the security within MSCA / CP shall be maintained at all times.
LT-MSCA and LT-CP shall establish an information security management system (ISMS) based on a risk assessment for all the operations. LT-MSCA and LT-CP shall ensure that the ISMS policies address personnel training, clearances and roles. The LT-MSCA and LT-CP, no later than 1 year after starting its operations, shall be accredited in accordance with general policy requirements according to LST EN ISO/IEC 27001:2017 “Information technologies. Safety methods. Information security management systems. Requirements.”.

5.2.5. Personnel security controls of MSCA / CP

The LT-MSCA and LT-CP assign roles to their employees, ensuring that no conflicts regarding the separation of duties arise. In case of LT-MSA e.g. members of the Operating Team shall not be PKI Security Officers and vice versa.
Except for the standard tasks performed by the Operating Team, security critical actions require at least two individuals having different roles (see Section 5.2.1 of this Policy) to jointly execute the steps.
The following activities require the presence of two persons in different roles:

- Generating the LT-MSCA signature keys – additionally in presence of the LT-MSA contact person;
- Installation, activation and backup the LT-MSCA signature keys - additionally in presence of the LT-MSA contact person;
- Recovery of the LT-MSCA signature keys;
- Export and import of the LT-MSCA signature keys via backup token;
- Exchange of the hardware modules containing LT-MSCA signature keys;
- Generating the LT-CP public keys (Card_MA/Card_Sign) used within the Card-CSR towards LT-MSCA.

5.2.6. Security management controls

The system roles (see Section 5.2.1 of the Policy) shall be implemented and enforced.

5.3. Personnel Controls

The individual assuming the role of a Certification Administrator / Personalization Administrator shall be of unquestionable reputation and shall undertake responsibility for his acts related to certification / personalization.

LT-MSCA / LT-CP personnel in sensitive positions, including Certification Administrator / Personalization Administrator and Information System Security Officer shall:

a) not be assigned other duties that may conflict with their duties and responsibilities as administrator / officer;

b) not have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;

c) have received proper training in the performance of their duties;

d) has been checked for clearance by police or equivalent organization and meet specified requirements:

- according to established government clearance schemes;
- for a clean criminal record;
- for a satisfactory credit check.

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

Personnel training and appointment to trusted roles shall be described in the respective PS and in accordance with the requirements defined in ERCA Policy.

LT-MSCA and LT-CP are operated by qualified and experienced specialists only. Background checks must be performed for each employee.

The trusted roles described in Section 5.2.1 of this Policy are in general only given to people:

- who are beyond doubt concerning their safety awareness, trustworthiness, integrity and loyalty;
- in whom there are no conflicts of their role with other tasks and responsibilities;
- not previously known to have acted careless or negligently in previous employments or employment relationships.

To get assigned a LT-MSCA or a LT-CP trusted role, staff are subjected to a security review as per the ordinance on security checks for persons.

Each employee is personally informed of the extent and limits of his area of responsibility. Each employee's employment contract contains a special confidentiality clause.

For LT-MSCA employees the use of PKI hardware and software requires authentication by smartcard with personal PIN. The access the CA Console application underlies additional password protection.

For LT-CP employees the use of PKI hardware and software requires authentication by UserID and password.

Before the staff can take up their duties, it is trained according to its role to be taken. The LT-MSCA as well as the LT-CP staff must be familiar with the software, hardware and internal operational workflows of the certificate infrastructure components they work with. They must understand the processes they are involved in and they have to understand the effects of all actions they take.

Each employee assigned a LT-MSCA or LT-CP task receives an initial training covering the PKI system operated, its organization, security policy, emergency plans, software used and the activities he will be tasked with.

Each employee assigned a LT-MSCA or LT-CP task shall complete the necessary training after each major enhancement of system, organization, tools and/or methods.

Unauthorised actions by LT-CP personel are sanctioned according to the labor regulation of LT-CP.

5.4. Audit Logging Procedures

All significant security events in LT-MSCA software shall be automatically time-stamped and recorded in the system log files.

Events, described in the ERCA policy, shall be recorded in the system register. The LT-MSCA may extend the list of registered events as described in the LT-MSCA's Terms of Reference (PS).

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 PS.
Audit logs shall be verified and consolidated at least monthly. At least two people in SA or ISSO roles (see Section 5.2.1 of the Policy) shall be present for such verification and consolidation.

5.4.1. Audit log backup procedures

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.
The audit log shall be protected from unauthorized access.

5.5. Records Archival

The log shall be processed regularly and analysed against malicious behaviour. Log procedures shall be described in the PS.
For all archived information, archival periods shall be indefinite.
Procedures shall be in place to ensure integrity, authenticity and confidentiality of the records.

5.5.1. Types of events recorded by the CIA

The records of the information system shall include all relevant evidence in the LT-CIA's possession including:

a) user's applications for cards, including the identity of the person responsible for accepting the application;

b) signed acceptance of the delivery of cards;

c) documents regarding certificates and associated cards;

d) card renewals and all messages exchanged with the user;

e) replacement requests and all recorded messages exchanged with the originator of the request and / or the user;

f) currently and previously implemented policy documents.

5.5.2. Types of events recorded by MSCA / CP

The records shall include all relevant evidence in LT-MSCA / LT-CP's possession including:

a) contents of issued certificates;

b) audit journals including records of annual auditing of LT-MSCA / LT-CP's compliance with its PS;

c) currently and previously implemented certificate policy documents;

Records of all digitally signed electronic requests made by LT-MSCA / LT-CP or Service Agency personnel (CA / PA) shall include the identity of the administrator responsible for each request together with all information required for non-repudiation checking of the request for as long as the record is retained.

5.5.3. Retention period for archive

Archives shall be retained and protected against modification or destruction unlimited period.

5.5.4. Procedures to obtain and verify archive information

The LT-MSCA / LT-CP shall act in compliance with the requirements regarding confidentiality as stated in Section 9.3 and 9.4 of the Policy.
Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.
LT-MSCA / LT-CP shall make available on request, documentation of the LT-MSCA / LT-CP's compliance with the applicable PS.

A reasonable handling fee may be charged to cover the cost of record retrieval.
LT-MSCA / LT-CP shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the LT-MSCA / LT-CP's operations are interrupted, suspended or terminated.
If LT-MSCA / LT-CP services are to be interrupted, suspended or terminated, the LT-MSCA / LT-CP shall send notification to LT-CIA to ensure the continued availability of the archive. All requests for access to archived information shall be sent to the LT-MSCA / LT-CP or to the entity identified by the LT-MSCA / LT-CP prior to terminating its service.

5.6. Key Changeover

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

5.7. Compromise and Disaster Recovery

LT-MSCA / LT-CP and subcontractors shall have routines established to prevent and minimize the effects of system disasters. These routines include secure and remote backup data storage, functioning data restoration procedures etc., to be detailed in a Security Incident Handling Procedure manual, which shall be issued to administrators and auditors. Procedure documentations are not publicly disclosed. These procedures are regularly tested and updated as needed. All backup and recovery systems are tested at least once a year.
Back-up and recovery procedures for all relevant data shall be described in a Back-up and Recovery Plan.
These events are considered disasters:
a) compromise or theft of a private key and / or a master key;
b) loss of a private key and / or a master key;
c) IT hardware failure.

In case of damage or theft of LT-MSCA's private or public keys, the LT-MSCA must immediately notify LT-MSA and ERCA. The LT-MSA must immediately take appropriate measures.
If the LT-MSCA's private key is damaged or suspected to be compromised, the LT-MSCA must report the incident to the ERCA and LT-MSA without undue delay and under no circumstances exceeding 8-hour period after the detection. In the notification of incident, the LT-MSCA shall indicate the circumstances in which the breach occurred. The LT-MSA shall conduct the investigation and report the results to the ERCA.

There is effectively no recovery form a loss of the keys, so loss shall therefore be prevented using multiple backup copies of the keys, subjected to periodic controls.
Loss shall therefore be prevented using multiple backup copies. In case of IT hardware failures, IT hardware shall be recovered within 24 hours.
The LT-MSCA and LT-CP personalizers shall maintain a Business Continuity Plan detailing how they will maintain their services in the event of an incident that affects normal operations. On detection of an incident, operations shall be suspended until the level of compromise has been established. The LT-MSCA and LT-CP shall furthermore assume that technological progress will render their IT systems obsolete over time. Measures to manage obsolescence shall be defined in the Business Continuity Plan.

5.8. MSCA or CP termination

The final termination of an LT-MSCA or LT-CP is regarded as the situation where all service associated with a logical entity is terminated permanently. It is not the case where the service is transferred from one organization to another or when LT-MSCA service is passed over from an old member state key pair to new member state key pair or ERCA key.

MSA shall ensure that the tasks outlined below are carried out.
Before LT-MSCA / LT-CP terminates its services, the following procedures shall be completed as a minimum:

a) all users and parties with whom the LT-MSCA / LT-CP has agreements or other form of established relations are informed;

b) information of its termination is made publicly available at least 3 months prior to termination;

c) LT-MSCA / LT-CP terminates all authorization of subcontractors to act on behalf of the LT-MSCA / LT-CP in the process of issuing certificates.

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

5.8.1. Transfer of MSCA or CP responsibility

Transfer of LT-MSCA or LT-CP responsibility occurs when MSA chooses to appoint a new LT-MSCA or LT-CP in place of the former entity.
MSA shall ensure that orderly transfer of responsibilities and assets is carried out.
The old LT-MSCA shall transfer all root keys to the new LT-MSCA in the manner decided by the MSA.
The old LT-MSCA shall destroy any copies of keys that are not transferred.

5.8.2. MSCA / CP continuity planning

LT-MSCA / LT-CP shall have a business continuity plan. This shall include events such as:

a) key compromise;

b) data loss due to e.g. theft, fire, failure of hardware or software;

c) system failure of other kinds.

6. Technical Security Controls

6.1. Key Pair and Symmetric Key Generation and Installation

Cryptographic key generation may be performed in advance of certificate request, or in direct connection with certificate request.
Batch processing must be performed in stand-alone equipment meeting the security requirements stated above. Key integrity shall be protected until certificate issuing is performed.

6.1.1. Key Pair Generation

6.1.1.1. Member state key pair generation

The LT-MSCA shall generate the member state key pair in accordance with Annex IC Appendix 11 of the Regulation.
Member state key pairs are generated by following a key generation script by personnel in trusted roles under (at least) dual person control. The key generation ceremony is documented and logged. Key pair generation is done within a hardware security module (HSM) in which the keys are subsequently stored.

6.1.1.2. Key pair generation for card personalisation

The card personalisation key pairs are exclusively generated by the LT-CP. The LT-CP shall generate the card personalisation key pairs in accordance with Annex IC Appendix 11 of the Regulation.
Following the chapter 1.5.3 of ERCA Policy, the LT-MSA requires from LT-CP to use Common Criteria certificated tachograph cards. The LT-MSA:

- require from LT-CP that any relevant prescription mandated by the Common Criteria security certification of the tachograph card is met during the complete life cycle of the cards;
- require that if equipment private key generation is not done onboard the equipment, private key generation takes place within an HSM;
- require that if equipment can generate 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.

The generation of card personalisation key pairs is the responsibility of the LT-CP. The key generation documentation shall be handed to the LT-MSA.

6.1.1.3. Key pair generation for transport

All key transport between LT-MSCA or / and LT-CP and ERCA shall use means, media and protocols defined by ERCA Policy. If physical media is used for key transport, LT-MSA will appoint the authorized person to carry the media.
The transport key pairs for the LT-MSCA, the LT-CIA and the LT-CP are provided by the authorized person. The handling of these keys corresponds to the specification of the internal LT-MSA safety procedures.
LT-MSCA or / and LT-CP key certification request shall use KCR protocol specified in the section 4.2 of ERCA Policy.
LT-MSCA or / and LT-CP shall accept the ERCA Public Key in distribution format described in the section 4.2 of ERCA Policy.
LT-MSCA shall ensure that the KID and modulus of the keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of LT-MSCA.
LT-MSCA or / and LT-CP shall ensure that private keys will remain in HSM and will be not transported during key certification operations.
LT-MSCA or / and LT-CP shall request Motion Sensor Key from the ERCA using KDR protocol specified in the section 4.2 of ERCA Policy.

6.1.2. Private Key Delivery to Subscriber

There is no delivery of private keys to subscribers implemented. The LT-CP generates the keys, transfers them to the associated tachograph card and send the card by mail to the LT-CIA.

6.1.3. Public Key Delivery to Certificate Issuer

The LT-CP sends card Certificate Signing Requests to the LT-MSCA in order to apply card certificates for driver cards, company cards, workshop cards and control cards. The requests are subject of signed files. The LT-MSCA validates the file signature before performing the certification. The request format is agreed between LT-CP and LT-MSCA. The file transfer underlies an encrypted data transfer protocol.

6.1.4. CA Public Key Delivery to Relying Parties

The member state public key is part of the response to every correctly processed Card Certificate Signing Request. The responses are subject of signed files. The LT-CP validates the file signature before the use of the keys for the card personalisation. The response format is agreed between LT-MSCA and LT-CP. The file transfer underlies an encrypted data transfer protocol.

6.1.5. Key Sizes

Key sizes are defined in accordance with Annex IC Appendix 11 of the Regulation.
The ERCA defined the resulting minimal key length in CSM_50, depending in the length of the European Root Certificate.
The LT-MSCA and LT-CP shall generate keys in the predetermined length.

For the key lengths in specific terms the documentation regarding the "Smart Tachograph Cryptographic keys and digital certificates sample set" states an initial key length (Effective Date is January 1st, 2017, 00:00:00) of the root certificate of 256 bits. As a result of this specification, the initial size of the member state key pair (LT-MSCA_Card.PK / LT-MSCA_Card.SK) and the tachograph key pairs (Card_MA / Card_Sign) has to be as well 256 bit. The initial key size of K_M, $K_{M\text{-}WC}$ and K_{DSRC} is 128 bit.
ERCA decided to extend the key sizes of the European Root Certificate with each new validity period. Starting from 2034 key length of the European Root Certificate will be 384 bit, starting from 2051 key length of the European Root Certificate will be 512 bit.
Key lengths of the LT-MSCA and LT-CP shall grow accordingly.

6.1.6. Public Key Parameters Generation and Quality Checking

All LT-MSCA and LT-CP keys are generated by a HSM.

6.1.7. Key Usage Purposes

The member state key pair is only used for signing the tachograph card certificates.
The tachograph card private keys are used for tachograph card personalisation only.
The tachograph card shall use its Card_MA key pair exclusively to perform mutual authentication and session key agreement towards vehicle units. The Driver cards and workshop cards shall use the private key Card_Sign.SK exclusively to sign downloaded data files. The driver cards and workshop cards shall use the corresponding public key Card_Sign.PK exclusively to verify signatures created by the card.
The workshop card motion sensor key is used for workshop cards only.
The DSRC master key is only used for control cards and workshop cards.

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

The private keys and master keys shall be generated and used in a trustworthy dedicated device which:

- is certified to EAL 4 or higher in accordance with ISO/IEC 15408-1:2009, Information technology - Security techniques - Evaluation criteria for IT security, Parts 1, 2 and 3, third edition, 2008 – 2014 using a suitable Protection Profile; or
- meets the requirements identified in ISO/IEC 19790:2012, Information technology - Security techniques - Security requirements for cryptographic modules, level 3; or
- meets the requirements identified in National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, 2001, level 3.

All activities on HSMs require the presence of at least two authorized staff members of the LT-MSCA or respectively of the LT-CP.
In particular these are the generation, backup and recovery, activation and deactivation of the keys and the exchange of HSMs.
All private keys and master keys shall immediately be deactivated (such that they cannot be used) if a compromise is suspected. The LT-MSCA shall investigate the suspected compromise. If a compromise is confirmed or cannot be ruled out, the keys shall be destroyed, as well 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.

6.2.1. Keys on cards

Pursuant to this Policy the validity of equipment private key shall not exceed the validity of the certificate.
LT-MSCA_Card certificate validity time – 7 years and 1 month.

6.2.2. VU keys

Not applicable in Lithuania for the time being.

6.2.3. Equipment private key protection and storage. Cards

LT-LT-CP shall ensure that:

a) the card private key, which is generated with a safe cryptographic device, is released from this device only for inserting into the card;

b) the card private key, which is generated with a safe cryptographic device, is deleted from this device immediately after releasing and inserting into the card;

c) the selected device ensures that upon inserting of the private keys into the card they can no longer be retrieved.

6.2.4. Equipment private key protection and storage. VU

Not applicable in Lithuania for the time being.

6.2.5. Equipment private key escrow and archival

Equipment private keys shall be neither escrowed nor archived.

6.2.6. Equipment public key archival

All certified public keys shall be archived by the certifying LT-MSCA.
There aren't any private keys archived.

6.2.7. Key and Symmetric Key Transfer into or from a Cryptographic Module

The private Member State keys are not transferred from the cryptographic module, except for the creation of a secure backup on a hardware token.
Master key import and export is only allowed for back-up and recovery purposes. Export of K_{DSRC} and $K_{M\text{-}WC}$ is allowed in encrypted form only, and only in response to a valid key distribution request from LT-CP by personnel in trusted roles under at least dual person control.
The aspect of transferring private keys from the HSM is not applicable to the private keys of the Card_MA and Card_Sign key pairs. These keys are exclusively stored on the associated tachograph card.

6.2.8. Key Storage on Cryptographic Module

The private Member State keys, master keys are stored encrypted within the HSMs and are decrypted only when activated.
The aspect of key storage on Cryptographic Module is not applicable to the private keys of the Card_MA and Card_Sign key pairs. These keys are exclusively stored on the associated tachograph card.

6.2.9. Method of Activating Private Key

The private Member State key is activated by the LT-MSCA person in charge. The LT-MSCA person in charge must identify himself with a valid personal ID card. The access the CA Console application underlies additional password protection. Key activation is limited to prior certification of the public Member State key by the ERCA.
The LT-MSA, LT-MSCA and LT-MSCA PKI person in charge are present at key activation (see Section 5.2). For CA Console application access PKI operational staff members must identify themselves as well with the help of their personal smartcard and password.
The private Member State keys are activated for a key usage period of two years, as defined by the ERCA. It shall not be used after its validity period for any purpose.
The aspect of private key activation is not applicable to the private keys of the Card_MA and Card_Sign key pairs.

The corresponding public key shall have no end of validity.

6.2.10. Method of Deactivating Private Key

Activating a new private Member State key deactivates the former private key. The CA Console supports the use of only one single active private Member State key at any time. LT-MSCA no longer has access to deactivated keys.
For role representatives required for private key activation see Section 6.2.9 of this Policy.

6.2.11. Method of Destroying Private Key

As soon as private Member State keys are deactivated, they are to be destroyed on the HSM. Similarly, at the end of their life cycle, symmetric master keys are to be destroyed.
Destruction of the private keys means all copies of the key and information required to regenerate or reconstruct the key must be deleted from all locations where they ever existed.

6.3. Other Aspects of Key Pair Management

The validity periods of all LT-MSCA certificates shall comply with Annex IC Appendix 11 of the Regulation.
Upon termination of use of a Member State key pair, the public key shall be archived, and the private key shall be destroyed in such a manner that the private key cannot be retrieved.

6.3.1. Public Key Archival

The LT-MSCA public key certificates and hence the public keys shall be archived indefinitely.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The validity periods of all ERCA root certificates, ERCA link certificates and LT-MSCA certificates shall comply with Annex IC Appendix 11 of the Regulation. The following validity and usage periods are defined:
LT-MSCA_Card (private key) – 2 years;
LT-MSCA_Card (certificate) – 7 years + 1 month;
Card_MA (certificate) – driver card – 5 years;
Card_MA (certificate) – company card – 5 years;
Card_MA (certificate) – control card – 2 years;
Card_MA (certificate) – workshop card – 1 year;
Card_Sign (certificate) – driver card – 5 years + 1 month;
Card_Sign (certificate) – workshop card – 1 year + 1 month;
$K_{M\text{-}WC}$ – 17 years (Validity starts one year before EUR root key pair validity);
K_{DSRC} – 17 years (Validity starts two years before EUR root key pair validity).
Private keys shall not be used after the private key usage period is over.
The Certificate Effective Date shall indicate the starting date and time of the validity period of the certificate. It shall be the date of issuance of the certificate by the LT-MSCA.
The Card_MA and Card_Sign certificates of a given driver card or workshop card shall have the same Certificate Effective Date.
Usage time of Card_MA.SK and Card_Sign.SK shall be the same as the validity period of the corresponding certificate.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Initialization of the system operating LT-MSCA's private certification keys shall require co-operation of at least two operators, both of which are securely authenticated by the system. The CA and

personalization systems do not require formal rating as long as they fulfil all the requirements in this section.
Activation data for the HSMs storing the LT-CP keys is as well generated individually by the different authorized LT-CP staff members and in compliance with the four eyes principle.
The passphrases and parameters are then (for LT-MSCA and LT-CP keys) entered as advised by the HSM's provider.
The duration of an authentication session shall not be unlimited.
For activation of the LT-MSCA software and the system on which this software is running, user authentication shall take place using proper means (e.g. by a passphrase)

6.4.2. Activation Data Protection

LT-MSCA and LT-CP PKI Operating role owner possessing parts of one or more HSMs' activation data shall keep this data locked at all times unless there is HSM to be activated or deactivated.

6.4.3. Other Aspects of Activation Data

Persons controlling the LT-CP keys have to authenticate themselves towards the HSM. Authentication shall take place by using comparable proper means (e.g. four eyes principle).

6.5. Computer Security Controls

LT-MSCA / LT-CP shall ensure that the information system is functioning in a safe and correct manner with minimal risk of failure.
In particular:

a) the integrity of systems and information shall be protected against viruses, malicious and unauthorized software;

b) damage from security incidents and malfunctions shall be minimized using regular checks.

LT-MSCA / LT-CP system shall contain sufficient measures for enforcing the separation of roles described in this Policy above.
The security controls shall include the possibility to trace the individual acts, which can potentially affect the issuing of certificates by LT-MSCA.
All security requirements described in this Policy shall also be applied to potential subcontractors engaged in performance of LT-MSCA / LT-CP functions.

6.6. Life Cycle Security Controls

LT-MSCA / LT-CP shall use trustworthy systems and products that are protected against modification.
An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by LT-MSCA / LT-CP or on behalf of the LT-MSCA / LT-CP to ensure that security is built into IT systems.
Change control procedures shall exist for releases, modifications and emergency software fixes for any operational software.

6.7. Network Security Controls

Controls (firewalls) shall be implemented to protect LT-MSCA / LT-CP's internal network domains from external network domains accessible by third parties.
Sensitive data shall be protected when exchanged over networks, which are not secure.

6.8. Timestamping

The time and date of an event shall be included in every audit trail entry. The LT-MSCA PS shall define how time is synchronised and verffied.

7. Certificate, CRL, and OCSP Profiles

The tachograph certificates are only for use within the tachograph system.

7.1. Certificate Profile

All certificates shall have the profile specified in Annex 1C, Appendix 11 and Appendix 1.

7.2. CRL Profile

The LT-MSCA tachograph card certificates described in the document on hand are never revoked or suspended. Therefore, no CRL will be kept, and no CRL is to be published.
For the ERCA, the status of all certificates issued can be found on the website https://dtc.jrc.ec.europa.eu/.

7.3. OCSP Profile

No OCSP shall be used.

8. Compliance Audit and Other Assessment

LT-MSA is responsible for ensuring that audit of LT-MSCA and LT-CP takes place. LT-MSA shall officially approve the audit results. LT-MSA shall notify the audit results and shall present audit report in the English to ERCA.

8.1. Frequency or Circumstances of Assessment

The MSA shall perform the first audit within 12 months of the start of the operations covered by the approved policy.
MSA shall have the right to carry out unplanned audit subject to notification.
Before the start of the operations covered by this Certification Policy, the LT-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 Certification Policy on hand.

8.2. Identity / Qualifications of Assessor

MSA shall carry out the audit itself or hire other institution for audit purposes. MSA shall accept audit conducted by a competent institution.
The auditor assigned has to be an independent company carrying out audits in accordance with the statutory and regulatory provisions.
The auditor has to be accredited by the accreditation body to perform the specific audits. In particular, 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.

Any person selected or proposed to perform a compliance audit has to be approved by LT-MSA in upfront.

8.3. Assessor's Relationship to Assessed Entity

The assessor shall be independent and not connected to the organisation being the subject of the audit. The assessor may not be a participant in the assessed organization and / or a member of the management body;
The assessor cannot be related to the family, close kinship, or affinity relationship with the assessed organization.
In addition to the foregoing prohibition on conflicts of interest, the assessor has a contractual relationship with the LT-MSA or the LT-MSCA for the performance of the audit, but otherwise, the

auditor shall be independent. The auditor shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4. Topics Covered by Assessment

The audit shall cover compliance to the Policy on hand and the associated procedures and techniques documented by the organisation to be audited. The scope of the compliance audit shall be the implementation of the technical, procedural and personnel practices described in these documents.
Some areas of focus for the audits shall be:

- identification and authentication
- operational functions/services
- organisation and management
- personnel training
- 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.
The audit shall produce the audit report, which defines the corrective actions with the implementation schedule, needed to fulfil requirements in this Policy.
The audit shall also consider the operations of any Service Agencies.

8.5. Actions Taken as a Result of Deficiency

If deficiencies or irregularities are found in the audit MSA shall take appropriate action depending on their severity.
When an audit finds no evidence of non-conformity, the next audit may be performed within 24 months.
In particular, the LT-MSA and LT-MSCA agree with the auditor on the necessary actions and time schedules to correct / eliminate the deficiencies identified. They will jointly see to the initiation and successful completion of the resulting tasks.
After the corrective actions have been fulfilled, a follow-up audit shall take place within 12 months.

8.6. Communication of Results

Results of the audits, following the security status level, shall be allways communicated to LT-MSA. Actual audit reports shall not be available to other legal persons except on need-to-know basis.
The LT-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. If requested by the ERCA, the LT-MSA shall send the full results of the compliance audit to the ERCA.

9. Other Business and Legal Matters

The provisions of the present Policy shall be interpreted in accordance with the legal acts of the European Union and the Republic of Lithuania.
The issues of confidentiality of information are governed by:

a) 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)

b) Law of the Republic of Lithuania on legal protection of personal data;

c) Law of the Republic of Lithuania on protection of copyrights and neighbouring rights;

d) Resolution No. 716 of 24 July 2013 of the Government of the Republic of Lithuania on general electronic information security requirements for the secure document describes the content of the

guidelines and the State information systems, registers and other information systems and electronic information classification importance of guidelines for approval of the description;

e) Lithuanian standard LST ISO / IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements (identical ISO/IEC 27001:2013), 2 December 2013.

9.1. Fees

The tax obligations are laid down in the agreement between the parties.

9.2. Financial Responsibility

Financial commitments are laid down in the agreement between the parties.

9.2.1. MSCA and CP asset management

LT-MSCA shall ensure that physical access to reliable systems and especially sensitive services is controlled and the physical risk to the assets is minimized.
In particular:

- physical access to the equipment related to key, certificates generation and management of termination is granted only to properly identified and authorized persons;
- control means are implemented in order to avoid:
- loss, breaking or damage to the assets and business interruptions;
- damage or theft of information and information processing equipment.
- equipment related to key, certificates generation, management of suspending and termination is used in a secure environment, which grants physical protection to the systems and services against breach as a result of unauthorized access to the systems or data;
- physical security shall be installed by developing clearly identified key generation, certificate generation and termination management security parameters.

Physical and environment security control measures in order to protect the system resources of the equipment storage facilities, the resources of the system itself and the equipment which is used to support work thereof shall be implemented. LT-MSCA PS shall define physical access control, security against natural disasters, fire security factors, break downs of supporting means, security against theft, inbreak and entry, emergency data recovery, etc.

9.3. Confidentiality of Business Information

All private and secret keys used and handled within the LT-MSCA / LT-CP operation under this Policy are to be kept confidential.
Audit logs and records shall not be made available except for the cases specified by laws when this is required by competent law enforcement institutions.
Any corporate information held by the LT-MSCA, the LT-CP or subcontractors / Service Agencies that is not appearing on issued cards or certificates 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, except for the cases specified by laws when this is required by competent law enforcement institutions.
Confidential data shall comprehend at least:

- Personal data (i.e., employees, components manufacturers or representatives of ERCA);
- Private keys;
- Symmetric master keys;
- Organizational or production data;
- Audit logs (unless required by law, regulation or CP or CPS);
- Detailed documentation regarding the PKI management;
- Internal and external assessment results and reports.

9.4. Privacy of Personal Information

Certificates are not considered confidential.
Personal identification information or other personal or corporate information provided on the card is not considered confidential except for the cases specified by laws.
Any personal information held by the LT-MSCA, the LT-CP or subcontractors / Service Agencies that is not appearing on issued cards or certificates 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, except for the cases specified by laws when this is required by competent law enforcement institutions.

9.5. Intellectual Property Rights

Rights to all Intellectual Property Objects, such as those created in the Policy Execution Process, if any, belong to the maximum scope of MSA, are permitted by legal norms and in accordance with the Republic of Lithuania Law on Copyright and Related Rights.

9.6. Representations and Warranties

The LT-MSCA, LT-CP undertakes to follow the provisions of the ERCA Policy as well as of this Policy and on hand.
The card holder undertake to follow the provisions of the Lithuania laws in particular according to the specifications for tachograph card usage.
Any service providers, appointed by the LT-MSA, the LT-MSCA or the LT-CP must undertake to comply with the ERCA Policy as well as of this Policy on hand.

9.7. Disclaimers and Warranties

The LT-MSA disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaim any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties. Warranties and obligations of the LT-MSCA and the LT-CP to the LT-MSA are subject to the underlying contracts and agreements. All other warranties by any of these parties identified are excluded.

9.8. Limitations of Liability

The liability of the LT-MSA, the LT-MSCA, LT-CIA and the LT-CP is limited to the extent permitted by applicable law.
In particular, the LT-MSA, the LT-MSCA, LT-CIA and the LT-CP are not liable for:

- all damages resulting from the usage of certificates or key pairs in any other way than defined in this document, in the PKI instructions or stipulated in the certificate itself;
- all damages caused by force majeure;

The LT-MSA, the LT-MSCA, LT-CIA and the LT-CP and their staff members are liable for damages caused by a breach of his due diligences (e.g. handing over personal token and PIN to somebody else).

9.9. Indemnities

No stipulation.

9.10. Term and Termination

The policy comes into force on the day following its approval by the EU and national institution.

9.11. Individual Notices and Communications with Participants

Any information, requests for clarification, complaints, communications or other correspondence between parties shall be in writing and signed by a qualified electronic signature. Documents addressed to LTSA and signed by electronic signature are sent by email. by mail – ltsa@ltsa.lt.

9.12. Amendments

9.12.1. Items that may change without notification

The only changes that may be made to this Policy without notification are:
a) editorial corrections;
b) changes to the contact details.

9.12.2. Amendments with notification

9.12.2.1. Notice

Any item in this Policy may be changed with 90 days notice to ERCA.
Changes to items which, in the judgment of MSA, will not materially impact a substantial majority of the users or relying parties using this Policy may be changed with 30 days notice.

9.12.2.2. Comment period

Impacted users may file comments with MSA within 15 days of original notice.

9.12.2.3. Whom to inform

Information about changes to this Policy shall be sent to:
a) ERCA;
b) LT-MSCA and LT-CP including Service Agencies.

9.12.2.4. 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.

9.12.3. Changes requiring a new Certification Policy approval

If a policy change is determined by MSA to have a material impact on a significant number of users of the Policy, MSA shall submit the revised National Certification Policy to the Commission for approval.

9.13. Dispute Resolution Procedures

The policy is implemented and the parties' disputes arising from its execution are settled by agreement between the parties. Without resolving the disputes by mutual agreement, the dispute is referred to the European institutions for decision.

9.14. Governing Law

Policy implementation, development, interpretation and validity are governed by EU legislation and ERCA policy.

9.15. Compliance with Applicable Law

The policy is in line with Regulation (EU) No. 165/2014 of the European Parliament and of the Council, as well Commission Implementing Regulation (EU) 2016/799. If the Policy is against EU legislation, EU legislation applies.

9.16. Miscellaneous Provisions

9.16.1. Equipment management

The equipment in the digital tachograph system is defined as:
a) cards;
b) vehicle units (VU);
c) motion sensors.
The equipment in the digital tachograph system is handled and managed by several roles:
a) LT-CIA (card registration, renewal, etc.);
b) LT-MSCA (generation of certificates, keys);
c) LT-CP (visual and electronic personalization, distribution, deactivation of cards);
MSA:
a) controls the quality of the functions performed by the entities involved in the management of digital tachograph system;
b) approves PS of LT-CIA, LT-MSCA and LT-CP.
LT-CIA:
a) accepts card applications;
b) handles identity data of cardholders (accepts applications, verifies the submitted data; verifies the identity of the applicant);
c) transfers the data of verified identity of cardholders to LT-CP;
d) issues personalized cards;
e) transfers PIN codes to workshop cardholders;
f) maintains white and black lists of the cards;
g) registers cards and stores data related to issuing of cards.
LT-CP:
a) records data on verification of cardholders' identity and other required data into the cards;
b) record keys and certificates into the cards;
c) prints the required data on the cards;
d) transfers PIN codes of the personalized cards and workshop cards to LT-CIA.
LT-MSCA:
a) generates and registers member state keys;
b) generates and registers card certificates;
c) registers European keys and certificates;
d) submits member state keys to ERCA for certification;
e) transfers card certificates to LT-CP.

9.16.2. Cards

9.16.3. Quality control

LT-MSCA and LT-CP shall ensure that only type approved cards, according to the Regulation, are personalized in the digital tachograph system (see also Section 9.16.9 of the Policy).

9.16.4. Accepting applications for card

LT-CIA performs card issuing function. LT-CIA informs the users about the conditions regarding the use of a card. This information shall be available in the Lithuanian and English languages.
The user shall, by applying for a card, and accepting delivery of the card, accept the conditions regarding the use of the card.
More detailed information shall be provided in the LT-CIA PS.

9.16.4.1. User application for a card

The form of application for a card shall be set by MSA. The application for a card shall contain the data, which ensures correct identification of the user.

9.16.4.2. Data defining a Driver card

Data defining a Driver card is:
a) personal data (name, surname, date of birth);
b) personal photo and signature;
c) number of the driving license.

9.16.4.3. Data defining a Workshop card

Data defining a Workshop card is:
a) data related to the workshop (name, address of the workshop);
b) personal photo and signature;
c) data related to the holder of the card (name, surname).

9.16.4.4. Data defining a Control card

Data defining a Control card is data related to the controlling institution (name, address of the controlling institution).

9.16.4.5. Data defining a Company card

Data defining a Company card is data related to the company (name, address, code of the company).

9.16.4.6. Obligation

User, when submitting an application for a card to LT-CIA, shall oblige that:
a) agrees to the conditions regarding use of the card;
b) from the time of card acceptance and throughout the operational period of the card, until LT-CIA is notified otherwise by the user:
- will not allow unauthorized person to have access to the user's card;
- all information given by the user to the LT-CIA relevant for the information in the card is true;
- the card is being conscientiously used in consistence with usage restrictions for the card.

9.16.4.7. Terms of CIA approval applicable to driver card

Driver card is only issued to natural persons permanently residing in the state of application for a driver card.
LT-CIA shall make sure that the person applying for a driver card does not have a valid driver card issued in another member state and has a valid driver's license of the appropriate category.

9.16.5. Renewal of cards

Workshop card shall be issued only to the staff of approved workshops.
Company card shall be issued only to the company engaged in hauling activities.
Control cards shall be issued only to the officers of competent control institutions.
The LT-CIA shall establish routines to remind the user of pending expiration.
Applications for renewal shall be submitted in the same procedure as these for a new card (see Section 9.16.4 of the Policy).
The LT-CIA issues a new card within 15 (fifteen) working days from the date of receiving a complete application for a driver, company or control card renewal and within 5 (five) working days from the date of receiving a complete application for a workshop card renewal.

9.16.5.1. Driver cards

The driver shall submit application for a renewal card not later than 15 (fifteen) days prior to card expiration (Article 28(1) of the Regulation No. 165/2014).
LT-CIA shall issue a new card before the current card expires if the application for a renewal card was submitted on time (Article 28(4)(3) of the Regulation No. 165/2014).

9.16.5.2. Workshop cards

The user shall apply for a renewal card at least 15 (fifteen) days prior to card expiration.
LT-CIA shall issue a new card within 5 (five) working days from the date of application (Article 25(2) of the Regulation No. 165/2014).

9.16.5.3. Company cards

The user shall apply for a renewal card at least 15 (fifteen) days prior to card expiration.
LT-CIA shall issue a new card before the current card expires if the application for a renewal card was submitted on time.

9.16.5.4. Control cards

The user shall apply for a renewal card at least 15 (fifteen) days prior to card expiration.
The LT-CIA shall issue a new card before the current card expires if the application for a renewal card was submitted on time.

9.16.6. Card exchange due to the change of administrative data

Where the driver's data (name, surname, personal identification code, date of birth) or company registration data (name, code, address of the company) changes an application for card exchange shall be submitted.
LT-CIA shall upon delivery of the new card take possession of the previous card and send it to LT-CIA of origin (Article 30(3) of the Regulation No. 165/2014).
Application for card exchange due to changed Member State of driver's residence and driver's data (name, surname, personal identification number, date of birth) shall otherwise follow the rules for new card issuing.
The LT-CIA issues a new card within 15 (fifteen) working days from the date of receiving a complete application for a driver, company or control card exchange and within 5 (five) working days from the date of receiving a complete application for a workshop card exchange.

9.16.7. Replacement of lost, stolen and malfunctioning cards

Stolen and lost cards shall be put on a blacklist available to competent authorities in all member states.
Malfunctioning cards shall be delivered to the issuing LT-CIA. The cards are withdrawn and put on a blacklist of cards. The cards are physically and electronically cancelled.
If a card is lost, stolen or malfunctioning, the user shall apply for a replacement card to LT-CIA within 7 (seven) days. (Article 29(4) of the Regulation No. 165/2014)
Provided the user follows the above requirements, the LT-CIA shall issue a replacement card with new keys and certificate within 5 (five) working days from receiving a complete application for replacement card. (Article 29(4) of the Regulation No. 165/2014)
The replacement card shall inherit the time of validity from the original card. If the replaced card has less than six months of remaining validity, LT-CIA may issue a renewal card instead of a replacement card (Section 7 of Annex 1C).

9.16.8. Registration of applications

LT-CIA shall perform registration of applications in the database.

9.16.9. Card personalization

Cards are personalized both visually and electronically. Where this process is carried out by subcontractors / Service Agents, the overall responsibility of LT-MSCA / LT-CP shall not be diminished.

9.16.9.1. Visual personalization of cards

Cards shall be visually personalized according to section 4 of Annex 1C).

9.16.9.2. User data entry

User's data shall be inserted in the card according to the structure in section 4, Appendix 2, Annex 1C, depending on card type.

9.16.9.3. Key entry

The private key shall be inserted in the card in the physically safe environment. The process shall be controlled. The environment of key generation must be safe and ensure that no person can get control of the generated private key.

9.16.9.4. Certificate entry

The certificate shall be inserted in the card before distribution of the card to the user.

9.16.9.5. Quality control

Special documented routines shall exist to ensure that the visual information on the cards and the electronic information in issued certificates and cards matches each other and matches the identity of the cardholder.
The routines shall be described in the LT-CP PS.

9.16.9.6. Withdrawing (destruction) of non-distributed cards

All cards that are damaged or for other reasons are not finalized and distributed during personalization shall be physically and electronically destroyed (withdrawn).
All destroyed (withdrawn) cards shall be registered in the blacklist of cards.

9.16.10. Card registration and data storage

LT-CP is responsible for keeping track of which card and card number is given to which user. The data shall be transferred from LT-CP to LT-CIA for the database of cards.

9.16.11. Card distribution to the users

LT-CIA shall be in charge of card distribution to the users.
The personalization shall be scheduled so as to minimize the time that the personalized card requires safekeeping before delivery to the user. Cards shall be stored in a special safe box.
The personalized cards shall always be kept separated from the non-personalized cards.
The personalized cards shall be immediately distributed to the users in order to mitigate the risk of their loss.
At the point of delivery of the card to the user, the user shall produce documented evidence of his identity.
The reception of the card shall be acknowledged by the user's signature.

9.16.12. Generation of authentication codes (PIN)

The provisions of this section apply only to workshop cards.
Workshop cards shall have a PIN code, used to authenticate the card (Appendix 11 of Annex 1C).
PIN codes shall consist of at least 4 (four) digits (Appendix 13 of Annex 1C).

9.16.12.1. PIN code generation

PIN codes shall be generated in a secure environment, securely transferred to workshop cards, and direct-printed to PIN-envelopes. PIN codes shall never be stored on a computer system in a manner that allows connection between PIN and the specific user. The PIN generation system shall meet the requirements of ITSEC E3, CC EAL4 or equivalent security criteria.

9.16.12.2. PIN code distribution

PIN codes shall be handed to the user personally.
PIN codes and workshop cards shall not be delivered to the specific user in the same envelope. These safety requirements are needed to ensure that the PIN code and the workshop card are not connected until they are distributed to the specific user.

9.16.13. Deactivation of cards

The card and the keys residing therein shall be deactivated permanently. A decision of deactivation shall be taken by LT-MSA or LT-CIA; the actual operation shall be carried out by LT-CIA or a selected subcontractor / Service Agency.
Deactivation of cards shall take place in equipment suitable for the operation. It shall be verified in the deactivation process that card functions and the keys are destroyed. The card shall also be visually destroyed.
Deactivation of cards shall be registered in the card database. The deactivated card number shall be put on the list of destroyed cards.

9.17. Other Provisions

9.17.1. General aspects of CP / MSCA, subcontractors and service agencies

Equipment (Card) initialization 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. Personalization system shall be operated by minimum two persons. A log shall be kept of the entries and the actions in the system.
The key may not leave the secure system.
No sensitive information related to the card personalization may leave the secure environment.
Organizations (subcontractors / Service Agencies) that perform key generation and card personalization on behalf of more than one member state shall do this in a clearly separate process for each of these. A log shall be kept of each individual process and the relevant MSA shall have access to this.
LT-MSCA / LT-CP / Service Agencies: the log shall contain references to the corresponding equipment numbers and certificates. The relevant MSA shall have access to the logs.
LT-MSCA / LT-CP / subcontractors / service agencies: the log shall contain references to the corresponding equipment numbers and certificates.