Latvian MSA Policy

for

the Digital Tachograph System

History of the versions of the Latvian MSA Policy for the Digital Tachograph System

Version	Date	Comments
1st version	July 21, 2005	Approved by Digital Tachograph Root Certification Authority Traceability and Vulnerability Assessment Unit European Commission Joint Research Centre, Ispra Establishment
2nd version	September 26, 2011	The following points amended by Road Transport Administration: 1.1; 1.2; 1.3; 3; 11.1.
3th version	September 7, 2016	The following points amended by Road Transport Administration: 1; 1.1; 1.2; 3.2.2; 5.1.4.

Table of Contents

1 Introduction

This document is the National MSA Policy of Latvia for the Digital Tachograph System.

This National MSA Policy is in accordance with:

- Council Regulation (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport
- Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport
- Regulation (EU) No 165/2014 of the European Parlament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport
- Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
- Guideline and Template National CA policy, version 1.0
- European Digital Tachograph Common Security Guideline, Version 1.0
- Digital Tachograph System European Root Policy, Version 2.1

Abbreviations used in this document are specified at end of this document, in chapter 14.2.

1.1 Responsible organization

The responsible body for this National MSA Policy is the Road Transport Administration of Latvia acting as the Member State Authority (MSA), the Member State Certification Authority (MSCA) and the Card Issuing Authority (CIA).

Road Transport Administration
30 Valnu str.
Rīga, LV-1050
Latvia

MSCA may subcontract its technical functionality to the Service Agency acting as Certificate Service Provider (CSP).

CIA may subcontract parts of processes to subcontractors (Service Agencies).

The use of Service Agencies in no way diminishes the MSA's overall responsibilities for these processes.

The appointed Service Agency for CSP, the detailed activities of which are specified in the Certificate Practice Statement (CPS), shall be Trüb Baltic AS.

Trüb Baltic AS
Laki 5, 10621, Tallinn, Estonia

The appointed Service Agency for Card Personalizer (CP), the detailed activities of which are specified in the Card Personalize Practice Statement (CP PS), shall be Trüb Baltic AS.

Trüb Baltic AS
Laki 5, 10621, Tallinn, Estonia

1.2 Approval

This National MSA Policy is approved by :
Digital Tachograph European Root Certification Authority – TP 361
European Commission
Joint Research Centre
Directorate E- Space, Security & Migration
Cyber & Digital Citizens' Security Unit
Via Enrico Fermi, 2749
I-21027 Ispra (VA), Italy
at October 15, 2011

1.3 Availability and contact details

The National MSA Policy is publicly available at http://www.atd.lv

Questions concerning this National MSA Policy should be addressed to:

Road Transport Administration
Valnu street 30, Riga, LV-1050, Latvia
Phone: (371) 67280485
Fax: (371) 67821107

2 Scope and applicability

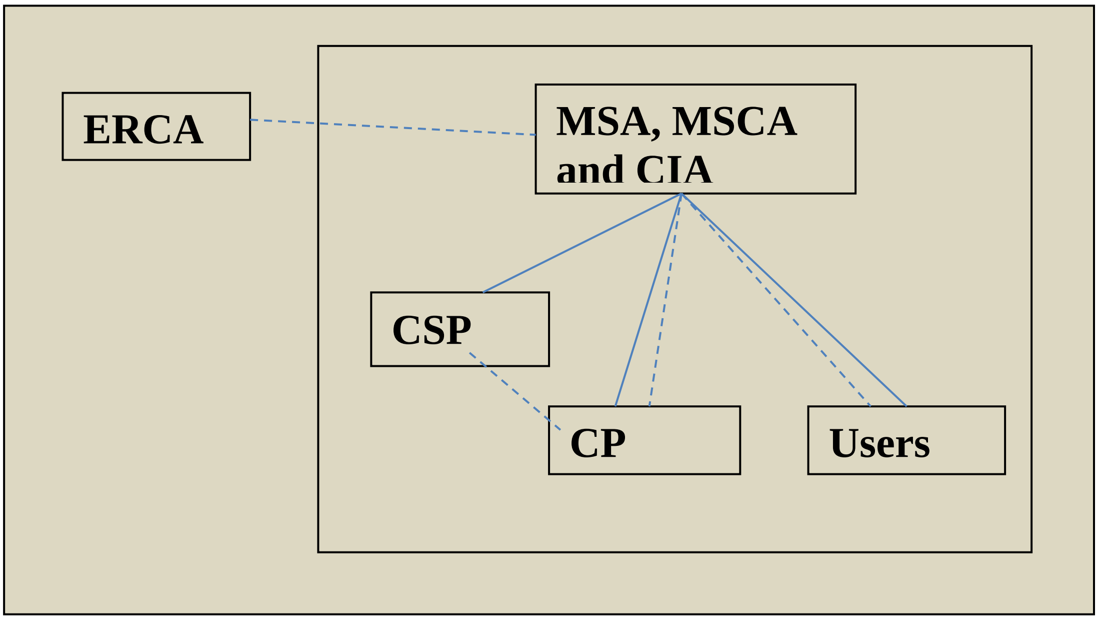
The National MSA Policy is valid for the Digital Tachograph system only.

The keys and certificates issued by the MSCA are only for use within the Digital Tachograph system.

The cards issued by the CIA are only for use within the Digital Tachograph system.

3 General provisions

This section contains provisions relating to the respective obligations of MSA, CIA, MSCA, CSP, CP, Service Agencies and users, and other issues pertaining to law and dispute resol



Hierarchy, relations and dataflow in the National Digital Tachograph system

Abbreviations and symbols used in picture:

ERCA	European Root Certification Authority
MSA	Member State Authority
MSCA	Member State Certification Authority
CSP	Certificate Service Provider
CIA	Card Issuing Authority
CP	Card Personalizer
────────	Responsibility hierarchy
– – – – – – – –	Data, information or card flow

More abbreviations in section 14.2

3.1 Obligations

This section contains provisions relating to the respective obligations of:

- MSA
- MSCA
- CIA
- CSP
- CP
- Service Agencies
- Users (Cardholders)

3.1.1 MSA obligations

With regard to this MSA Policy, the MSA has the following obligations.

The MSA shall:

a) Maintain the National MSA Policy

b) Appoint an MSCA and CIA;

c) Audit the MSCA, CIA, CSP, CP, including Service Agencies;

d) Inform the appointed parties and Service Agencies about this policy;

e) Let this policy be approved by the ERCA.

3.1.2 MSCA obligations

The MSCA shall:

a) Follow this National MSA Policy;
b) Publish CPS that includes a reference to this National MSA Policy, to be approved by the MSA;
c) Oversee that the ERCA Root Policy requirements will be implemented in MSCA certification requests;
d) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National MSA Policy, in particular to bear the risk of liability damages as stated in chapter 3.2.

The MSCA shall ensure that all requirements for the MSCA, as detailed in this policy, are implemented.

The MSCA has the responsibility for conformance with the procedures prescribed in this policy, even when the MSCA's technical functionality is undertaken by a subcontractor, Service Agency (CSP). The MSCA is responsible for ensuring that the Service Agency provides all its services consistent with its (CPS) and the National MSA Policy.

3.1.3 CIA obligations

The CIA shall:

a) Follow this National MSA Policy;

b) Publish (CP PS) that includes reference to this National MSA Policy, to be approved by the MSA;

c) Ensure that correct and relevant user information from the application process is passed to the CP;

d) Inform the users of the requirements in this policy related to the use of the system;

e) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National MSA Policy, in particular to bear the risk of liability damages as stated in chapter 3.2.

3.1.4 CSP obligations

The CSP shall:

a) Ensure that correct certificates are passed to the CP;

b) Maintain confidentiality of the MSCA private key;

c) Follow this National MSA Policy;

d) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National MSA Policy, in particular to bear the risk of liability damages as stated in chapter 3.2.

3.1.5 CP obligations

The appointed CP shall:

a) Follow this National MSA Policy;

b) Ensure that all requirements on it, as detailed in this policy, are implemented.

The CP has the responsibility for conformance with the procedures prescribed in this policy, even when the CP functionality is undertaken by subcontractor, Service Agency.

3.1.6 Service Agency obligations

Service Agencies, when used to operate services covered by this policy, have obligations towards the MSA, MSCA and CIA according to contractual agreements. Despite of such agreements, MSA retains full responsibility for any Tachograph services, covered in this document.

3.1.7 Cardholder obligations

The CIA shall oblige, through agreement (see 5.1.2.2), the user (or user's organization) to fulfil the following obligations:

3.1.7.1 All card types

a) accurate and complete information is submitted to the CIA in accordance with the requirements of this policy, particularly with regards to registration;

b) the keys and certificate are only used in the Tachograph system;

c) the card is only used in the Tachograph system;

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

e) a user may only under very special, and duly justified, circumstances have both a workshop card and a company card;

f) a user shall not use a damaged or expired card;

g) a user shall not tamper with or attempt to modify cards in any way;

h) the user shall notify the CIA without any reasonable delay if any of the following occurs up to the end of the validity period indicated in the certificate:

- the equipment private key or card has been lost, stolen or potentially compromised; or
- the certificate content is, or becomes, inaccurate.

3.1.7.2 Driver card

a) a user may have only one valid driver card;
b) the user may only use his/her own keys, certificate and card;

3.1.7.3 Workshop card

a) a user must protect his/her PIN-code
b) the card should not leave the premises of workshop unless required by installation, calibration and repair operations

3.1.8 VU manufacturers' obligations (role as personalization organization)

Not applicable in Latvia for the time being or in the foreseeable future.

3.1.9 Motion Sensor manufacturers' obligations (role as personalization organization)

Not applicable in Latvia for the time being or in the foreseeable future.

3.2 Liability

3.2.1 MSCA, CPS, CP and liability towards the MSA and the CIA

The MSCA, CPS, CP bear the responsibility for proper execution of their tasks, even if some or all of the tasks are outsourced to Service Agencies. If the MSCA or CIA intends to subcontract to other parties, they shall inform the MSA of such intentions beforehand.

The MSCA, CIA is liable for damages resulting from failures to fulfil these obligations only if it has acted negligently. If the organization has acted according to this National MSA Policy and the corresponding PS, it shall not be considered to have been negligent.

The MSCA, CSP, CP does not carry any liability towards end users, only towards the MSA and CIA.

Any liability issues towards end users are the responsibility of the MSA or CIA.

3.2.2 MSA and CIA liability towards end users and related parties

The MSA is liable for correct implementation of Regulation (EEC) no. 3821/85, as amended by Regulation (EC) no. 2135/98 and its Annex IB and Regulation (EU) No 165/2014. This means particularly that the MSA is liable for ensuring that:

a) the certificate is created in accordance with the provisions of the Regulation and this MSA Policy;

b) the certificate contains all the information required for the Tachograph certificate at the time of issuance and in particular, that data of the cardholder corresponds to the information in the application.

CIA is liable for verifying that in the certificate the data of the cardholder corresponds to the information in the application.

The MSA or the CIA is not liable for damages towards end users and related parties caused by:

1) false or incomplete information given by the applicant unless the MSA or the CIA is proven to have been negligent;

2) use of the certificate, either in or out of the scope of the Regulation;

3) revealing of PIN code unless it is directly caused by acts of the MSA or the CIA;

4) malfunctioning of the VU, telecommunications or similar, which hinders the use of certificate within the Tachograph system.

The MSA or the CIA is never liable for indirect financial loss or other indirect damages towards end users, related parties or their contracting parties.

In addition, Tachograph cards, keys and certificates are only for use within the Tachograph system. Any other certificates present on Tachograph cards are in violation of this policy, and hence neither the MSA nor the CIA carries any liability in respect to any such violation.

3.2.3 Corresponding legislation

Liability of damages shall be decided in accordance with Latvian national Law on Administrative Procedure (published: Latvijas Vēstnesis 14.11.2001).

3.3 Interpretation and enforcement

3.3.1 Governing law

Provisions of this Policy shall be interpreted according to the Latvian legislation.

3.4 Confidentiality

Confidentiality is restricted according to Directive 95/46/EC and Law on Physical Person Data Protection (published: Latvijas Vēstnesis 06.04.2000).

3.4.1 Types of information to be kept confidential

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

All private and secret keys used and handled within the MSCA or CP operation under this National MSA Policy are to be kept confidential.

Audit logs and records shall not be made available as a whole, except as required by law.

3.4.2 Types of information not considered confidential

Certificates are not considered to be confidential.

Identification information or other personal or corporate information appearing on cards and in certificates is not considered to be confidential, unless statutes or special agreements so dictate.

4 Practice Statement (PS)

The MSCA, CIA, CSP, CP shall have practice statements describing practices and procedures used to address all the requirements identified in this National MSA Policy. The MSA shall approve such PS.

In particular:

a) The PS shall identify the obligations of all the external organizations supporting the MSCA and CIA services including the applicable policies and practices.

b) The PS shall be made available to the MSA, to users of the Tachograph system, and to related parties (e.g. control bodies);

However, the MSCA/CIA is not generally required to make all the details of its practices public and available for the users.

c) The management of the MSCA/CIA has responsibility for ensuring that the PSs are properly implemented.

d) The MSCA/CIA shall define a review process for the PS;

e) The MSCA, CIA, CSP, CP shall give due notice of changes it intends to make in its PS and shall, following approval, make the revised PS immediately available.

5 Equipment management

The equipment in the Tachograph system is defined as:

- Tachograph cards
- Vehicle units
- Motion Sensors

Due to the fact that Vehicle units or Motion Sensors are not manufactured in Latvia, this section of Policy only covers Tachograph cards.

The equipment is handled and managed by several roles:

- CIA (cancellation of cards, card registration, renewal, etc.);
- MSCA (Motion Sensor keys);
- CP (visual and electronic personalization, keys);
- CSP (certificates).

The following functions are carried out by the MSA:

- Quality control (type approval). The actual work will be carried out by Service Agency appointed to role of CP;
- Practice statements approvals.

The following functions are carried out by the CIA:

- Applications for cards;
- Application approval registration;
- Provision of personalization data to CP;
- Data storage (DB);
- Exchange of information with other Member States;
- User registration;

- Card issuing to users;
- Handling of lost and found cards;

The following functions are carried out by the MSCA:

- Generation of MSCA keys for Latvia and managing interface with the ERCA certification process.

The following functions are carried out by the CSP

- Generation of certificates for cards upon requests from CP;
- Storing the issued certificates in DB;
- Maintaining the security of the MSCA keys.

The following functions are carried out by the CP

- Quality control (test card samples);
- Sending certificate requests to CSP;
- Key and certificate insertion;
- Personalization of cards;
- Capability to Card functionality verification;
- Card delivery to the CIA
- Workshop card and PIN delivery to the CIA.

5.1 Tachograph cards

5.1.1 Quality control – MSA/CP function

The MSA/CP shall ensure that only type approved cards, according to the Regulation, are personalized.

5.1.2 Application for card – handled by the CIA

The CIA shall inform the user of the terms and conditions regarding use of the card. This information shall be available at least in Latvian and English.

The user shall, by applying for a card, and accepting delivery of the card, accept the terms and conditions.

5.1.2.1 User application

Applicants for a Tachograph card shall submit an application in a form to be determined by the CIA. As a minimum, the application shall include the data needed to ensure the correct identification of the user. For company, workshop and control cards, the necessary identity of the legal organization for which card is applied, shall be included.

The following information is required for issuing a card. Unless gathered from other sources, it should be included in the application:

Driver card specific:

- Full name
- Date and place of birth
- Place of residence
- National registration number (if available)
- Postal address

- Photo
- Driving license number

Workshop card specific:

Workshop cards shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

full name and legal status of the associated legal person or other organizational entity;

full name (including surname, given names and national registration number and photo) of the cardholder.

Control card specific:

Control cards shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

full name and legal status of the associated legal person or other organizational entity;

optional full name and photo (including surname, given names and national registration number) of the cardholder, minimum is unit identification;

Company card specific:

Company cards shall be issued to individual representatives of companies owning or holding vehicles fitted with a Digital Tachograph and who can provide evidence of:

full name and legal status of the associated legal person or other organizational entity;

any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;

the user's association with the legal person or other organizational entity;

optional full name (including surname, given names and national registration number) of the cardholder.

5.1.2.2 Agreement

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

- the user agrees to the terms and conditions regarding use and handling of the Tachograph card;
- the user agrees to, and certifies, that from the time of card acceptance and throughout the operational period of the card, until CIA is notified otherwise by the user:
    - user will not allow unauthorized person to have access to the user’s card;
    - all information given by the user to the CIA relevant for the information in the card is true;
    - the card is being conscientiously used in consistence with usage restrictions for the card.

5.1.2.3 CIA terms of approval - Driver card specific

A Driver card shall only be issued to individuals having permanent residence in the country of application.

The CIA shall ensure that the applicant does not have a valid Driver card issued in Latvia or in another Member State.

The CIA shall ensure that the applicant for a Driver card has a valid driving license of appropriate class.

5.1.2.4 CIA terms of approval – Workshop card specific

Workshop card shall only be issued to a workshop having valid workshop accreditation for the Digital Tachograph.

5.1.2.5 CIA terms of approval – Control card specific

Control card shall only be issued to a party nominated as an official control body.

5.1.2.6 CIA terms of approval – Company card specific

Company card shall only be issued to a company registered according to the national legislation.

5.1.3 Validity period of cards

Workshop cards shall be valid for no more than **one** year from issuance.

Driver cards shall be valid no more than **five** years from issuance.

Company cards shall be valid no more than **five** years from issuance.

Control cards shall be valid no more than **two** years from issuance.

The CIA shall establish routines to remind the user of a pending expiration.

An application for renewal shall follow the procedures described in section 5.1.2.

5.1.4 Card renewal – handled by the CIA

The user shall apply for a renewal card at least **15** working days prior to card expiration.

If the user complies with the above rule, the CIA shall issue a new card before the current card expires.

5.1.5 Card update or exchange – handled by the CIA

A user who changes country of residence may request to have his/her driver card exchanged. If the current card is valid, the user shall only show proof of Latvian residence in order to have the application granted.

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

Card exchange due to changed country of residence shall otherwise follow the rules for new card issuing (section 5.1.2).

5.1.6 Replacement of lost, stolen, damaged and malfunctioning cards – handled by the CIA

If a card is lost or stolen, the user shall report this to CIA.

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

Damaged and malfunctioning cards shall be delivered to the issuing CIA, by whom they shall be visually and electronically cancelled, and put on a blacklist

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

Provided that the user follows the above requirements, the CIA shall issue a replacement card with new keys and certificate within 5 working days from receiving a complete application.

The replacement card shall inherit the time of validity from the original card. If the replaced card has less than three months remaining validity, the CIA may issue a renewal card instead of a replacement card.

5.1.7 Application approval registration – handled by the CIA

The CIA shall register the approved applications in a database. This data shall be made available for the CP, which uses the information as input to the certificate generation and card personalization processes.

5.1.8 Card personalization – handled by the CP

Cards are personalized both visually and electronically. Even if this process will be carried out by Service Agent (CP) this does not diminish the overall responsibility of the MSA.

5.1.8.1 Visual personalization

Cards shall be visually personalized according to Regulation Annex 1B, section IV [REG-A].

- A photograph of card holder must appear on a driver card and workshop card.

5.1.8.2 User data entry

Data shall be inserted in the card according to the structure in Regulation 1360/2002, Annex 1B, appendix 2 [REG-A], rules TCS_403, TCS_408, TCS_413 and TCS_418, depending on card type.

5.1.8.3 Key entry

The private key shall be inserted in the card without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection. It is intended, where possible, that keys are generated on card or by HSM. See also equipment key management, section 7.2.

5.1.8.4 Certificate entry

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

5.1.8.5 Quality Control

Documented routines shall exist to ensure that the visual information on users' cards and the electronic information in issued cards and certificates matches each other and also matches the validated owner. The routines shall be described in the CP PS.

5.1.8.6 Cancellation (destruction) of non-distributed cards

All cards that are damaged or destroyed (or for other reasons are not finalized and distributed) during personalization shall be physically and electronically destroyed.

5.1.9 Card registration and data storage (DB) – handled by the CP and the CIA

The CP and CIA are responsible for keeping track of which card and card number is given to which user. Data shall be transferred from the CP to the CIA database.

5.1.10 Card distribution to the user – handled by the CP and CIA

a) The personalization shall be scheduled so as to minimize the time that the personalized card require safekeeping before delivery to the user. Storage over night requires secure safekeeping. Documented routines shall exist for exception handling, including disturbances in the production process, failure of delivery, and loss of or damage to cards.
b) Personalized cards shall be immediately transferred to the place where they are to be delivered or distributed to the user, i.e. a controlled area.
c) Personalized cards shall always be kept separated from non-personalized cards.
d) The Tachograph card shall be distributed in a manner so as to minimize the risk of loss.
e) At the point of delivery of the card to the user, who has not been authenticated at the time of card application, evidence of the user's identity (e.g. name) shall be checked against a physical person.
f) The user shall present valid means of identification
g) The reception of the card shall be acknowledged by the user's signature.

5.1.11 Authentication codes (PIN) – generated by the CP

This section applies only to Workshop cards.
Workshop cards shall have a PIN code, used for authenticating the card to the Vehicle unit (Regulation Annex 1B, App 10 [REG-A]: Tachograph cards: 4.2.2)

PIN codes shall consist of at least **4** digits (Regulation Annex 1B, App 10 [REG-A]: Vehicle Units: 4.1.2).

5.1.10.1 PIN generation

PIN codes shall be generated in a secure system, 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 user. The PIN generation system shall meet the requirements of ITSEC E3, CC EAL4 or equivalent security criteria.

5.1.10.2 PIN distribution

PIN codes may be distributed by regular mail.

PIN codes shall not be distributed in connection with the corresponding cards.

5.1.12 Card deactivation – handled by CIA and CP

It shall be possible to permanently deactivate a card and any keys residing thereon. A decision of deactivation shall be taken by the CIA; the actual operation should be carried out by the CIA or CP.

Deactivation of cards shall take place in equipment suitable for the operation and it shall be verified that card functions and keys are destroyed. The card shall also be visually cancelled.

Deactivation of cards shall be registered in the card database and the card number shall be put on the blacklist.

5.2 Vehicle Units and Motion Sensors

Not applicable in Latvia for the time being or in the foreseeable future, except case of damaged or defective vehicle units. Workshop shall if possible extract data from the Vehicle unit and deliver it to the company. In case, where this cannot be done, workshop shall write statement to the company.

6 Key management: European Root key, Member State keys, Motion Sensor keys

This section contains provisions for the management of

- European Root key - the ERCA public key;
- Member State keys, i.e. the Member State signing key pair(s);
- the Motion Sensor keys.

The **ERCA public key** is used for verifying the Member State certificates. The ERCA private key is not dealt with here, since it never leaves the ERCA.

The **Member State keys** are the Member State signing keys and may also be called Member State root keys.

The **Motion Sensor keys** are the symmetric keys to be placed in the workshop card, VU and Motion Sensor for mutual recognition. The MSCA receives the Motion Sensor keys from the ERCA, stores them and distributes them to CP.

The **transport keys** are asymmetric key pairs to be used in secure transfer of Motions Sensor keys between ERCA and MSCA.

If the MSCA has a need for other cryptographic keys than the above, these shall not be considered part of the Tachograph system, and is not dealt within this policy.

The Member State keys and transport keys are generated and stored in physically highly secured environment, with 24/7 organized security by human control. All access to the environment is protected by electronic locks. Premises shall have a recording video control system.

6.1 ERCA public key

The MSCA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times. If the EUR.PK is stored in the CSP, the same rule applies.

The CP shall ensure that EUR.PK is inserted in all Tachograph cards and vehicle units.

6.2 Member State keys

The Member State keys are the MSCA signing key pair(s), which is used to sign all Tachograph card certificates. The MSCA does not produce vehicle unit certificates.

The key pair consists of a public key (MS.PK) and a private key (MS.SK).

The MSCA public key is certified by the ERCA, but it is always generated by the MSCA itself.

The Member State keys must not be used for any other purposes than

a) signing the Tachograph card certificates

b) signing the ERCA key certification request, KCR, as described in Annex A [ERCA]

6.2.1 Member State keys generation

Member State key pair generation shall be carried out within a HSM, which either:

meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or

meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or

is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

The actual device used and requirements met shall be stated in the CPS.

MSCA key-pair generation shall require the active participation of at least three separate individuals, who have trusted roles within MSCA or CSP. At least one of these individuals shall have role of CA, who is responsible for MSCA operations.

Keys shall be generated using the RSA algorithm with a key length of modulus n=1024 bits (Regulation Annex 1B, app 11:2.1/3.2).

The MSCA shall have more than one Member State key pair with associated signing certificates to ensure continuity all the time.

6.2.2 Member State keys' period of validity

The Member State private key shall not be valid for more than **2** years from the issuance of the corresponding public key's certificate, and shall not be used after its validity period for any purpose.

Due to the ERCA signing process for more than one Member State key pair, public key shall have no end of validity. Actual validity for Member State public key certificates is defined and decided by the ERCA Root Policy.

6.2.3 Member State private key storage

The private keys shall be contained in and operated from inside a specific tamper resistant device (HSM), which:

- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

For access to the 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.

6.2.4 Member State private key backup

The Member State private signing keys may be backed up, using a key recovery procedure requiring at least dual control. The procedure used shall be stated in the CPS. It is allowed to backup private signing keys in encrypted format; if decrypting requires HSM and at least dual control and requirements in section 6.2.3 is fulfilled. However, if MSCA has multiple key pairs according to section 6.2.1, no backup is really needed.

6.2.5 Member State private key escrow

The Member State private signing keys shall not be escrowed.

6.2.6 Member State keys compromise

A written instruction shall exist, included in the CPS, which states the measures to be taken by users and security responsible persons at the MSCA and/or Service Agencies (CSP), if the Member State private keys has become exposed, or is otherwise considered or suspected to be compromised.

In such case the MSCA shall as a minimum:

- without delay inform the MSA, the ERCA and all other MSCAs.

- have backup system with pre-generated and ERCA certified MSCA key pairs, which allow continuing MSCA operations without remarkable delays

6.2.7 Member State keys end of life

The MSCA shall have routines to ensure that it always has a valid, certified Member State signing key pair.

Upon termination of use of a Member State signing key pair, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved;
- retained in a manner such that it is protected against being put back into use.

6.3 Motion Sensor keys

The MSCA shall, as needed, request motion sensor keys Km, Km_{VU} and Km_{WC} from the ERCA (Regulation Annex 1B [REG-A]: app 11:3.1.3).

The MSCA shall only forward the workshop key Km_{WC} to the CP for insertion into Workshop cards. The workshop Km_{WC} shall be transported to CP in encrypted format using means and media defined by the ERCA Root Policy annex C [ERCA].

The MSCA shall not handle with motion sensor master key Km or vehicle unit motion sensor key Km_{WU} and MSCA will ensure that they are not used for any purposes and that they will never leave the secure environment of MSCA.

The CP shall undertake the MSCA's task to ensure that the workshop key Km_{WC} is inserted into all issued Workshop cards (Regulation Annex 1B [REG-A]: app 11:3.1.3).

The MSCA and/or CP shall during storage, use and distribution protect the motion sensor key Km_{WC} with high assurance physical and logical security controls.

The asymmetric transport keys used for requesting, storing and distribution of Motion Sensor keys and the Motion Sensor key KM_{wc} itself should be generated by, contained in and operated from a specific tamper resistant device which:

- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

6.4 Key transports

All key transport between MSCA and ERCA shall use the means, media and protocols defined by the ERCA Root Policy annex C [ERCA]. If physical media is used for key transport, MSA will appoint the authorized person to carry the media.

MSCA key certification request shall use KCR protocol specified in the ERCA Root Policy annex A [ERCA]

MSCA shall accept the ERCA Public Key in distribution format described in the ERCA Root Policy annex B [ERCA]

MSCA shall ensure that KID and modulus of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the Domain of MSCA.

MSCA shall request Motion Sensor Key from the ERCA using KDR protocol specified in the ERCA Root Policy annex D [ERCA].

7 Equipment keys (asymmetric)

Equipment keys are asymmetric keys generated somewhere in the issuing/manufacturing process, and certified by the MSCA for the equipment in the Tachograph system:

- Tachograph cards;
- Vehicle Units (Not applicable for Latvia for the time being or or in the foreseeable future).

The symmetric Motion Sensor keys are not handled here.

7.1 General aspects CP/MSCA incl. Service Agencies

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

No sensitive information contained in the key generation systems may leave the system in a way that violates this policy.

No sensitive information in the card personalization system may leave the system in a way that violates this policy.

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 the log on request.

MSCA/CP/Service Agencies: The log of the personalization system shall contain a reference to the order, and list the corresponding equipment numbers and certificates. The relevant MSA shall have access to the logs on request.

7.2 Equipment key generation

Keys may be generated either by the equipment manufacturer, by the CP or by the MSCA. (Annex 1B [REG-A], Appendix 11:3.1.1)

The entity that performs the key generation shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

Key generation shall be carried out within a device which either:

meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or

meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or

is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

Keys shall be generated using the RSA algorithm having a key length of modulus *n* 1024 bits. (Annex 1B [REG-A]: Appendix 11:2.1/3.2)

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

It is the responsibility of CP to undertake adequate measures to ensure that the public key identifier is unique within its domain before the certificate request is sent the CSP. (This is presumably done by making sure that the actual card serial number is used as part of Key Identifier and ensuring that the manufacturing process keeps card serial numbers unique.)

CSP shall ensure the uniqueness of public keys in Tachograph card certificates within its domain.

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

Batch processing must be performed in stand-alone equipment meeting the security requirements stated above. Key integrity has to be protected until the certificate issuing is performed.

7.3 Equipment key validity

7.3.1 Keys on cards

Usage of an equipment private key in connection with certificates issued under this policy shall never exceed the end of validity of the certificate.

7.3.2 Vehicle units

Not applicable in Latvia for the time being or in the foreseeable future.

7.4 Equipment private key protection and storage - Cards

The CP shall ensure that the card private key is protected by, and restricted to, a card that has been delivered to the user according to the procedures stated in this policy.

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

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

7.5 Equipment private key protection and storage – VUs

Not applicable in Latvia for the time being or in the foreseeable future.

7.6 Equipment private key escrow and archival

Equipment private keys shall be neither escrowed nor archived.

7.7 Equipment public key archival

All certified public keys shall be archived by CSP on behalf of the certifying MSCA.

7.8 Equipment keys end of life

Upon termination of use of a Tachograph card, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved, if it is within ability of CIA to do so; or
- retained in a manner such that it is protected against being put back into use.

Upon termination of use of a Vehicle Unit, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

8 Equipment certificate management

This section describes the certificate life cycle, containing registration function, certificate issuing, distribution, use, renewal, revocation (if applicable) and end of life.

8.1 Data input

8.1.1 Tachograph cards

Card holders do not apply for certificates, their certificates are issued based on the information given in the application for a Tachograph card (section 5.1.2) and captured from the CIA register. The public key to be certified is extracted from the key generation process.

The CIA shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique. The MSCA shall verify the uniqueness of the CHR within its domain.

Certificate request protocol shall ensure the integrity and origin of a request without exposing the private key.

8.3.2 Vehicle units

Not applicable in Latvia for the time being or in the foreseeable future.

8.2 Tachograph card certificates

8.2.1 Driver certificates

Driver certificates are issued only to valid applicants for a Driver card.

8.2.2 Workshop certificates

Workshop certificates are issued only to valid applicants for a Workshop card.

8.2.3 Control body certificates

Control body certificates are issued only to valid applicants for a Control card.

8.2.4 Company certificates

Company certificates are issued only to valid applicants for a Company card.

8.3 Vehicle unit certificates

Not applicable in Latvia for the time being or in the foreseeable future.

8.4 Equipment certificate time of validity

Certificates shall not be valid longer than the corresponding equipment

- Driver certificates shall not be valid more than **5** years.
- Workshop certificates shall not be valid for more than **1** year.
- Control body certificates shall not be valid more than **2** years.
- Company certificates shall not be valid more than **5** years.

8.5 Equipment certificate issuing

The MSCA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by Regulation Annex 1B [REG-A], appendix 11.

8.6 Equipment certificate renewal and update

See Equipment management (section 5). Since certificates and cards have the same time of validity, they are dealt with together. VU certificates have either no end of, or a very long time of validity, it is assumed that the lifetime of the equipment is shorter than that of the certificate.

8.7 Dissemination of equipment certificates and information

The CIA shall ensure that certificates are made available as necessary to users and related parties.

The CIA shall ensure that all terms and conditions, as well as relevant parts of the CSP PS, and other relevant information, are made readily available to all users, related parties and other relevant groups.

8.8 Equipment certificate use

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

8.9 Equipment certificate revocation

Certificates are not revoked, however, the MSCA shall maintain and make certificate status information available on request for relevant parties, such as

- MSAs and Control authorities of Member states
- The EU-Comission

9 MSCA, CIA, CP, CSP Information Security management

Each party maintains its own information security policy documentation. The parties have signed an information security agreement, which handles in details overall security management of the parties.

Each party shall adopt an information security management system equivalent to BS7799 [ISO 17799]. Formal certification is not required.

Each party shall ensure that they will all the time have personnel which as minimum:

- is trained for their part of the Tachograph system

- has their roles specified in the Tachograph system
- has been checked for their clearance by police or equivalent organization

Each party shall ensure that they maintain archives of records of their operations and they have a policy that defines the archive periods for those records.

10 MSCA or CP Termination

10.1 Final termination - MSA responsibility

Final termination of an MSCA or CIA is regarded as the situation where all service associated with MSCA or CIA is terminated permanently. It is not the case where the service is transferred from one organization to another or when the MSCA service is passed over from an old Member State key pair to a new Member State key pair or the ERCA key. It implies the situation where the Member State withdraws from the Tachograph system or termination of the entire Tachograph system.

The MSA shall ensure that the tasks outlined below are carried out.

Before the MSCA/CIA terminates its services the following procedures has to be completed as a minimum:

a) Inform all users and parties with whom the MSCA/CIA has agreements or other form of established relations;

b) Make publicly available information of its termination at least **3** month prior to termination;

c) The MSCA/CIA shall terminate all authorization of subcontractors to act on behalf of the MSCA/CIA in the process of issuing certificates;

d) The MSCA/CIA shall perform necessary undertakings to maintain and provide continuous access to record archives.

10.2 Transfer of CSP or CP responsibility

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

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

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

The old CSP shall destroy any copies of MSCA keys.

11 Audit

The MSA is responsible for ensuring that audits of the CP and CSP take place. Audit reports shall also be available in English.

11.1 Frequency of entity compliance audit

The CP and CSP operating under this National MSA Policy shall be audited at least once in two years period for conformance with the policy.

11.2 Topics covered by audit

The audit shall cover the MSCA/CP/CSP practices.

The audit shall cover the MSCA/CP/CSP compliance with this National MSA Policy.

The audit shall also consider the operations of any Service Agencies.

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 cover the CP and CSP compliance with requirements defined in ERCA – CP § 5.3

11.3 Who should do the audit

The MSA may consult an external certification or accreditation organization for approval of the CP/CSP/ PS in order to increase relying parties' trust in the implementation. Otherwise the MSA shall undertake the auditing.

11.4 Actions taken as a result of deficiency

If irregularities are found in the audit the MSA shall take appropriate action depending on its severity.

11.5 Communication of results

Results of the audits, on a security status level, shall be available upon request. Actual audit reports shall not be available, except on need-to-know basis. Audit reports shall be submitted to the ERCA.

12 National MSA Policy change procedures

12.1 Items that may change without notification

The only changes that may be made to this specification without notification are

a) Editorial or typographical corrections
b) Changes to the contact details.

12.2 Changes with notification

12.2.1 Notice

Any item in this policy may be changed with **90** days notice.

Changes to items, which in the judgement of the policy responsible organization (the MSA), **will not** materially impact a substantial majority of the users or related parties using this policy, may be changed with **30** days notice.

12.2.2 Comment period

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

12.2.3 Whom to inform

Information about changes to this policy shall be sent to:

- the ERCA
- MSCA and CIA including Service Agencies
- All other MSAs

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.

12.3 Changes requiring a new National MSA Policy approval

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

13 References

[REG] Council Regulation 3821/85 as amended by Council Regulation (EC) No 2135/98 of 24th September 1998

[REG-A] Annex I(B) to Council Regulation 2135/98 *Requirements for construction, testing, installation and inspection*

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 15 December 2003, owned by the Commission

[CC] Common Criteria. ISO/IEC 15408 (1999): "Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3)".

[CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Policy requirements for certification authorities issuing public key certificates

[FIPS] FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)

[ISO 17799] BS ISO/IEC 17799: 2000. Information technology - Code of practice for information security management.

[CSG] Common Security Guidline , Card Issuing Project., owned by the Commission

[ERCA] Digital Tachograph System European Root Policy version 2.0

Special Publication I.04.131

-

-

14 Glossary/Definitions and abbreviations

14.1 Glossary/Definitions

MSA Policy: A named set of rules that indicates the applicability of keys, certificates and equipment to a particular community and/or class of application with common security requirements.

Card/Tachograph cards: Integrated Circuit equipped card, in this policy this is equivalent to the use of the terms ”**IC-Card**” and ”**Smart Card**”.

Card holder: A person or an organization that is a holder and user of a Tachograph card. Included are drivers, company representatives, workshop workers and control body staff.
Certificate: In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.
Certification Authority System (CAS): A computer system in which certificates are issued by signing certificate (user) data with the CA private signing key.
Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual MSA policy.
Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.
Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.
Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.
Practice Statement: A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.
Private key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called a Secret key.
Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.
Service Agency: An entity that undertakes to tasks on behalf of an MSCA, CIA or CP, a subcontractor.
Tachograph cards/Cards: Four different type of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.
User: Users are equipment users and are either **Card Holders** for card or **manufacturers** for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

<u>In this document:</u>
Signed: Where this policy requires a signature, the requirement is met by a secure and verifiable digital signature.
Written: Where this policy requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for the parties concerned.

14.2 List of abbreviations

CA	Certification Authority
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card Personalizer
CP PS	Card Personalizer Practice Statement
CPS	Certification Practice Statement
CSP	Certificate Service Provider
DB	Database

ERCA	European Root CA
HSM	Hardware Security Module
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KG	Key Generation
MS	Member State of Tachograph system
MSA	Member State Authority
MSCA	Member State CA
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	A specific Public key algorithm
SA	System Administrator
PS	Practice Statement
VU	Vehicle Unit
VUP	VU Personalizing organization

15 Correspondence table with the ERCA Policy

This is a correspondence table linking the ERCA Root Policy [ERCA] chapter 5.3 requirements to this national MSA Policy.

ERCA CP	LV MSA	Remarks
§5.3.1	§1.1	CPS for entities involved. It will be made available to the ERCA.
§5.3.2	§6.2.1, §6.2.3, §6.3	CPS will identify actual (certified) HSM device to be used. CPS will be made available to the ERCA
§5.3.3	§6, §6.2.1	CPS will identify actual physical security control systems used. It will be made available to the ERCA
§5.3.4	§6.2.2	
§5.3.5	§6.2.1	
§5.3.6	§6.4	
§5.3.7	§6.4	
§5.3.8	§6.4	
§5.3.9	§6.4	
§5.3.10	§6.4	
§5.3.11	§6.2.7	
§5.3.12	§7.1,	CP PS will identify actual (certified) HSM device to be used.

ERCA CP	**LV MSA**	**Remarks**
	§7.2, §5.1.1	It will be made available to the ERCA CP PS will identify actual (certified) card to be used. It will be made available to the ERCA
§5.3.13	§3.4.1, §6.2.1, §7.2	
§5.3.14	§6.2.3, §7.3, §7.4	
§5.3.15	§6.2.4	
§5.3.16	§7.2	
§5.3.17	§6.2.5, § 7.6	
§5.3.18	§6.3	
§5.3.19	§6.3	
§5.3.20	§6.3	Not applicable
§5.3.21	§6.3	
§5.3.22	§3.1.9, §6.3	Not applicable
§5.3.23	§3.4.1, §6.3	
§5.3.24	§6.3	
§5.3.25	§6.2, §6.3, §7.5	Latvian MSA Policy will not support VU-manufacturers
§5.3.26	§6.2.1	
§5.3.27	§6.2	
§5.3.28	§6.2.3	
§5.3.29	§7.2	
§5.3.30	§7.3 §8.1.1	
§5.3.31	§5.1.6 §8.9	
§5.3.32	§8.4	
§5.3.33, §5.3.34		Not applicable, as no undefined validity certificates (required for service to VU manufacturers) are handled under the LV-

ERCA CP	**LV MSA**	**Remarks**
		MSA Policy.
§5.3.35	§5.1.2, §5.1.10	
§5.3.36	§6.2.6	
§5.3.37	§6.2.6	
§5.3.38	§9	
§5.3.39	§9	
§5.3.40	§9	
§5.3.41	§10	
§5.3.42	§12	
§5.3.43	§11.2	
§5.3.44	§11.1	
§5.3.45	§11, §11.5	
§5.3.46	§11,2, §11.4	