MINISTRY OF INFRASTRUCTURE

Member State Authority Policy - Poland

Warsaw, 14th September 2018 – ver. 01.05.18

Document approval

	Name	Organization	Date	Signature
Comments received from European Commission	James Bishop	EU Commission	24.11.2005	
Comments received from European Commission	James Bishop	EU Commission	20.12.2005	

Document version control

Version	Issue date	Description
01.01	20/10/2005	Initial version
01.02	01/12/2005	Modified version according to Mr James Bishop's and Ministry of Transport and Construction remarks.
01.03	05/01/2006	Updated version based on Mr James Bishop's remarks stated in the Attachment 1 "Review Findings" to the document: G07-TRVA/JB/jb/(2005)D32853, dated 20th December 2005. All proposed changes in the mentioned above document have been adapted.
01.04.08	22/01/2008	Changes: a) in order to update contact details b) due to the amendment in the Art. 20.1 point 2) of the national legislation [5] regarding the company card (the change has no a material impact on significant number of users of the DTS) c) in order to make few editorial corrections

01.05.18	14/09/2018	Changes: a) in order to update the reference to binding EU legal basis b) in order to add the reference to newly introduced relevant national legislation, namely the Tachographs Act of 5 July 2018 which will replace the Digital Tachograph Act of 28 July 2005 [5] c) in order to update contact details d) resulting from commencement of the provision of the services for manufacturers of motion sensors e) due to entry into force of the General Data Protection Regulation (EU) 2016/679 provisions

Rational:

ERCA Policy v.2.1	PL-MSA Policy	Remarks
§5.3.1	§1.2, §1.4	
§5.3.2	§6.2.1, §6.2.3, §6.2.4, §6.4	
§5.3.3	§6.2.1, §9.3.1	
§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	§5.1.1, §7.1, §7.2	
§5.3.13	§3.1.3, §5.1.8.3, §6.2.1, §6.2.3, §7.1, §7.2	
§5.3.14	§3.1.6, §5.1.8.3, §6.2.3, §7.2.3	
§5.3.15	§6.2.4	
§5.3.16	§5.1.8.3, §6.4, §7.2.3	
§5.3.17	§6.2.5, §7.2.4	
§5.3.18	§6.3	
§5.3.19 §5.3.20	§6.3	No VU manufactures in Poland. Applicable to motion sensors.
§5.3.21	§3.1.4, §6.3	
§5.3.22	§6.3	No VU manufactures in Poland. If, at any time in the future, PL-MSA will establish an agreement to provide services to the VU manufactures the PL-MSA Policy will be modified appropriately and re-submitted to the ERCA for approval.
§5.3.23	§3.4, §6.3	
§5.3.24	§6.3	
§5.3.25	§6, §6.2, §6.2.1, §6.2.2	No VU manufactures in Poland. Applicable to cards.
§5.3.26	§6.1, §6.2.1	
§5.3.27	§6.2	
§5.3.28	§6.2.3	
§5.3.29	§8.1.1	
§5.3.30	§6.2.3, §8.4	
§5.3.31	§8.6, §8.8	
§5.3.32	§8.3	
§5.3.33	§8.3	
§5.3.34	§8.3	No VU manufactures in Poland. Applicable to cards.
§5.3.35	§5.1.2, §5.1.8.5	

§5.3.36	§6.2.6	
§5.3.37	§6.2.1, §6.2.4, §9.6	
§5.3.38	§9.1, §9.2	
§5.3.39	§9.3.1, §9.3.2, §9.3.3, §9.3.4	
§5.3.40	§9.5.1, §9.5.3	
§5.3.41	§10	
§5.3.42	§12	
§5.3.43	§11, §11.2	
§5.3.44	§11.1	
§5.3.45	§11.5	
§5.3.46	§11.4, §11.5	

List of contents

1 Introduction

This document establishes the Polish Member State Authority (MSA) Policy, referred to hereinafter in brief as “the PL-MSA Policy”. The PL-MSA Policy will be followed in the operation of the Digital Tachograph System (DTS).

The PL-MSA Policy is a document that contains requirements for secure management of keys, certificates and associated equipment used within the DTS.

The PL-MSA Policy complies with:

- Annex 1B to the Council Regulation (EEC) N° 3821/85 as amended (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1536131379135&uri=CELEX%3A01985R3821-20160222)..[1]
- The Guideline and Template National CA policy (http://www.urba2000.com/chrono/public/ts-NCA-POLICY%20Guideline%20v1.pdf)..[2]
- The Common Security Guideline (http://www.urba2000.com/chrono/public/CommonSecurityGuideline10.pdf) ………...[3]
- The Digital Tachograph European Root Policy v.2.1 (https://dtc.jrc.ec.europa.eu/erca_of_doc/JRC53429_ERCA_CP_v2_1.pdf) ………………………………………………[4]
- The law of 28 July 2005 on the Digital Tachograph System (OJ of 2005, No 180, item 1494) and Tachographs Act of 5 July 2018 (Journal of Laws of 2018, item 1480)……………………………………………………………………………...[5]
- Common Criteria. ISO/IEC 15408 (1999): "Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3)"……………………………………..[CC]
- CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP) …………………………………………[CEN]
- FIPS PUB 140-2 (May 25, 2001): „Security Requirements for Cryptographic Modules”. Information Technology Laboratory, National Institute of Standards and Technology (NIST) ……………………………………………………………………………..[FIPS]

1.1 Goal

The goal of the Digital Tachograph System (DTS) is to implement the Europe-wide plan to control the driving and rest periods of truck and bus drivers more efficient thus to improve working conditions and road safety.

That is to be achieved by replacing the present paper-discs based system with a digital recording device which drivers, control bodies, etc. must authenticate themselves using a smart card with cryptographically secured certificates. The system shall use 4 card types: driver card, workshop card, company card and control card.

1.2 Responsible organizations

PL-MSA

The organization responsible for the implementation of [1] in Poland will be Ministerstwo Infrastruktury (Ministry of Infrastructure) hereinafter, in conformity with international usage, be referred to as the PL-MSA. The official contact is:

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

PL-MSCA

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

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

PL-CIA

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

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)

ul. Karczunkowska 30,

02-871 Warszawa

Poland

Telephone: (+48-22) 332-92-90

Fax:(+48-22)332-92-98

e-mail: tachograf@pwpw.pl

http://info-car.pl/infocar/tachograf

PL-CP

The Card Personalization centre in Poland (be referred to as the PL-CP) shall be:
Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30,
02-871 Warszawa
Poland
Telephone: (+48-22) 332-92-90
Fax: (+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

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

1.3 Approval

PL-MSA Policy is approved by:
Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)
at *Member State Authority Policy - Poland, ver. 01.05.18* under the No D Ares(2019)220781 - 15/01/2019

1.4 Availability and contact details

Public availability:

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

Questions concerning this PL-MSA Policy should be addressed to:

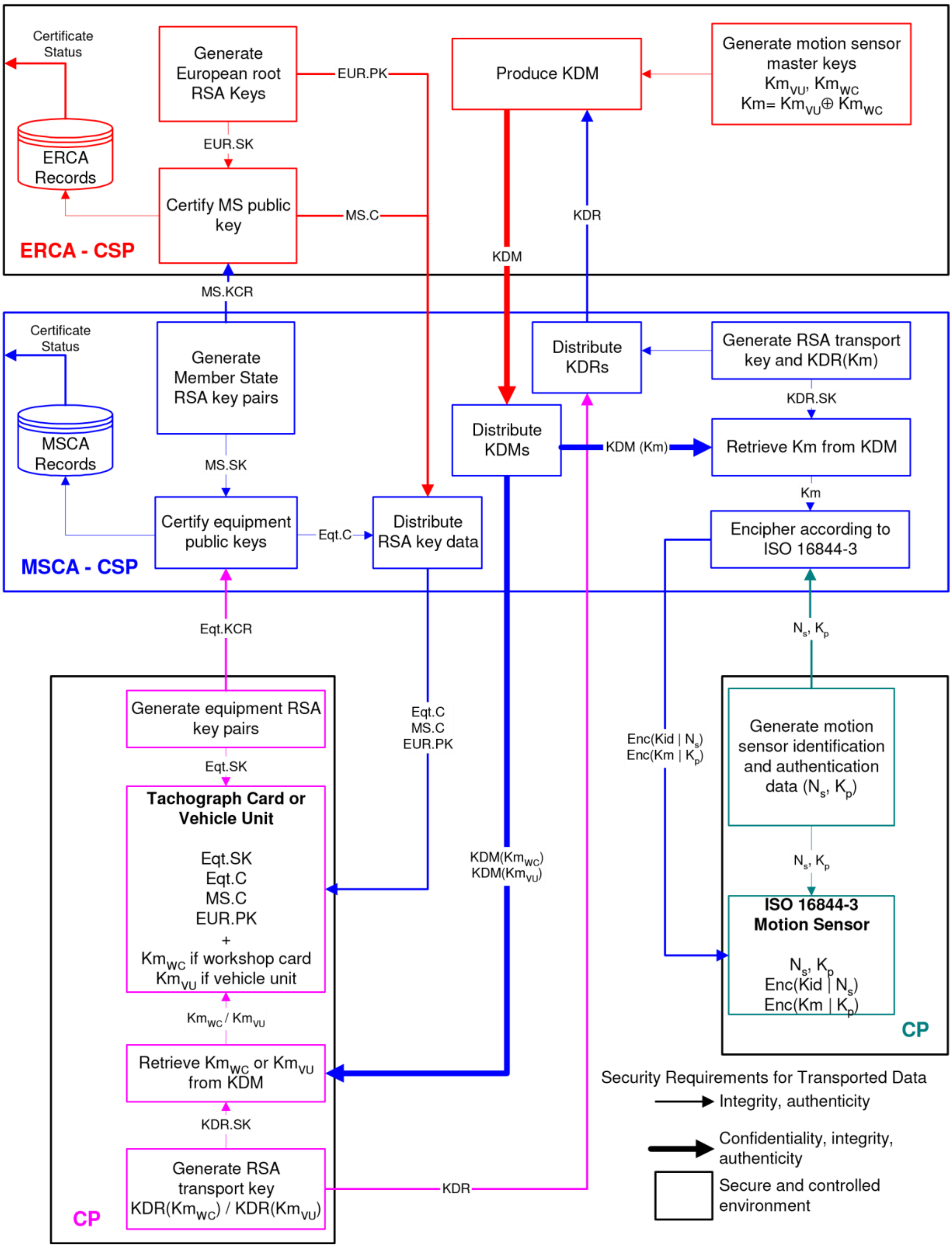
Ministerstwo Infrastruktury (Ministry of Infrastructure)
Departament Transportu Drogowego (Road Transport Department)
ul. Chałubińskiego 4/6,
00-928 Warszawa
Poland
Telephone: (+48-22) 630-12-51
Fax: (+48-22) 630-12-02
e-mail: anna.kowalczyk@mi.gov.pl

Contact details for this PL-MSA Policy:

Name of the document:
Member State Authority Policy - Poland
Identity of this document:
PLMSAPolicy v 01-05.18 Polish.pdf - Polish version
PLMSAPolicy v 01-05.18 English.pdf - English version

2 Scope and applicability

The PL-MSA Policy is valid for the DTS only.
The keys and certificates issued by the PL-MSCA are only for the use within the DTS.
The cards issued by the system are only for the use within the DTS.


Certificate Status
ERCA Records
Generate European root RSA Keys
EUR.PK
EUR.SK
Certify MS public key
MS.C
ERCA - CSP
Produce KDM
Generate motion sensor master keys
Km_{VU}, Km_{WC}
$Km= Km_{VU} \oplus Km_{WC}$
KDM
KDR
MS.KCR
Certificate Status
MSCA Records
Generate Member State RSA key pairs
MS.SK
Certify equipment public keys
Eqt.C
Distribute RSA key data
Distribute KDMs
Distribute KDRs
Generate RSA transport key and KDR(Km)
KDR.SK
KDM (Km)
Retrieve Km from KDM
Km
Encipher according to ISO 16844-3
MSCA - CSP
Eqt.KCR
Eqt.C
MS.C
EUR.PK
N_s, K_p
Enc(Kid | N_s)
Enc(Km | K_p)
Generate equipment RSA key pairs
Eqt.SK
Tachograph Card or Vehicle Unit
Eqt.SK
Eqt.C
MS.C
EUR.PK
+
Km_{WC} if workshop card
Km_{VU} if vehicle unit
$KDM(Km_{WC})$
$KDM(Km_{VU})$
Km_{WC} / Km_{VU}
Retrieve Km_{WC} or Km_{VU} from KDM
KDR.SK
Generate RSA transport key
$KDR(Km_{WC})$ / $KDR(Km_{VU})$
KDR
CP
Generate motion sensor identification and authentication data (N_s, K_p)
N_s, K_p
ISO 16844-3 Motion Sensor
N_s, K_p
Enc(Kid | N_s)
Enc(Km | K_p)
CP
Security Requirements for Transported Data
Integrity, authenticity
Confidentiality, integrity, authenticity
Secure and controlled environment

The figure above presents the DTS logical infrastructure. Scope of the PL-MSA Policy is marked with bold lines.

3 General provisions

3.1 Obligations

This section contains provisions relating to the respective obligations of:

- PL-MSA;
- PL-CIA;
- PL-MSCA;
- PL-CP;
- DTS users – cardholders;
- Manufacturers of vehicle units and manufactures of motion sensors.

3.1.1 The PL-MSA obligations

The PL-MSA shall:

- Maintain the PL-MSA Policy;
- Appoint the PL-MSCA, the PL-CIA and the PL-CP;
- Audit the appointed PL-MSCA, PL-CIA and PL-CP;
- Audit the manufactures of vehicle units and manufactures of motion sensors;
- Approve the Practice Statement (PS) of the PL-MSCA/PL-CP and manufacturers of vehicle units and manufacturers of motion sensors and the PS of other external service providers, if necessary;
- Inform the appointed parties about the PL-MSA Policy;
- Let the PL-MSA Policy be approved by the ERCA.

3.1.2 The PL-CIA obligations

The appointed PL-CIA shall:

- Follow the PL-MSA Policy;
- Publish the PL-CP PS that complies with the PL-MSA Policy;
- Ensure that correct and relevant user information from the application process is passed to the PL-CP;
- Inform the users of the requirements in the PL-MSA Policy related to the use of the DTS;
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy.

3.1.3 The PL-MSCA obligations

The appointed PL-MSCA shall:

- Follow the PL-MSA Policy;
- Publish the PL-MSCA PS that complies with the PL-MSA Policy;
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy in particular to bear the risk of liability damages;
- The PL-MSCA shall ensure that all requirements on the PL-MSCA, as detailed in the Policy, are implemented.

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

3.1.4 The PL-CP obligations

The appointed PL-CP must:

- Follow the PL-MSA Policy;
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the PL-MSA Policy, in particular to bear the risk of liability damages.

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

The PL-CP has the responsibility for conformance with the requirements prescribed in the PL-MSA Policy, even when the PL-CP functionality is undertaken by subcontractors.

3.1.5 Cardholder obligations

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

3.1.6 Manufacturers of VU and MoS obligations

Manufacturers of vehicle units and manufacturers of motion sensors have to especially ensure that they:

- observe the requirements, which are relevant to them - i.e. [1] and all other laws and decrees relevant in this regard, especially of this PL-MSA Policy, to the best of their knowledge and according to the respective current technological developments,
    - that the integrated keys and certificates or those to be integrated in the equipment manufactured by them can be used only for proper purposes within the scope of [1],
    - take measures in order to ensure the confidentiality of the private as well as secret keys during the complete production process and also during the total service period of the equipment.
- provide the PL-MSA with names of all external service providers subcontracted with the responsibility of production and personalisation of their equipment at all required times and make it obligatory for them to adhere to the corresponding requirements. As long as the manufacturer passes on his tasks to a third party, his rights and duties remain unaffected by the same.
- draw up a PS, in which at least the method of implementation of the PL-MSA Policy, Root Policy and legal provisions is explained,
- immediately inform the PL-MSA or one of its authorised agencies about all security relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them.
- permit the PL-MSA or one of its authorised agencies to evaluate the practical execution of their duties.

3.2 Liability

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

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

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

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

PL-MSA and PL-CIA liability towards the DTS users

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

PL-MSCA and PL-CP liability towards PL-MSA and PL-CIA

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

3.3 Interpretation and enforcement

3.3.1 Governing law

Any controversy arising from the interpretation performance of the PL-MSA Policy shall be interpreted according to the Polish legislation.

3.4 Confidentiality

3.4.1 Personal data

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

In order to ensure the confidentiality and protection of individuals, the processing of personal data and the transfer of such data shall be limited in accordance with:

- 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) (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679),
- Personal Data Protection Act (Journal of Laws of 2018 item 1000)

(http://dziennikustaw.gov.pl/du/2018/1000/D2018000100001.pdf).

3.4.2 Business information

Confidentiality must at least be kept of:

- Private keys,
- Symmetric primary keys,
- Logs and audit logs,
- Detailed documentation regarding PKI management,

used within PL-MSCA/PL-CP/manufactures of vehicle units/manufactures of motion sensor in accordance with this PL-MSA Policy.

Confidential information may not be disclosed, made available unless the applicable law provides otherwise.

3.4.3 Information, that is not threated as confidential

Certificates are not considered confidential.

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

4 Practice Statement (PS)

The PL-MSCA, PL-CP and manufacturers of vehicle units and manufacturers of motion sensors shall have a statement which shall document the practices and procedures used to address all the requirements identified in the PL-MSA Policy, here below- known as PS. The PL-MSA will approve the PS.

In particular:

- The PS will identify the obligations of all external organizations supporting the PL-MCSA, PL-CP, manufacturers of vehicle units and manufacturers of motion sensors services including the applicable policies and practices;
- The contents of PS will be made available to the PL-MSA, to users of the DTS and to relying parties (e.g. control bodies), however, the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors is not generally required to make all the details of its practices public and available for the DTS users;
- The PS must explain how the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors fulfils its duties regarding the information-management.
- The management of the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors has a responsibility for ensuring the PS is properly implemented;
- The PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors shall define a review process for the PS;
- The PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors shall give due notice of changes it intends to make in its PS and shall, following approval from the PL-MSA, make the revised PS immediately available.

- The PS contains a listing of incidents which could lead to compromising of keys. This listing must be treated as confidential.

5 Equipment management

The equipment in the DTS is defined as:

- DTS cards, hereinafter referred as “cards”;
- Vehicle Units (VUs);
- Motion sensors (MoS).

The equipment is handled or managed by:

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

The following functions are carried out by the PL-MSA:

- Quality control;
- PS approvals;
- PL-MSCA security monitoring. The PL-MSA shall have suitable monitoring procedures and means of enforcement in place to ensure that the certificates generated by the PL-MSCA and the cryptographic keys provided are only, in conformity with their intended purpose that meet the requirements of the [1].

The following functions are carried out by the PL-CIA:

- Application approval registration and processing related to issuing, renewing, replacing of lost, stolen and damaged cards for drivers, companies, workshops and control bodies;
- Card issuing. The PL-CIA shall ensure that issuing of new, replaced and exchanged cards is conducted in compliance with the [1] and that the specified deadlines can be observed;
- Exchange information with others Member States;
- Data storage and status info for registered cards.

The following functions are carried out by the PL-CP:

- Sending certificate request to PL-MSCA;
- Key and certificate insertion;
- Personalization of card:
    a) Applicant (user) data entry;
    b) Quality control (format and completeness).
- PIN code generation for workshop card;
- Card distribution to the applicant;
- Cancellation of non-distributed cards;
- Cancellation (destruction) of distributed but invalid cards.

The following functions are carried out by the PL-MSCA:

- Handling certificate requests form PL-CP;
- Generation of PL-MSCA keys for Poland and managing interface with ERCA certification process;

- Sending requests to ERCA for issuing symmetric primary keys to secure communication between VU devices and motion sensors (MoS);
- Encryption of pairing keys for motion sensors and delivering them to the right manufacturers of motion sensors;
- Encryption of serial numbers for motion sensors and delivering them to the right manufacturers of motion sensors.

The following functions are carried out by the manufacturers of motion sensors:

- Generating pairing keys for motion sensors and sending them to PL-MSCA;
- Embedding encrypted pairing keys into motion sensors;
- Generating serial numbers for motion sensors (MoS);
- Embedding encrypted serial numbers into motion sensors.

5.1 Cards

5.1.1 Quality control - the PL-MSCA/PL-CP function

The PL-MSCA/PL-CP shall ensure that only type approved cards according to [1] are personalized and issued for use.

5.1.2 Application for card

Applicant for a card shall deliver an application form to the PL-CIA in a format which has been determined by the PL-MSA. The application with appropriate attachments shall include the data needed to ensure the correct identification of the applicant for driver, company, workshop and control card, the correct identity of the legal organization on behalf of which they are applying.

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

The applicant shall, by applying for a card and accepting delivery of the card, accept the associated terms and conditions specified in particular in [1] and [5].

5.1.2.1 Agreements

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

- The applicant agrees to the terms and conditions regarding the use and handling of the card specified in [1] and [5];
- The applicant agrees to and certifies that:
    a) from the moment of receipt of the card and throughout the operational period of the card will not allow illicit access to or use of the card;
    b) at time of application all information provided by the applicant to the PL-CIA is true.

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

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

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

The PL-CIA shall make reasonable endeavours to check that the applicant for a driver card has a valid driving license of appropriate class (Category B or above).

5.1.3 Validity period of cards

Driver cards shall be valid for no more than **five years** from commencement of validity and no longer than Driver License validity (if this validity is limited).

Workshop cards shall be valid for no more than **one year** from commencement of validity, but no longer than the period of validity of the workshop technician's certificate issued by the competent authority, which constitutes the authorization to perform activities in an approved workshop, in accordance with the provisions of [5].

Company cards shall be valid for no more than **five years** from commencement of validity and no longer than the Licence or the Certificate for the own account carriage validity.

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

5.1.4 Card renewal - handled by the PL-CIA

5.1.4.1 Card expiry date

. The PL-CIA will issue a new card before the current card validity expires, provided that application is made for card renewal at least 15 days prior to any card’s expiration.
The PL-CIA shall establish routines to remind cardholders of the impending expiration of their cards.
An application for card renewal shall follow the same procedure as an application for a new card.

5.1.4.2 Modification of personal and administrative data

The change of surname of the driver or the fitter, the change of the working place of the fitter or any other data change crucial for the identification of the cardholder justify the need to exchange an existing card in order to modify administrative data. PL-CIA shall follow the rules of the renewal if previous card was issued within the same Member State (Poland).

5.1.5 Card exchange - handled by the PL-CIA

5.1.5.1 Change a country of residence

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

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

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

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

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

5.1.6.1 Replacement of stolen cards

If a card is stolen, its cardholder shall notify this to the authorised control body performing road transport checks or to the local Police in the country where the theft occurred and receive a copy of the notification.
Theft of the card must be reported also to the PL-CIA. PL-CIA shall register the report of the stolen card.
When a cardholder of stolen card submits an application for the card replacement to the PL-CIA, he or she shall attach to an application the notification from authorised control body performing road transport checks or Police.
Stolen card number shall be put on a blacklist available to the appropriate authorities in all Member States.

5.1.6.2 Replacement of lost cards

The loss of the card must be reported to the PL-CIA. PL-CIA shall register the report of the loss of the card.
A cardholder of lost card submits an application for card replacement to the PL-CIA.
The lost card number shall be put on a blacklist available to authorities in all Member States.

5.1.6.3 Replacement of damaged and malfunctioning cards

Damaged and malfunctioning cards shall be delivered to the PL-CIA. If damaged or malfunctioning cards are returned to the PL-CIA their numbers shall be put on a blacklist, visually and electronically cancelled, and subsequently destroyed.
If the card is lost, stolen, damaged or malfunctioning, the cardholder shall apply for a replacement within 7 calendar days.
The PL-CIA shall issue a replacement card with new keys and certificate within 5 working days from receiving a completed application, provided that the cardholder follows the above requirements.
The replacement card shall inherit the time of validity from the original card. If the replaced card has less than 2 months of validity remaining, the PL-CIA shall renew the card instead of replacing it.

5.1.7 Application approval registration

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

5.1.8 Card personalisation

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

5.1.8.1 Visual Personalisation

Cards shall be visually personalized according to Regulation Annex IB [1], specifically:

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

5.1.8.2 Applicant data entry

Data shall be inserted in the card according to the structure in Regulation Annex 1B [1], 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 inside HSM.

5.1.8.4 *Certificate entry*

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

5.1.8.5 Quality control

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

5.1.8.6 Cancellation and destruction of non-delivered cards

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

5.1.8.7 Cancellation and destruction of returned cards

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

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

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

The PL-CP is responsible for keeping track of which card and card number is given to which applicant. Necessary data from card applications that are transferred from PL-CIA to PL-CP for card personalization are removed from PL-CP resources after this operation.
Data shall be transferred from the PL-CP to the PL-CIA register.

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

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

5.1.10 Card distribution to the applicant

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

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

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

5.1.11 Authentication codes (PIN)

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

5.1.11.1 PIN generation

The PIN codes shall consist of at least 4 digits (Annex IB, Appendix 10: VU general security targets 4.1.2 [1]) and shall be generated in a secure system and securely transferred to the applicants of workshop cards.

5.1.11.2 PIN distribution

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

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

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

5.1.12 Card deactivation

In the event that cards are returned to PL-CIA, this information will be supplied to other Member States on a “need to know” basis.
In the event when the card which has been issued in the other Member State, is returned to the PL-CIA, the PL-CIA shall return the card to that issuing authority with the appropriate information of the reason for returning it.

6 Root keys and transport keys management: European Root key, Member State keys, motion sensor keys, transport keys

This section contains provisions for the management of:

- European Root key (the ERCA public key - EUR.PK);
- Member State keys, i.e. the Member State signing key pair(s) (MS.SK, MS.PK);

- The motion sensor keys (Km, Km_{VU} and Km_{WC});
- The transport keys (between the ERCA and the PL-MSCA).

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 keys used to sign certificates for digital tachograph cards.

The motion sensor keys are the symmetric keys to be placed in the workshop card and VU. The MSCA receives the motion sensor keys from the ERCA, stores them and distributes them to manufacturers.

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

The PL-MSCA use separate key pairs to sign certificates for digital tachograph cards and those keys what are delivered to digital tachograph manufacturers.
If the PL-MSCA has a need for other cryptographic keys than the above, these shall not be considered part of the DTS, and is not dealt with in the PL-MSA Policy.

6.1 ERCA public key

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

6.2 Member State keys

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

In Poland the Member State keys are the PL-MSCA signing key pair(s), which are used to sign all equipment certificates.

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

The Member State keys must not be used for any other purposes than signing Tachograph equipment certificates and generating Key Certificate Requests (KCR) according to [4] 5.3.27 b.

6.2.1 Member State keys generation

Member State key pair 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 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 key generation device should be stand-alone.

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

The generation of member state key pair(s) shall occur in a physically secured environment. The PL-MSCA key-pair generation shall require the active participation of at least two separate individuals. At least one of these shall have a role of CAA/PA (certification authority/ personalization administrator), the others may have other trusted roles (see section 9.3.1 for role descriptions).

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

The PL-MSCA shall have at least two (2) and maximum six (6) Member State key pairs with associated signing certificates to ensure continuity, since the ERCA cannot issue replacement Member State certificates rapidly.

6.2.2 Member State keys' period of validity

The Member State private key’s usage period is **2** years from certification of the corresponding public key. After this period, the key cannot be used. The appropriate public key is valid for an unlimited period. The public key certificates issued by the ERCA are valid for **7** years from the date of issuance.

6.2.3 Member State private key storage

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

- 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 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 PL-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 PL-MSCA private signing keys may be backed up, using a key backup procedure requiring at least dual control. The procedure used shall be stated in the PL-MSCA PS.

6.2.5 Member State private key escrow

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

6.2.6 Member State keys compromise

A written instruction shall exist, included in the PL-MSCA PS, which states the measures to be taken by persons responsible for security at the PL-MSCA when the PL-MSCA private keys has become exposed, or is otherwise considered or suspected to be compromised.
In such case the PL-MSCA shall as a minimum inform without delay the ERCA, the PL-MSA, and all other MSCAs.

6.2.7 Member State keys end of life

The PL-MSCA shall have routines to ensure that it always has a valid, certified Member State signing key pair.
Upon termination of use of the PL-MSCA signing key pair, the public key shall be archived, and the private key shall be destroyed such that the private key cannot be retrieved.

6.3 Motion sensor keys

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

The PL-MSCA shall forward the workshop key Km_{WC} to the PL-CP for insertion into workshop cards.

The PL-CP shall undertake the PL-MSCA's task to ensure that the workshop key Kmwc is only inserted into all issued Workshop cards ([1] Annex IB, app 11:3.1.3).

The PL-MSCA safely transfers the Km_{VU} key at the request of the digital tachograph manufacturer solely for the purpose of inserting it in the VU.

The PL-MSCA and/or PL-CP shall, during storage, use and distribution, protect the motion sensor keys with usage of effective logical and physical security measures. The keys should be 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
- 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 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 Transport keys

For secure data communication with ERCA the PL-MSCA shall generate and use an RSA key pair. The PL-MSCA shall, during generation and storage, protect these keys with usage of effective logical and physical security measures. The keys should be 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
- 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.

All key transport between the PL-MSCA and the ERCA shall use means, media and protocols defined by the ERCA Root Policy. If physical media is used for key transport, the PL-MSA will appoint the authorized person to carry the media.
The PL-MSCA key certification request shall use KCR protocol specified in the ERCA Root Policy, Annex A.
The PL-MSCA shall accept the ERCA Public Key in distribution format described in the ERCA Root Policy, Annex B.
The PL-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 the PL-MSCA.
The PL-MSCA shall request motion sensor key from the ERCA using KDR protocol specified in the ERCA Root Policy, Annex D.
The PL-MSCA receives the key of the motion sensor in an encrypted form in accordance with the ERCA Policy (KDM message).

7 Equipment keys (asymmetric)

Equipment keys are asymmetric keys generated by the equipment manufacturer, the PL-MSCA or the PL-CP, and certified by the PL-MSCA for the following equipment:

- Digital tachograph cards (DTC),
- Vehicle units (VU).

The symmetric motion sensor keys are not handled here.

7.1 General aspects concerning the PL-CP/PL-MSCA

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 of the entries and the actions shall be kept in the system.

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

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

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

7.2 Equipment key generation

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

Key generation shall be carried out within 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 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 IB, [1]).

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

It is the responsibility of the key generation entity to undertake adequate measures to ensure that the public key is unique within its domain before binding certification takes place. To this end, it must be ensured that the key generation system operates in a random manner, and therefore the likelihood of generating identical keys would be close to zero.

7.2.1 Batch key generation

Cryptographic key generation may be performed by batch processing in advance of certificate request, or in direct connection with certificate request.
Batch processing must be performed in stand-alone equipment. Key integrity has to be protected until certificate issuing is performed.

7.2.2 Equipment key validity

7.2.2.1 Keys on cards

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

7.2.3 Equipment private key protection and storage - cards

The PL-CP and the PL-CIA shall ensure that the card private key is protected by, and restricted to, a card that has been delivered to the cardholder according to the procedures stated in the PL-MSA Policy.
Copies of the private key shall not be kept anywhere except in the card, unless it is required during key generation and device personalization.
In no case the card private key may be exposed or stored outside the card.

7.2.4 Equipment private key escrow and archival

Equipment private keys shall be neither escrowed nor archived.

7.2.5 Equipment public key archival

All certified public keys shall be archived by the PL-MSCA, or by the PL-CIA.

7.2.6 Equipment keys end of life

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

8 Equipment certificate management

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

8.1 Data input

8.1.1 Cards

Cardholders do not apply for certificates. Certificates are issued on the basis of the information contained in the application for a card.

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

8.2 Card certificates

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

8.3 Equipment certificate time of validity

Certificates shall not be valid longer than the corresponding equipment:

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

The period of validity of certificates for vehicle units is undefined.

8.4 Equipment certificate issuance

The PL-MSCA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by in [1], Annex IB, Appendix 11 and submitted by the PL-CP to the PL-MSCA.

The PL-MSCA shall therefore validate proof of origin and integrity of the certificate requests.

Proof of origin and integrity check mechanisms may not rely on techniques that would cause private keys to be revealed.

8.5 Equipment certificate renewal and update

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

8.6 Dissemination of equipment certificates and information

The PL-CIA provides, if necessary, the availability of certificate information for cardholders

and relevant parties.

8.7 Equipment certificate use

The DTS certificates are only for use within the DTS.

8.8 Equipment certificate revocation

Although the PL-MSA Policy does not specify any rules as for the revocation of card certificates, the PL-CIA records the details of cards that have been lost, declared stolen, returned, destroyed or otherwise no longer in use. Information from this record will be made available to relevant parties and other Member States on request.

9 The PL-MSCA and the PL-CP information security management

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

9.1 Information Security management of the PL-MSCA and the PL-CP

The PL-MSCA/PL-CP shall ensure that adequate and consistent with the generally accepted standards of the administration and information security management procedures are applied.

The PL-MSCA/PL-CP shall retain responsibility for all aspects of the provision of key certification services, even if some of these functions are outsourced to subcontractors. The PL-MSCA/PL-CP clearly defines the scope of third parties liability and shall make reasonable efforts to ensure that third parties are required to implement any control mechanisms required by PL-MSCA/PL-CP.. PL-MSCA/PL-CP is obliged to disclose relevant PS to all interested parties.

The information security infrastructure necessary to manage the security within the PL-MSCA/PL-CP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the PL-MSA.

The PL-MSCA/PL-CP shall adopt a security management system equivalent to ISO-17799. Formal certification is not required.

9.2 PL-MSCA/PL-CP assets management and their classification

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

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

9.3 Personnel security controls of the PL-MSCA/CP

9.3.1 Trusted roles

The PL-MSCA and the PL-CP, supporting the PL-MSA Policy, should recognize three distinct roles, as outlined below. Different division of duties is allowed, provided that the protection against attack from the inside or fraud is at least as strong as with the model recommended below and provided that the roles are described in the PL-MSCA/PL-CP PS.

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

The roles are:

- Certification Authority Administrator or Personalization Administrator (CAA/PA);
- System Administrator (SA);
- Information System Security Officer (ISSO).

The CAA/PA role includes:

- The PL-MSCA key generation;
- Supervision over the generation of certificates;
- Administrative functions related to maintaining the PL-MSCA/PL-CP database and assistance in investigating infringements.

The SA role includes:

- Performing initial configuration of the system including secure boot start-up and shut down of the system;
- Initial set up of all new accounts;
- Setting the initial network configuration;
- Creating emergency system restart media to recover from catastrophic system loss;
- Performing system backups, software upgrades and recovery, including the secure storage and distribution of the backups and upgrades to an off-site location.

The ISSO role includes:

- Assigning security privileges and access controls of CAA/PA;
- Archiving of required system records;
- Review of the audit log to detect CAA/PA compliance with system security policy. Review of the audit log shall be done at least once per week;

- Personally conducting or supervising an annual inventory of the PL-MSCA/PL-CP's records;
- Participating in the PL-MSCA key generation.

Note that the ISSO, who is not directly involved in issuing certificates, performs a supervisory function by examining system records or audit logs to ensure that other persons are acting within their respective competences.

9.3.2 Separation of roles

In the case of PL-MSCA/PL-CP, each of the three roles described above shall be performed by different individuals and at least one individual shall be appointed per task.

9.3.3 Background, qualifications, experience, and clearance requirements

The CAA/PA which involves creating and managing certificates and key information, is a critical position. The individual assuming the CAA/PA role should be of unquestionable loyalty, trustworthiness and should have demonstrated a security consciousness and awareness in his or her daily activities.

All the PL-MSCA/PL-CP personnel in sensitive positions, including, at least, CAA/PA and ISSO (Information System Security Officer) roles, shall:

- Not be assigned other duties that may conflict with their duties and responsibilities as CAA/PA and ISSO;
- Have an impeccable reputation from previous jobs, in which they performed similar roles ;
- Have received proper training in the performance of their duties;
- Have a clean criminal record and satisfactory credit check.

9.3.4 Training requirements

Personnel shall have adequate training for the role and job.

9.4 System security controls of the PL-MSCA and the PL-CP

The PL-MSCA/PL-CP shall ensure that the systems are secured and correctly operated, with minimal risk of failure.

In particular:

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

9.5 Security audit procedures

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

9.5.1 Types of event recorded

The security audit functions related to the PL-MSCA/PL-CP computer/system shall log, at least, for audit purposes:

- The creation of accounts (privileged or not);

- Transaction requests together with record of the requesting account, type of request, indication of whether the transaction was completed or not and eventual cause of uncompleted transaction;
- Installation of new software or software updates;
- Time and date and other descriptive information about backups;
- Shutdowns and restarts of the system;
- Time and date of all hardware upgrades.

9.5.2 Retention period for audit log

Audit log shall be retained for at least **7** years.

9.5.3 Protection of audit log

Integrity of audit logs shall be appropriately protected.

Audit logs shall be verified and consolidated at least once every month. At least two people in SA or ISSO roles shall be present at such verification and consolidation.

9.5.4 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.

9.6 The PL-MSCA/PL-CP continuity planning

The PL-MSCA/PL-CP shall have a business continuity plan (BCP). This shall include (but is not limited to) events such as:

- Key compromise;
- Catastrophic data loss due to e.g. theft, fire, failure of hardware or software;
- System failure of other kinds.

9.6.1 Member State keys compromise

The PL-MSCA keys compromise is dealt with in accordance with the ERCA Policy.

9.7 Physical security control of the PL-MSCA and the PL-CP

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

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

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

9.7.1 Physical access

Access to the PL-MSCA/PL-CP facilities shall be limited to those personnel performing one of the described above roles. Access may be controlled through the use of an access control list to the room housing the systems.

10 The PL-MSCA or the PL-CP termination

10.1 Final termination - The PL-MSA responsibility

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

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

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

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

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

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

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

11 Audit

The PL-MSA is responsible for ensuring that audits of the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors take place.

11.1 Frequency of entity compliance audit

A PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors operating under the Polish MSA Policy shall be audited at least every 12 months for conformance with the policy.

11.2 Topics covered by audit

The audit shall cover the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors practices as defined in §5.3 ERCA Policy [4].

The audit shall cover the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors compliance with the PL-MSA Policy.

The audit shall also consider the operations of any subcontractors.

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

11.3 Who should do the audit

The PL-MSA may consult an external certification or accreditation organization for approval of the PL-MSCA/PL-CP/manufacturers of vehicle units/manufacturers of motion sensors PS in order to increase relying parties' trust in the implementation.

11.4 Actions taken as a result of deficiencies

If irregularities are found in the audit, the PL-MSA shall take appropriate action depending on risks and their severity. Audit reports sent to ERCA shall describe corrective actions and associated implementation schedule.

11.5 Communication of results

Results of the audits on a security status level shall be submitted in English to the ERCA.

12 The PL-MSA Policy change procedures

12.1 Items that may change without notification

Without notice, the following changes can be made to the PL-MSA Policy:

- Editorial or typographical corrections;
- Changes to the contact details.

12.2 Changes requiring notification

12.2.1 Notice

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

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

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 in the PL-MSA Policy shall be sent to:

- ERCA;
- PL-MSCA, PL-CIA, PL-CP, manufacturers of vehicle units and manufacturers of motion sensors.

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 Polish MSA Policy approval

If the PL-MSA considers that a change to the PL-MSA Policy has a significant impact on a significant number of DTS users, the PL-MSA shall submit a revised Polish MSA Policy to the ERCA for approval.

13 Glossary / Definitions and abbreviations

13.1 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: Integrated Circuit equipped card, in the PL-MSA Policy this is equivalent to the use of the terms “IC-Card” and “Smart Card”.

Cardholder: A person or an organization that is a holder and user of a card. Included are drivers, road transport companies, approved workshops and their fitters workers, control bodies and their staff.

Card type: In the DTS are used four different type of smart cards: driver card, company card, workshop card, control card.

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: A computer system in which certificates are issued by signing certificate (user) data with the CA private signing key.

Equipment: In the DTS the following equipment exists: cards, VU (vehicle units) and motion sensors.

Manufacturer/Equipment manufacturer: Manufacturers of the VUs or motion sensors.

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 DTS 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.

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 keys in the DTS.

13.2 Abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card Personalisation Centre
CPS	Certification Practice Statement
DTS	Digital Tachograph System
EEC	European Economic Community
ERCA	European Root Certification Authority
EUR.PK	ERCA Public Key
EUR.SK	ERCA Secret Key
HSM	Hardware Security Module (Sprzętowy moduł bezpieczeństwa)
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KCR	Key Certification Request
KDM	Key Distribution Message
KDR	Key Distribution Request
KG	Key Generation
KID	Key Identifier
Km	Motion Sensor Master Key
Km_{VU}	Motion Sensor Master Key – Vehicle Unit
Km_{WC}	Motion Sensor Master Key – Workshop Card
MoS	Motion Sensor
MS	Member State
MSA	Member State Authority
MSCA	Member State Certification Authority
MS.PK	Member State Public Key
MS.SK	Member State Secret Key
PIN	Personal Identification Number
PK	Private Key, RSA Private Key
PKI	Public Key Infrastructure
PL-CIA	Polish Card Issuing Authority
PL-CP	Polish Card Personalisation Centre
PL-MSCA	Polish Member State Certification Authority
PL-MSA Policy	Polish Member State Authority Policy
PS	Practice Statement

RSA	Rivest-Shamir-Adleman (asymmetric encryption scheme)
SA	System Administrator
SK	Secret Key, RSA Secret Key
TC	Tachograph Card
VU	Vehicle Unit (Digital Tachograph)