MOTORFAHRZEUGKONTROLLE
FÜRSTENTUM LIECHTENSTEIN

SMART TACHOGRAPHS LIECHTENSTEIN CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

Year of issue 2018, V1.00

Imprint

Creation date / Revision date:	21.11.2018 / -
Author:	Motorfahrzeugkontrolle Fürstentum Liechstenstein (MFK FL)
Page number:	55
Approval date:	21.11.2018
Approved by:	EU Commission, Joint Research Center (JRC)

Change history

Version	Date	Author	Remarks
V0.10	20.07.18	MFK FL	Version sent to ERCA for 1st review
V0.20	16.11.18	MFK FL	Changes after 1st review of ERCA
V0.30	20.11.18	MFK FL	Version sent to ERCA for final review and approved by ERCA
V1.00	21.11.18	MFK FL	Set to productive version 1.00 after official approval of the Liechstenstein MSA Policy (ERCA confirmation letter on 21.11.18, Ref. Ares(2018)5947343)

CONTENTS

1. INTRODUCTION 9
1.1. Overview 9
1.1.1. Smart Tachograph – the Second Generation of Digital Tachographs 9
1.1.2. Liechtenstein – PKI Member State and EEA EFTA state 9
1.1.3. No Component Manufacturers in Liechtenstein 9
1.1.4. Liechtenstein specific PKI role allocation 9
1.1.5. Liechtenstein specific Certificates and Keys in use 10
1.1.6. Liechtenstein specific Requests and Responses 12
1.1.7. The Transition from First Generation to Second Generation 12
1.1.8. The Policy Transition from First Generation to Second Generation 13
1.1.9. Particularities when using Abbreviations in this Policy 13
1.1.9.1. The Abbreviation CP 13
1.1.9.2. The Abbreviations for the Master Keys KM_{DSRC} and $K_{M\text{-}WC}$ 14
1.1.9.3. The Abbreviations MSA / FL-MSA, MSCA / FL-MSCA, FL-CIA, FL-CP 14
1.1.9.4. The Abbreviations MSCA_Card and MSCA_VU-EGF 14
1.2. Document Name and Identification 15
1.3. PKI Participants 15
1.3.1. Certification Authorities 15
1.3.1.1. European Root Certification Authority (ERCA) 15
1.3.1.2. Member State Certificate Authorities (MSCA) 15
1.3.1.3. Liechtenstein Member State Certificate Authority (FL-MSCA) 15
1.3.2. Registration Authorities 16
1.3.3. Subscribers (End Entities) 16
1.3.4. Relying Parties 17
1.3.5. Other Participants 17
1.4. Certificate Usage 17
1.4.1. Appropriate Certificate Uses 17
1.4.2. Prohibited Certificate Uses 18
1.5. Policy Administration 18
1.5.1. Organization Administering the Document 18
1.5.2. Contact Person 19
1.5.3. Person Determining CPS Suitability for the Policy 19
1.5.4. CPS approval procedures 19
1.6. Definitions and Acronyms 19
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 21
2.1. Repositories 21
2.2. Publication of Certification Information 21
2.3. Time or Frequency of Publication 21
2.4. Access Controls on Repositories 21
3. IDENTIFICATION AND AUTHENTICATION 21
3.1. Naming 21
3.1.1. Types of Names 21
3.1.1.1. Certificate Signing Request 21
3.1.1.2. Key Distribution Requests and Key Distribution Messages 22
3.1.1.3. Document Signer Certification Request 22
3.1.1.4. Card Personalisation Request 22
3.1.1.5. Card Certificate Signing Request 23
3.1.2. Need for Names to be Meaningful 23
3.1.3. Anonymity or Pseudonymity of Subscribers 23
3.1.4. Rules for Interpreting Various Name Forms 23
3.1.5. Uniqueness of Names 23
3.1.6. Recognition, Authentication, and Role of Trademarks 23
3.2. Initial Identity Validation 23

3.2.1. Method to Prove Possession of Private Key 23
3.2.2. Authentication of Organization Identity 24
3.2.3. Authentication of Individual Identity 24
3.2.4. Non-Verified Subscriber Information 24
3.2.5. Validation of Authority 24
3.2.6. Criteria for Interoperation 24
3.3. Identification and Authentication for Re-Key Requests 24
3.3.1. Identification and Authentication for Routine Re-Key 24
3.3.2. Identification and Authentication for Re-Key after Revocation 25
3.4. Identification and Authentication for Revocation Request 25
4. CERTIFICATE AND KEY LIFE-CYCLE OPERATIONAL REQUIREMENTS 25
4.1. Certificate Application 25
4.1.1. Who can submit a Certificate Application 25
4.1.2. Enrolment Process and Responsibilities 25
4.2. Certificate Application Processing 27
4.2.1. Performing Identification and Authentication Functions 27
4.2.1.1. Verification of Card Personalisation Request content 27
4.2.1.2. Verification of Card Certificate Signing Request content 27
4.2.1.3. Verification of Card CSR Response content 27
4.2.2. Approval or Rejection of Certificate Applications 27
4.2.3. Time to Process Certificate Applications 27
4.3. Certificate Issuance 28
4.3.1. CA Actions during Certificate Issuance 28
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate 28
4.4. Certificate Acceptance 28
4.4.1. Conduct Constituting Certificate Acceptance 28
4.4.1.1. Certificate Signing Requests (CSRs) 28
4.4.1.2. Card Certificate Signing Request (Card-CSRs) 29
4.4.2. Publication of the Certificate by the CA 29
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 29
4.5. Key Pair and Certificate Usage 29
4.5.1. Subscriber Private Key and Certificate Usage 29
4.5.2. Relying Party Public Key and Certificate Usage 29
4.6. Certificate Renewal 30
4.6.1. Circumstance for Certificate Renewal 30
4.6.2. Who May Request Renewal 30
4.6.3. Processing Certificate Renewal Requests 30
4.6.4. Notification of New Certificate Issuance to Subscriber 30
4.6.5. Conduct constituting acceptance of a renewal certificate 30
4.6.6. Publication of the renewal certificate by the CA 30
4.6.7. Notification of certificate issuance by the CA to other entities 30
4.7. Certificate Re-Key 30
4.7.1. Circumstance for Certificate Re-Key 30
4.7.2. Who May Request Certification of a New Public Key 30
4.7.3. Processing Certificate Re-Keying Requests 30
4.7.4. Notification of New Certificate Issuance to Subscriber 30
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 30
4.7.6. Publication of the Re-Keyed Certificate by the CA 30
4.7.7. Notification of Certificate Issuance by the CA to Other Entities 30
4.8. Certificate Modification 30
4.8.1. Circumstance for Certificate Modification 31
4.8.2. Who May Request Certificate Modification 31
4.8.3. Processing Certificate Modification Requests 31
4.8.4. Notification of New Certificate Issuance to Subscriber 31
4.8.5. Conduct Constituting Acceptance of Modified Certificate 31
4.8.6. Publication of the Modified Certificate by the CA 31

4.8.7. Notification of Certificate Issuance by the CA to Other Entities 31
4.9. Certificate Revocation and Suspension 31
4.9.1. Circumstances for Revocation 31
4.9.2. Who can Request Revocation 31
4.9.3. Procedure for Revocation Request 31
4.9.4. Revocation Request Grace Period 31
4.9.5. Time within which CA Must Process the Revocation Request 31
4.9.6. Revocation Checking Requirement for Relying Parties 31
4.9.7. CRL Issuance Frequency (if applicable) 31
4.9.8. Maximum Latency for CRLs (if applicable) 32
4.9.9. On-Line Revocation/Status Checking Availability 32
4.9.10. On-Line Revocation Checking Requirements 32
4.9.11. Other Forms of Revocation Advertisements Available 32
4.9.12. Special Requirements Re-Key Compromise 32
4.9.13. Circumstances for Suspension 32
4.9.14. Who can Request Suspension 32
4.9.15. Procedure for Suspension Request 32
4.9.16. Limits on Suspension Period 32
4.10. Certificate Status Services 32
4.10.1. Operational Characteristics 32
4.10.2. Service Availability 32
4.10.3. Optional Features 32
4.11. End of Subscription 32
4.12. Key Escrow and Recovery 32
4.12.1. Key Escrow and Recovery Policy and Practices 32
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 33
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 33
5.1. Physical Controls 33
5.1.1. Site Location and Construction 33
5.1.2. Physical Access 33
5.1.3. Power and Air Conditioning 33
5.1.4. Water Exposures 33
5.1.5. Fire Prevention and Protection 33
5.1.6. Media Storage 33
5.1.7. Waste Disposal 33
5.1.8. Off-Site Backup 33
5.2. Procedural Controls 33
5.2.1. Trusted Roles 33
5.2.2. Number of Persons Required per Task 34
5.2.3. Identification and Authentication for Each Role 34
5.2.4. Roles Requiring Separation of Duties 34
5.3. Personnel Controls 35
5.3.1. Qualifications, Experience, and Clearance Requirements 35
5.3.2. Background Check Procedures 35
5.3.3. Training Requirements 35
5.3.4. Retraining Frequency and Requirements 35
5.3.5. Job Rotation Frequency and Sequence 35
5.3.6. Sanctions for Unauthorized Actions 35
5.3.7. Independent Contractor Requirements 35
5.3.8. Documentation Supplied to Personnel 35
5.4. Audit Logging Procedures 36
5.4.1. Types of Events Recorded 36
5.4.2. Frequency of Processing Log 36
5.4.3. Retention Period for Audit Log 36
5.4.4. Protection of Audit Log 36
5.4.5. Audit Log Backup Procedures 36

5.4.6. Audit Collection System (Internal vs. External) 37
5.4.7. Notification to Event-Causing Subject 37
5.4.8. Vulnerability Assessments 37
5.5. Records Archival 37
5.5.1. Types of Records Archived 37
5.5.2. Retention Period for Archive 37
5.5.3. Protection of Archive 37
5.5.4. Archive Backup Procedures 37
5.5.5. Requirements for Time-Stamping of Records 38
5.5.6. Archive Collection System (Internal or External) 38
5.5.7. Procedures to Obtain and Verify Archive Information 38
5.6. Key Changeover 38
5.7. Compromise and Disaster Recovery 38
5.7.1. Incident and Compromise Handling Procedures 38
5.7.2. Computing Resources, Software, and/or Data are corrupted 38
5.7.3. Entity Private Key Compromise Procedures 38
5.7.4. Business Continuity Capabilities after a Disaster 38
5.8. CA or RA Termination 39
5.8.1. Final termination - MSA responsibility 39
5.8.2. Transfer of FL-MSCA or FL-CP responsibility 39
6. TECHNICAL SECURITY CONTROLS 39
6.1. Key Pair Generation and Installation 39
6.1.1. Key Pair Generation 39
6.1.1.1. Member state key pair generation 39
6.1.1.2. Key pair generation for card personalisation 39
6.1.1.3. Key pair generation for transport 40
6.1.2. Private Key Delivery to Subscriber 40
6.1.3. Public Key Delivery to Certificate Issuer 40
6.1.4. CA Public Key Delivery to Relying Parties 40
6.1.5. Key Sizes 40
6.1.6. Public Key Parameters Generation and Quality Checking 40
6.1.7. Key Usage Purposes 40
6.2. Private Key Protection and Cryptographic Module Engineering Controls 41
6.2.1. Cryptographic Module Standards and Controls 41
6.2.2. Private Key (n out of m) Multi-Person Control 41
6.2.3. Private Key Escrow 41
6.2.4. Private Key Backup 41
6.2.5. Private Key Archival 41
6.2.6. Private Key Transfer into or from a Cryptographic Module 41
6.2.7. Private Key Storage on Cryptographic Module 41
6.2.8. Method of Activating Private Key 41
6.2.9. Method of Deactivating Private Key 42
6.2.10. Method of Destroying Private Key 42
6.2.11. Cryptographic Module Rating 42
6.3. Other Aspects of Key Pair Management 42
6.3.1. Public Key Archival 42
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 42
6.4. Activation Data 43
6.4.1. Activation Data Generation and Installation 43
6.4.2. Activation Data Protection 43
6.4.3. Other Aspects of Activation Data 43
6.5. Computer Security Controls 43
6.5.1. Specific Computer Security Technical Requirements 43
6.5.2. Computer Security Rating 43
6.6. Life Cycle Technical Controls 43
6.6.1. System Development Controls 43

6.6.2. Security Management Controls 43
6.6.3. Life Cycle Security Controls 44
6.7. Network Security Controls 44
6.8. Time-Stamping 44
7. CERTIFICATE, CRL, AND OCSP PROFILES 44
7.1. Certificate Profile 44
7.1.1. Version Number(s) 44
7.1.2. Certificate Extensions 44
7.1.3. Algorithm Object Identifiers 44
7.1.4. Name Forms 44
7.1.5. Name Constraints 44
7.1.6. Certificate Policy Object Identifier 44
7.1.7. Usage of Policy Constraints Extension 44
7.1.8. Policy Qualifiers Syntax and Semantics 44
7.1.9. Processing Semantics for the Critical Certificate Policies Extension 45
7.2. CRL Profile 45
7.2.1. Version Number(s) 45
7.2.2. CRL and CRL Entry Extensions 45
7.3. OCSP Profile 45
7.3.1. Version Number(s) 45
7.3.2. OCSP Extensions 45
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 45
8.1. Frequency or Circumstances of Assessment 45
8.2. Identity/Qualifications of Assessor 45
8.3. Assessor's Relationship to Assessed Entity 46
8.4. Topics Covered by Assessment 46
8.5. Actions Taken as a Result of Deficiency 46
8.6. Communication of Results 46
9. OTHER BUSINESS AND LEGAL MATTERS 46
9.1. Fees 46
9.1.1. Certificate Issuance or Renewal Fees 47
9.1.2. Certificate Access Fees 47
9.1.3. Revocation or Status Information Access Fees 47
9.1.4. Fees for Other Services 47
9.1.5. Refund Policy 47
9.2. Financial Responsibility 47
9.2.1. Insurance Coverage 47
9.2.2. Other Assets 47
9.2.3. Insurance or Warranty Coverage for End-Entities 47
9.3. Confidentiality of Business Information 47
9.3.1. Scope of Confidential Information 47
9.3.2. Information Not Within the Scope of Confidential Information 47
9.3.3. Responsibility to Protect Confidential Information 48
9.4. Privacy of Personal Information 48
9.4.1. Privacy Plan 48
9.4.2. Information Treated as Private 48
9.4.3. Information not Deemed Private 48
9.4.4. Responsibility to Protect Private Information 48
9.4.5. Notice and Consent to use Private Information 48
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 48
9.4.7. Other Information Disclosure Circumstances 48
9.5. Intellectual Property Rights 48
9.6. Representations and Warranties 49
9.6.1. CA Representations and Warranties 49
9.6.2. RA Representations and Warranties 49
9.6.3. Subscriber Representations and Warranties 49

9.6.4. Relying Party Representations and Warranties 49
9.6.5. Representations and Warranties of other Participants 49
9.7. Disclaimers of Warranties 49
9.8. Limitations of Liability 49
9.9. Indemnities 49
9.10. Term and Termination 49
9.10.1. Term 49
9.10.2. Termination 49
9.10.3. Effect of Termination and Survival 50
9.11. Individual Notices and Communications with Participants 50
9.12. Amendments 50
9.12.1. Procedures for Amendment 50
9.12.1.1. Items that may change without notification 50
9.12.1.2. Changes with notification 50
9.12.1.3. Comment period 50
9.12.1.4. Whom to inform 50
9.12.1.5. Period for final change notice 51
9.12.1.6. Changes requiring a new ERCA approval 51
9.12.2. Notification Mechanism and Period 51
9.12.3. Circumstances under which OID must be changed 51
9.13. Dispute Resolution Provisions 51
9.14. Governing Law 51
9.15. Compliance with Applicable Law 51
9.16. Miscellaneous Provisions 51
9.16.1. Entire Agreement 51
9.16.2. Assignment 51
9.16.3. Severability 52
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) 52
9.16.5. Force Majeure 52
9.17. Other Provisions 52
REFERENCES 53
LIST OF FIGURES 53
LIST OF TABLES 53

1. INTRODUCTION

1.1. Overview

This document on hand is the Liechtenstein Certification Authority Policy for the smart tachograph system in accordance with the following EU documents:

- Regulation (EU) No 165/2014 [11]
- Commission Implementing Regulation (EU) 2016/799 [1]
- Commission Implementing Regulation (EU) 2018/502 amending Implementing Regulation (EU) 2016/799 [12]
- Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy [3]

1.1.1. Smart Tachograph – the Second Generation of Digital Tachographs

Smart tachographs are the second generation of on-board mandatory digital recorders to enforce the EU legislation on professional drivers driving and resting times (social regulation). The new features make full use of advanced digital technologies such as satellite positioning and short range communication for road enforcers, through a harmonised Intelligent Transport System interface. It will allow automatic recording of start and final location of journeys and will enable remote access to some tachograph data via wireless data transmission to control authorities.

The smart tachograph will be mandatory the 15th June 2019.

1.1.2. Liechtenstein – PKI Member State and EEA EFTA state

Liechtenstein is a Member State of Smart Tachograph Public Key Infrastructure (PKI) set up by the ERCA, based on the EU Regulation [11] and the related EU Commission Implementing Regulations [1], [12].

Liechtenstein, as an EEA EFTA State, meaning being a member of the European Free Trade Association (EFTA) and being a party of the Agreement on the European Economic Area (EEA). The Smart Tachograph EU regulations are part of the EEA Annex XIII [14].

Based on this, Liechtenstein is participating the Smart Tachograph Public Key Infrastructure in the Member State role.

1.1.3. No Component Manufacturers in Liechtenstein

The Smart Tachograph Public Key Infrastructure (PKI) set up by the ERCA contains specifications for certificates and keys for component manufacturers. Following [1], component means any of the following elements: the Vehicle Unit (VU), the Motion Sensor (MoS), the Tachograph Card, the Record Sheet, the external GNSS facility (EGF) and the Remote Early Detection Facility.

As there are no component manufactures in Liechtenstein, the functionality for the delivery of Smart Tachograph certificates for Vehicle Units (VU), Motion Sensors (MoS) and External GNSS Facilities (EGF) is not implemented on national level. Device Manufacturer address their certification and key requests to the responsible Member State Certificate Authority.

The applicability of this Certification Policy and Certification Practice Statement on hand is therefore limited to Card Issuing, Card Personalisation and interoperability of cards with EU conform Tachograph VUs, MoSs and EGFs.

1.1.4. Liechtenstein specific PKI role allocation

The Commission Implementing Regulation [1] as well as the EU Certification Policy [3] already define the roles and responsibilities for the effective hierarchy and the PKI participation. Following the EU regulations, the roles on European level are given. The following Liechtenstein specific roles are to be appointed:

- Liechtenstein Member State Authority (FL-MSA)

- Liechtenstein Member State Certificate Authority (FL-MSCA)
- (No Registration Authority (RA))
- Subscriber (FL-CP)
- Participants (Liechtenstein Tachograph Card Holder)

A particularity, deviating from the defined roles, is the relocation of the personal examination (company audit) for card applications to an additional role, the Card Issuing Authority (FL-CIA). The Applicants (Tachograph Card Requester) role has been separated from the Relying Parties (Tachograph Card Holder) as they are not fully congruent, in case of rejection of card application.

An overview of the roles and hierarchies involved in the Liechtenstein Tachograph Certification can be found in the following figure.

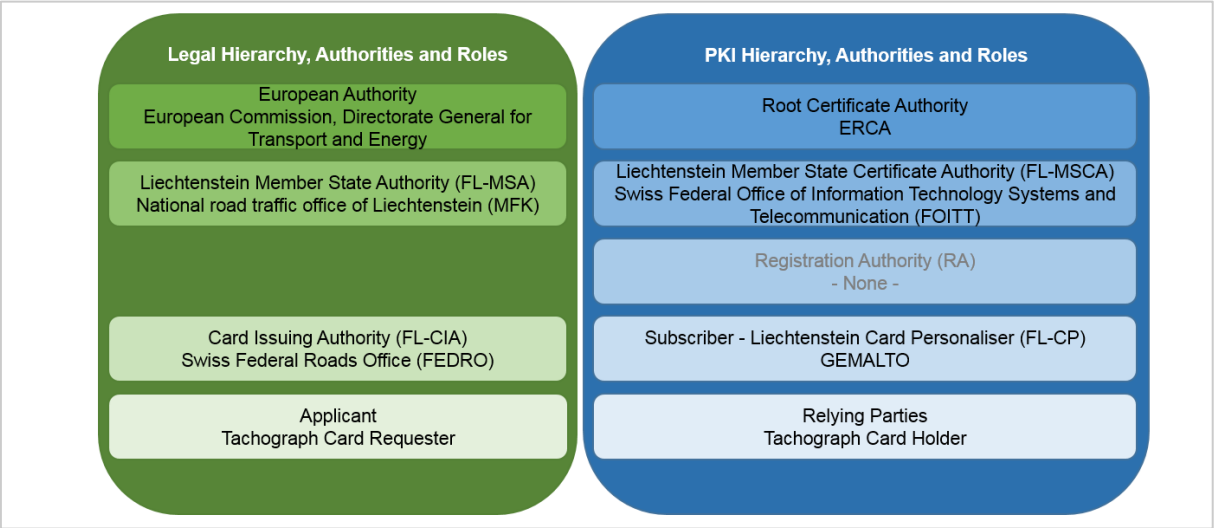

Figure 1: Legal Hierarchy and PKI roles for Liechtenstein

Note: Liechtenstein delegated:

- *The Card Issuing Authority to the Swiss Federal Roads Office (FEDRO)*
- *The Member State Certification Authority to the Swiss Federal Office of Information Technology Systems and Telecommunication (FOITT)*

1.1.5. Liechtenstein specific Certificates and Keys in use

The Public Key Infrastructure (PKI) for the Liechtenstein Smart Tachograph system consists of the following three levels:

- the European level, managed by the European Root Certificate Authority (ERCA).
- the Member State level, managed by the Liechtenstein Member State Certificate Authority (FL-MSCA)
- the equipment level, managed by the Liechtenstein Card Personaliser (FL-CP)

Each level is provided with its own certificates, as shown in the following Figure.

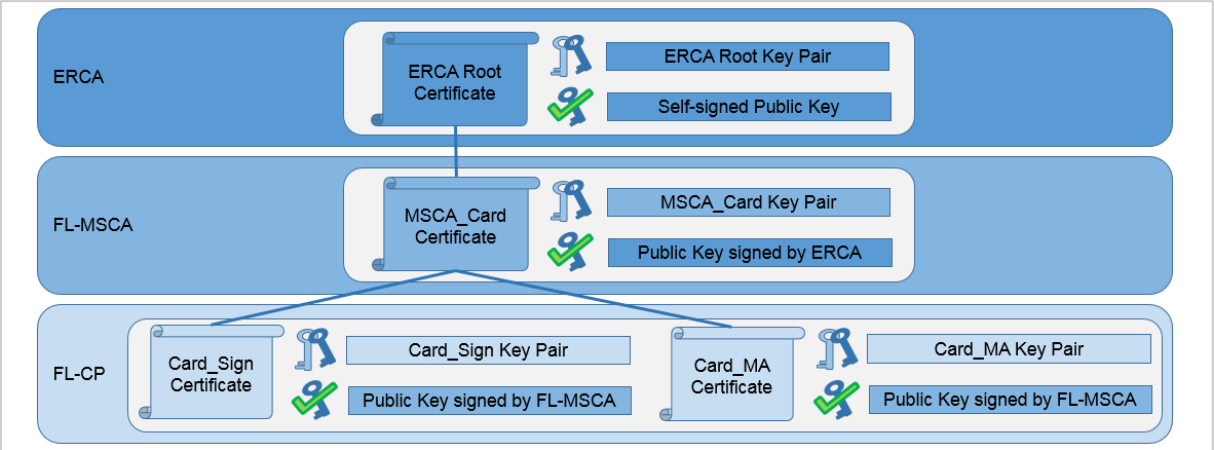

Figure 2: Liechtenstein specific certificates of the Tachograph PKI

The ERCA creates a single ECC (Elliptic Curve Cryptography) key pair that serves as the root key pair of the entire PKI. The ERCA also creates a self-signed root certificate containing the root public key. The ERCA uses the corresponding private key to sign FL-MSCA certificates on request.

The FL-MSCA needs to issue certificates for tachograph cards. The FL-MSCA creates an MSCA_Card key pair and asks the ERCA to sign the public key and send the corresponding certificate as a response. Subsequently, the FL-MSCA uses the corresponding private keys to sign equipment keys.

The FL-CP creates a Card_MA key pair for mutual authentication as well as a Card_Sign key pair (for workshop cards and driver cards) to sign downloaded data. The generated public keys are sent to the FL-MSCA for signing and generating of the respective certificate.

Note: The signature on the certificate shall be created over the encoded certificate body, including the certificate body tag and length. The signature algorithm shall be ECDSA, using the hashing algorithm linked to the key size of the signing authority (see [1] CSM_50). The signature format shall be plain.

The following picture illustrates who is responsible for generating which keys within the Liechtenstein Tachograph PKI:

Figure 3: Liechtenstein specific key generation responsibilities of the Tachograph PKI

Note: There is an additional certificate in use for the communication between FL-CIA, FL-CP and FL-MSCA, for Card-CSR and Card-CSR responses (see also sections 2.1 and 3.1.1.3). The used DocSigner certificate secures that the requests and responses are sent by authorised sender only and that the request content has not been manipulated. The details of the DocSigner certificate are laid down in the corresponding certification policy [4] and certification practice statement [5] and are not object of the document on hand.

1.1.6. Liechtenstein specific Requests and Responses

The Tachograph PKI is based on three Liechtenstein specific requests:

- Certificate Signing Request (CSR) = FL-MSCA asks ERCA to sign MSCA_Card.PK and send corresponding certificate (request triggered by the end of validity period of the former certificate)
- Key Distribution Requests (KDR) = FL-MSCA asks ERCA to distribute the Master key $K_{M\text{-}WC}$ resp. KM_{DSRC} and the corresponding version number (request triggered by the end of validity period of the former Master keys)
- Card Certificate Signing Request (Card-CSR) = FL-CP asks FL-MSCA sign Card_MA.PK and if needed (for driver cards and workshop cards) Card_Sign.PK and send corresponding certificate (request triggered by the Card Personalisation Request sent from FL-CIA to FL-CP)

The following picture illustrates Liechtenstein specific requests and responses:

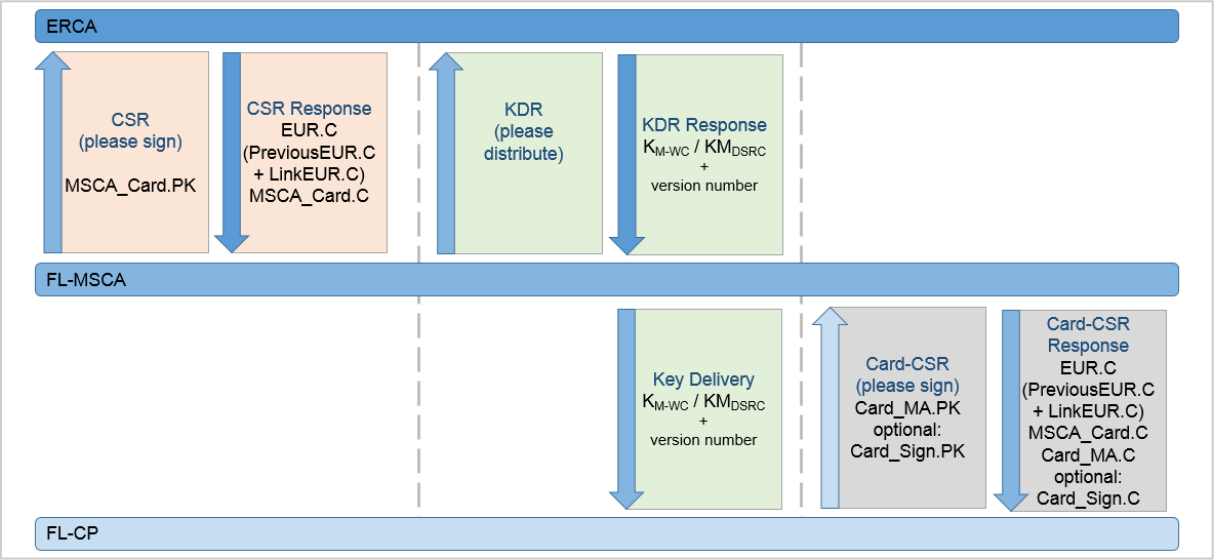

Figure 4: Liechtenstein specific requests and responses of the Tachograph PKI

Note: The ERCA is generating new root key pairs and corresponding EUR.C certificates every 17 years. The validity of the EUR.C certificate is 34 years. Due to the overlapping validity period, as of 2034, two certificates will always be valid at the same time. In Addition the ERCA will provide a link certificate containing the new ERCA public key signed with the previous ERCA private key. The link certificate offers equipment issued under previous certification a method to trust equipment issued under new certification.

In addition, this overlapping validity of the root key also affects the validity and use of the work-shop cards master key ($K_{M\text{-}WC}$) and the DSRC master key (KM_{DSRC}). Related cards (workshop cards and control cards) must be equipped with up to three $K_{M\text{-}WC}$ keys resp. KM_{DSRC} keys. The corresponding version number is used to distinguish the keys (for detailed descriptions see [1]).

1.1.7. The Transition from First Generation to Second Generation

The first generation digital tachograph system has been deployed since 1 May 2006. It may be used until its end of life for domestic transportation. For international transportation, instead, starting from March 2031 (15 years after the entry into force of the European Commission Regulation [1]), all vehicles shall be equipped with a compliant second generation smart tachograph, introduced by the European Commission Regulation.

Starting from its introduction date, second generation recording equipment shall be installed in vehicles registered for the first time, and second generation tachograph cards shall be issued.

In order to foster a smooth introduction of the second generation tachograph system:

- second generation tachograph cards shall be designed to be also used in first generation vehicle units, and
- replacement of valid first generation tachograph cards at the introduction date shall not be requested

This allows drivers to keep their unique driver card and use both systems with it.

Therefore, second generation tachograph cards shall contain two different card applications - first generation (TACHO) and second generation (TACHO_G2) application. Furthermore, in addition to the second generation keys and certificates, tachograph cards shall also contain the keys and certificates of the first generation - equipment key EQT.PK, Equipment certificate EQT.C, Member State certificate MS.C and European public key EUR.PK. And in case of workshop cards additionally the master key Km_{WC}.

For the period before the introduction date of the second generation Tachograph PKI, the following rules are set by the European Commission (see Requirements MIG_020, MIG_021 in [1]):

- Member states shall be able to issue second generation workshop cards at the latest 3 months before the introduction date.
- Member States shall be able to issue all types of second generation tachograph cards at the latest 1 month before the introduction date.

Note: Second generation recording equipment shall only be calibrated using second generation workshop cards.

1.1.8. The Policy Transition from First Generation to Second Generation

The second generation Liechtenstein Tachograph Certification Policy and Certification Practice Statement on hand is not meant to replace the first generation Liechtenstein Tachograph Policy [13]. In the transitional phase, in which first generation and second generation devices are in use for international transportation, the former Policy [13] continues to apply. After the transitional phase, at the earliest from March 2031 (see section 1.1.7), the Policy of the first generation will be suspended.

1.1.9. Particularities when using Abbreviations in this Policy

This document applies some special rules for the use of abbreviations. These rules ensure the uniformity and uniqueness of the abbreviations used throughout the document.

1.1.9.1. The Abbreviation CP

For use in this document, the abbreviation "CP" could be used at least for the following terms:

- Card Personaliser
- Component Personalisers
- Certificate Policy

As there are no other Component Personalisers than Card Personalisers involved in the PKI regulations touched by the Certification Policy and Certification Practice Statement on hand, CP is used for the Card Personaliser exclusively. To avoid any confusion, the use of the abbreviation "CP" is additionally limited to the use within "FL-CP". FL-CP is the Liechtenstein Card Personaliser, acting according to this Policy on Liechtenstein national level.

Exceptions to this rule can be found only in the referenced file names and web links that use the abbreviation CP for Certificate Policy.

1.1.9.2. The Abbreviations for the Master Keys KM_{DSRC} and K_{M-WC}

This policy deals with two master keys for the second generation Tachograph systems, issued by the ERCA:

- KM_{DSRC}: AES Master Key of the second generation Tachograph system, for Dedicated Short Range Communication; Key inserted in control cards and workshop cards for the verification of the integrity and authenticity of data sent by a VU over the remote communication channel and to decrypt this data.
- K_{M-WC}: AES Master Key of the second generation Tachograph system, inserted in workshop cards, allowing a Vehicle Unit to derive the Motion Sensor Master Key if a workshop card is inserted into the Vehicle Unit.

The abbreviation KM_{DSRC} is used exactly this way in the Commission Implementing Regulation [1]. In deviation, the European Policy [3] uses K_{DSRC} (without the use of the letter M) instead of $KM_{DSRC.}$ Throughout this Certification Policy and Certification Practice Statement on hand, the used second generation DSRC master keys is named as $KM_{DSRC.}$

For first generation Tachograph systems there were no DSRC Master keys introduced, but there was a Master Key for workshop cards defined already:

- $Km_{WC:}$ TDES key of the first generation Tachograph system, inserted in workshop cards

The only section this "old" master key is mentioned within this policy is 1.1.7, where the transition from first to second generation is treated. But nevertheless it is important that these different keys are not mixed up, despite the very similar notation.

1.1.9.3. The Abbreviations MSA / FL-MSA, MSCA / FL-MSCA, FL-CIA, FL-CP

The Commission Implementing Regulation [1] as well as the European Certification Policy [3] define roles, rules and regulations for the Member State Authorities (MSA) and the Member State Certificate Authorities (MSCA). Whenever theses specifications are used for the Certification Policy and Certification Practice Statement on hand, meaning MSAs resp. MSCAs in general, they are used in unchanged form (e.g. see section 1.3.1.2). For the Liechtenstein specific regulations, which are covered in this document, the abbreviations FL-MSA and FL-MSCA are used for the appointed organisations in charge.

Based on this argumentation in consistency to the abbreviations named above, the following additional Liechtenstein specific roles are named as follows:

- FL-CIA Liechtenstein Card Issuing Authority
- FL-CP Liechtenstein Card Personaliser

1.1.9.4. The Abbreviations MSCA_Card and MSCA_VU-EGF

The Commission Implementing Regulation [1] delimits MSCAs as MSCA_Card and MSCA_VU-EGF according to their responsibilities.

An MSCA responsible for the issuance of tachograph card certificates is named MSCA_Card; an MSCA responsible for the issuance of VU and/or EGF certificates is named MSCA_VU-EGF.

Following the definition of the Commission Implementing Regulation [1] and taking into account the limitations of the Liechtenstein responsibilities described in 1.1.3:

- the FL-MSCA is an MSCA_Card, and
- there is no appointed MSCA_VU-EGF for Liechtenstein

For the Certification Policy and Certification Practice Statement on hand this means that the two abbreviations FL-MSCA and MSCA_Card are of the same meaning, and designate the only Certification Authority appointed for Liechtenstein (see section 1.5.3).

The usage of the abbreviation MSCA_Card is limited to the parts of this document recalling the regulations which expressly use this term and which are applicable to this document (e.g. for naming the MSCA_Card key pair).

1.2. Document Name and Identification

The name of the document on hand is "Smart Tachographs Liechtenstein Certificate Policy and Certification Practice Statement"

The name of the file of the document on hand is "SMART_TACHOGRAPHS_LIECHTENSTEIN_CP_AND_CPS.pdf".

The OID is 2.16.756.1.17.3.82.2 (see also section 7.1.6)

The published and currently valid version can be found under the following link: http://www.dfs.astra.admin.ch.

1.3. PKI Participants

This chapter introduces the roles and responsibilities of PKI participants. A simplified overview of the PKI roles can also be found in section 1.1.4.

1.3.1. Certification Authorities

1.3.1.1. European Root Certification Authority (ERCA)

The ERCA is the root Certification Authority (CA) that signs public key MSCA certificates. It operates the following component services (see [2]): registration service, certificate generation service, dissemination service.

The ERCA generates PKI root key pairs and respective certificates, along with link certificates to create a chain of trust between different root certificates.

The ERCA is also the entity generating, managing and distributing on request the symmetric master keys, i.e. the Motion Sensor Master Key–VU part ($K_{M\text{-}VU}$), the Motion Sensor Master Key-Workshop Card part ($K_{M\text{-}WC}$) and the DSRC Master Key (KM_{DSRC}).

1.3.1.2. Member State Certificate Authorities (MSCA)

The MSCAs operate as sub-CAs under the ERCA. They sign public key certificates for equipment. For this, they operate a registration service, certificate generation service and dissemination service. The MSCAs receive the certificate requests from component personalisers and disseminate the certificates to these parties. There are two types of MSCA key pair(s) and corresponding MSCA certificate(s): one for the issuance of VU and EGF certificates, called an MSCA_VU-EGF key pair; and one for the issuance of Card certificates, called an MSCA_Card key pair. Each MSCA may request from the ERCA either or both types of MSCA certificate, depending on their responsibilities regarding the issuance of equipment. An MSCA responsible for the issuance of tachograph card certificates is indicated in this document as an MSCA_Card. An MSCA responsible for the issuance of VU and/or EGF certificates is indicated as an MSCA_VU-EGF.

The MSCAs are also the entities requesting symmetric master keys from the ERCA, again depending on their responsibilities. The MSCAs distribute $K_{M\text{-}VU}$ to VU manufacturers, and $K_{M\text{-}WC}$ and KM_{DSRC} to card personalisers. The MSCAs may also use the Motion Sensor Master Key (K_M) to encrypt motion sensor pairing keys (K_P) on request of a motion sensor manufacturer and derive the motion sensor Identification Key (K_{ID}) from K_M, which they then subsequently use to encrypt motion sensor serial numbers on request of a motion sensor manufacturer. Finally, MSCAs may use KM_{DSRC} to derive VU-specific keys by request of a VU manufacturer on basis of the VU serial number.

1.3.1.3. Liechtenstein Member State Certificate Authority (FL-MSCA)

The Liechtenstein MSCA (FL-MSCA) operates as sub-CA under the ERCA as described in the previous chapter. As there are no manufacturers of related equipment in Liechtenstein, the functionality for the delivery of Smart Tachograph certificates for Vehicle Units (VU), Motion Sensors (MoS) and External GNSS Facilities (EGF) is not implemented.

As a result, the FL-MSCA responsibilities are limited to MSCA_Card responsibilities, in particular the responsibilities are:

- sign public key certificates for tachograph cards, and for this:
  - operate a registration service for tachograph cards
  - operate a certificate generation service for tachograph cards and
  - operate a dissemination service for tachograph cards

The FL-MSCA handles the MSCA key pair and corresponding MSCA certificate for the issuance of card certificates, called an MSCA_Card key pair.

The FL-MSCA submits the requests for symmetric master keys KM_{DSRC} and $K_{M\text{-}WC}$ towards ERCA and distributes the received keys to the FL-CP, the Liechtenstein card personaliser.

The FL-MSCA receives the certificate requests from the FL-CP and disseminates the certificates to this party. Additionally, for driver cards and workshop cards, the FL-MSCA ensures that Card_MA and Card_Sign certificates have the same Certificate Effective Date.

As a result of their responsibilities, the FL-MSCA disposes of the following cryptographic keys and certificates, at any moment in time:

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

1.3.2. Registration Authorities

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

1.3.3. Subscribers (End Entities)

The only subscribers to the ERCA public key certification service are the MSCAs.

The only subscribers to the FL-MSCA public key certification service are the component personalisers of the tachograph cards (FL-CP). The component personalisers of the tachograph cards are responsible for the personalisation of the four different types of tachograph cards: driver cards, company cards, workshop cards and control cards.

The tachograph cards contain cryptographic keys and certificates.

The driver cards and workshop cards have two key pairs and corresponding certificates issued by an MSCA_Card, namely:

- a key pair and certificate for mutual authentication, called Card_MA
- a key pair and certificate for signing, called Card_Sign

All cards have the EUR certificate containing the EUR.PK public key to be used for verification of the MSCA_Card certificate. If existing, the previous EUR certificate as well as the link certificate are stored on the cards (see also section 1.1.6). Additionally, for control cards, company cards and workshop cards only, and only if such cards are issued during the first three months of the validity period of a new EUR certificate: cards shall contain the EUR certificate that is two generations older, if existing.

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

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

The control cards also contain KM_{DSRC}.

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

The card personaliser for driver and workshop cards:

- ensures generation of the two card key pairs, for mutual authentication and signing
- performs the certificate application process with the MSCA_Card
- performs the application for $K_{M\text{-}WC}$ and KM_{DSRC} (workshop cards only)
- ensures availability in the card of keys and certificates for mutual authentication and signing (with identical Certificate Effective Date), MoS-VU pairing and DSRC communication decryption and verification of data authenticity (workshop cards only)

The card personaliser for company and control cards:

- ensures generation of the card key pair for mutual authentication
- performs the certificate application process with the MSCA_Card
- performs the application of KM_{DSRC} (control cards only)
- ensures availability in the card of keys and certificates for mutual authentication and DSRC communication decryption and verification of data authenticity (control cards only)

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

Card Type	Card_MA	Card_Sign	$K_{M\text{-}WC}$*	KM_{DSRC}*
Driver Card	X	X		
Company Card	X			
Workshop Card	X	X	X	X
Control Card	X			X

*: In fact a workshop card resp. a control card has up to three $K_{M\text{-}WC}$ keys resp. KM_{DSRC} keys and the corresponding version numbers, as they relate to the root keys and their overlapping validity periods (for more details see [1])

Table 1: Necessary keys on the respective card type

1.3.4. Relying Parties

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

Parties relying on the FL-MSCA certification service are the holder of the tachograph cards:

- natural persons holding a driver card or workshop card
- juristic persons holding a company card or control card

1.3.5. Other Participants

There are no other entities with PKI related services involved.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

The ERCA root certificates and ERCA link certificates shall be used to verify MSCA certificates issued by the ERCA.

The ERCA certificates will be the highest trust point for the PKI and shall be placed in VUs, cards and EGFs, as specified in Appendix 11 [1]. All MSAs and PKI participants (see section 1.3 of the European Root Certificate Policy [3]) shall recognise the ERCA public key certificates, provided they are published by the ERCA according to the requirements in the European Root Certificate Policy [3], chapter 2.

The ERCA shall use its ERCA private keys only for:

- Signing of ERCA root, ERCA link and MSCA certificates, in accordance with Annex IC Appendix 11 [1].

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

- Signing of equipment certificates, in accordance with Annex IC Appendix 11 [1].
- Signing of Certificate Signing Requests (see section 4.1.1)

Note: The Requirement "An MSCA shall use its Member State private keys only for Issuing Certificate Revocation Lists, if such a method is used for providing certificate status information." is not applicable for the FL-MSCA. The FL-MSCA tachograph card certificates described in the document on hand are never revoked or suspended.

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

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

The Card_Sign certificates shall be used to verify the authenticity and integrity of data downloaded from the card.

The Card_Sign private key may only be used to sign data downloaded from the card.

$K_{M\text{-}WC}$ and the corresponding version number shall be provided to component personalisers for their installation respectively in workshop cards.

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

Note: As there are no manufactures of related equipment in Liechtenstein, the functionality for the delivery of Smart Tachograph certificates for Vehicle Units (VU), Motion Sensors (MoS) and External GNSS Facilities (EGF) is not implemented (see chapter 1.3.1.3). Motion sensor manufacturer and vehicle unit manufacturer apply their key request to the responsible Member State Certificate Authority. The card personaliser ensures the availability of the $K_{M\text{-}WC}$ and KM_{DSRC} keys to be used within in the control cards and workshop cards.

1.4.2. Prohibited Certificate Uses

The ERCA shall not use the symmetric master keys for any purpose except distribution to the MSCAs.

The FL-MSCA as well as the FL-CP shall not use the smart tachograph certificates and keys underlying the policy on hand for any purpose except the ones described above.

1.5. Policy Administration

1.5.1. Organization Administering the Document

Each Member State shall set up a Member State Authority (MSA). Each Member State Authority shall lay down and document an MSA certificate policy in conformance with all applicable requirements in the ERCA certificate policy [3].

An MSA certificate policy may consist of a collection of documents, as appropriate to the organisation of its component services. An MSA certificate policy's contents shall comply with all applicable requirements in the ERCA certificate policy [3].

The Liechtenstein Member State Authority (FL-MSA) is the National road traffic office / "Driver and Vehicle Licensing Authority" (Motorfahrzeugkontrolle (MFK) of Liechtenstein):

Motorfahrzeugkontrolle (MFK) Fürstentum Liechtenstein
Gewerbeweg 2,
FL - 9490 Vaduz

Email: info.mfk@llv.li

1.5.2. Contact Person

For the contact address of the FL-MSA (MFK), see Chapter 1.5.1.

1.5.3. Person Determining CPS Suitability for the Policy

The PKI-Manager of the appointed Liechtenstein Member State Certification Authority (FL-MSCA) is determining the suitability of the CPS aspects of the policy on hand.

The appointed FL-MSCA is:
Federal Office of Information Technology Systems and Telecommunication FOITT
Swiss Government PKI
Monbijoustr. 74, CH-3003 Bern
Email: pki-info@bit.admin.ch

1.5.4. CPS approval procedures

See section 9.12 of this document.

1.6. Definitions and Acronyms

Acronym	Definition / Meaning
AES	Advanced Encryption Standard
AdminDir	Directory service of the Swiss Government Certification Authority
AdminPKI	PKI of the Swiss Government Certification Authority
BOV	Begin Of Validity
CA	Certificate Authority
Card-CSR	Card Certificate Signing Request (from FL-CP towards FL-MSCA)
Card_MA	Key pair and certificate for mutual authentication (belonging to tachograph cards)
Card_Sign	Key pair and certificate for signing (belonging to tachograph cards)
FL-CIA	Liechtenstein Card Issuing Authority
FL-CP	Liechtenstein Card Personaliser, personalisers of the tachograph cards
FL-MSA	Liechtenstein Member State Authority
FL-MSCA	Liechtenstein Member State Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request (from FL-MSCA towards ERCA)
DSG	Schweizer Bundesgesetz über den Datenschutz (SR 235.1) (Swiss Federal Act on Data Protection (FADP))
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level (International standard computer security standard used to approve cryptographic modules)
ECC	Elliptic Curve Cryptography
EEA	European Economic Area
EFTA	European Free Trade Association
EGF	External GNSS Facility
EOV	End Of Validity
EQT	Equipment
ERCA	European Root Certification Authority
FADP	Swiss Federal Act on Data Protection (FADP) (Schweizer Bundesgesetz über den Datenschutz (DSG), SR 235.1)
FDF	(Swiss) Federal Department of Finance

FIPS	Federal Information Processing Standard (U.S. government computer security standard used to approve cryptographic modules)
FOITT	Swiss Federal Office of Information Technology Systems and Telecommunication
GebV ASTRA	Gebührenverordnung-ASTRA (SR 172.047.40) (ASTRA fee ordinance)
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
KDM	Key Distribution Message (= KDR Response, containing the keys)
KDR	Key Distribution Request
KM_{DSRC}	Master Key of Dedicated Short Range Communication
K_{M-VU}	Key inserted in vehicle units, allowing a Vehicle Unit to derive the Motion Sensor Master Key if a workshop card is inserted into the Vehicle Unit
K_{M-WC}	Key inserted in workshop cards, allowing a Vehicle Unit to derive the Motion Sensor Master Key if a workshop card is inserted into the Vehicle Unit
Km_{WC}	Master key of the first generation Tachograph system, key to be inserted into workshop cards
MFK	Motorfahrzeugkontrolle (National road traffic office of Liechtenstein)
MoS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
MSCA_Card	MSCA responsible for the issuance of tachograph card certificates, also used to distinguish the Member State Keys of an MSCA_Card (MSCA_Card.PK / MSCA_Card.SK) from the Member State Keys of an MSCA_VU-EGF.
MSCA_VU-EGF	MSCA responsible for the issuance of VU and/or EGF certificates
NTP	Network Time Protocol
OID	(globally unique) Object Identifier
OCSP	Online Certificate Status Protocol
LDAP	Lightweight Directory Access Protocol, protocol standard for interacting with directory servers, mainly used for authentication and storing information about users, groups, and applications.
PK	Public Key
PKI	Public Key Infrastructure
RA	Registration Authority
SK	Secret Key (= Private Key)
SR	Systematische Sammlung des Bundesrechts (Swiss Classified Compilation)
TDES	Triple Data Encryption Standard
TSA	Time Stamping Authority
UPS	Uninterruptible Power Supply
VU	Vehicle Unit
ZertES	Bundesgesetz über die elektronische Signatur (SR 943.03) (Federal law on the electronic signature)

Table 2: Acronyms and meanings

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The FL-MSA shall be responsible for the Liechtenstein Tachograph content on the public website http://www.dfs.astra.admin.ch, which shall be the repository for FL-MSA documents. The FL-MSA certificates and certificate status information are part of the ERCA repository described in section 2.1 of the European Policy [3].

The FL-MSCA shall be responsible for the PKI's web site http://www.pki.admin.ch, which shall be the repository for FL-MSCA documents, and certificate status information.

The FL-MSCA shall be responsible for storing all issued equipment certificates in the directory service AdminDir. AdminDir is a trusted source, i.e. all data therein has been formally verified and may be used within certificates without additional validation. AdminDir is available from the Swiss federal administration's Intranet or using LDAP. The public version of AdminDir is accessible from the Internet using LDAP.

The DocSigner Certificates used for the Card Personalisation Request (by FL-CIA towards FL-CP), the Card Certificate Signing Request (by FL-CP towards FL-MSCA) and the Card Certificate Signing Response (by FL-MSCA towards FL-CP) are issued by the FL-MSCA in their AdminPKI role (see also section 3.1.1.3). DocSigner Certificates and documents are stored in the AdminDir, mentioned above.

2.2. Publication of Certification Information

The FL-MSA shall publish the following information on the website http://www.dfs.astra.admin.ch:

- "Smart tachographs Liechtenstein certificate policy and certification practice statement"
- Policy and certification practice statement change history
- Reference links to the ERCA publications and policy
- Reference links to the relevant FL-MSCA publications and documentations

By publishing the information, the FL-MSA certifies that the information stated in the certificate is ERCA compliant (verified and accepted) and was verified in accordance with this policy and practice statement.

2.3. Time or Frequency of Publication

Information relating to changes in this policy shall be published according to the schedule defined by the change (amendment) procedures laid down in section 9.12 of this document. The FL-MSCA shall bring the list of issued certificates, the certificate and key status information up to date immediately upon executing a key ceremony.

2.4. Access Controls on Repositories

The FL-MSA shall make its information on http://www.dfs.astra.admin.ch public available in a read-only manner.

3. IDENTIFICATION AND AUTHENTICATION

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

3.1. Naming

3.1.1. Types of Names

3.1.1.1. Certificate Signing Request

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

Entity	Identifier	Construction
ERCA	Certification Authority Key Identifier (KID)	Nation numeric (253) Nation alpha (EC) Key serial number (unique value) Additional info (PRODUCTIVE KEY) CA identifier (1)
FL-MSCA	Certification Authority Key Identifier (KID)	Nation numeric (13) Nation alpha (FL) Key serial number (unique value) Additional info (PRODUCTIVE KEY) CA identifier (1)

Table 3: Identifiers for certificate issuers and subjects

3.1.1.2. Key Distribution Requests and Key Distribution Messages

The key identifier value of the Key Distribution Requests (KDR) and Key Distribution Messages (KDM = KDR Response) towards ERCA is determined according to section 3.1.1.1 as follows:

- NationNumeric: 13
- NationAlpha: FL
- keySerialNumber: unique for the requesting entity
- additionalInfo: KR (for Key Request)
- CA identifier: 1

Note: The FL-MSCA uses Key Distribution Requests (KDR) only for $K_{M\text{-}WC}$ and KM_{DSRC}. The complete structure of a KDR can be found in the European Policy [3], section 4.2.1. The distinction of the requested key is done, as described there, via the "Message Recipient Authorization" data object. It contains the key type "27" for $K_{M\text{-}WC}$ resp. "09" for KM_{DSRC}.

3.1.1.3. Document Signer Certification Request

The DocSigner Certificate is issued by the FL-MSCA and is used for signing the Card Personalisation Requests (FL-CIA / FL-CP) and the Card Certificate Signing Request (Card-CSR) and Responses (FL-MSCA / FL-CP). The Certification Authority for the DocSigner Certificate, the "Swiss Government Regular CA 01", is part of the FL-MSCA. The DocSigner key is a soft token with a 2048 length, hashed with the SHA-256 algorithm. The distinguished names (DN) used for the smart tachograph requests are:

Entity	DN (Distinguished Name)
FL-CIA	DFS-CIA FL
FL-CP	DFS-CP FL
FL-MSCA	DFS-CA FL

Table 4: Identifiers of the DocSigner certificate

Note: The details of the DocSigner Certificate are laid down in the corresponding certification policy [4] and certification practice statement [5] and are not object of the document on hand.

3.1.1.4. Card Personalisation Request

The FL-CIA make use of a specific signature algorithm as well as of the Certificate Holder Reference (CHR) within Card Personalisation Request assigned to the FL-CP. The identifier of the issuer and subject are embedded in the signature in the following way:

Field	Meaning	Additional information
ET	Equipment Type	
BOV	Begin Of Validity	
EOV	End Of Validity	
CHR	Certificate Holder Reference	

S_{out}	Order Signature Value	including S_{in}=Input Data Signature, including issuer and subject fields as stated above

Table 5: Identifier of the Card Personalisation Request

Note: The identification of the natural and juristic persons requesting cards as well as the corresponding permission validation is done by the FL-CIA. The person identifier are part of the Card Personalisation Request. The person identifiers are not used for any request identification and validation.

3.1.1.5. Card Certificate Signing Request

The FL-CP sends Card Certificate Signing Requests (Card-CSRs) to the FL-MSCA in order to apply card certificates for driver cards, company cards, workshop cards and control cards. The following identifiers are used for the issuer and subject of card certification request:

Identifier	Value / Content
CPInformation	CP FL
SequenceNumber	Unique Identifier of the Card Certificate Signing Request
CardOrderInformation	Signed content of the card personalisation request
RSAPublicKey	EQT.PK
ECPublicKey	Card_MA.PK
ECPublicKey	Card_Sign.PK (for driver cards and workshop cards)

Table 6: Identifier of the Card Certification Request

3.1.2. Need for Names to be Meaningful

The names of the certificates subjects are given by ERCA, FL-MSA and FL-MSCA as well as by the national register of the tachograph cards as described in the section above. There is no field of application for the stipulation of need for names to be meaningful.

3.1.3. Anonymity or Pseudonymity of Subscribers

The only subscriber is the appointed FL-CP (see section 1.3.3). The FL-CP is not anonymous. The FL-CP is as well not unknown due to the use of a pseudonym.

In addition, the subjects of the certificates are not personal in nature and do not enable to draw conclusions about the person (natural or juristic) holding the certificate. On that note, pseudonyms are used for identification of certification subjects. Anonymity is not allowed.

3.1.4. Rules for Interpreting Various Name Forms

All name forms, name interpretation and character sets are used conforming to the specifications in Appendix 1C, Annex 1 [1].

3.1.5. Uniqueness of Names

Subject fields in all certificates shall be unique in such a manner that all valid certificates with identical subject fields must belong to the same individual or organisation.

3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

FL-MSCA submitting Certificate Signing Requests (CSRs) shall prove possession of the corresponding private key with an internal signature as requested by ERCA (see [1] and [3]). FL-MSCA submitting key distribution requests (KDR) shall prove possession of the

corresponding private key with an internal signature and an outer signature as requested by ERCA (see [3]).

Card personalisation request submitted by the FL-CIA do not contain private keys, but order value authentication shall be proved by FL-CIA signature.

FL-CP submitting Card Certificate Signing Requests (Card-CSRs) shall prove possession of the corresponding private key with the FL-CP signature and shall prove the integrity and request authentication with the request signature.

For details about the signatures mentioned here, see section 4.1.1.

3.2.2. Authentication of Organization Identity

As the FL-MSCA as well as the FL-CIA are part of the swiss federal administration no authentication processes for FL-MSCA and FL-CIA are implemented.

The FL-MSA delegates contractual and operational tachograph business to the the Swiss Federal Roads Office (FEDRO). FEDRO initially authenticates the only subscriber, the FL-CP, before contracting the collaboration. For the Document Signer Certification Request (see section 3.1.1.3.) the authentication follows the rules laid down in the corresponding certification policy and certification practice statement [5]. During PKI operation every subscriber request (Card Certificate Signing Request, Card-CSR) is checked against the request identifier and the FL-CP signature (see section 3.1.1.5).

For organisations and juristic persons, the FL-CIA rely on the authentication process of the appointed card application authorities for company card, workshop card and control card applications. In detail:

- company cards applications are limited to companies with a valid permission for Liechtenstein road carriers
- workshop card applications are limited to approved assembly sites for the digital tachograph
- control card applications are limited to enforcement authorities

3.2.3. Authentication of Individual Identity

The FL-CIA authenticates natural persons during card application validation and approval process for driver cards based on the already authenticated entries of the national register of drivers and vehicle owners (natural persons must personally present to the authentication for driver's licence application).

3.2.4. Non-Verified Subscriber Information

The only subscriber is the appointed FL-CP (see section 1.3.3). There is no need to define regulations on "unverified subscriber information".

3.2.5. Validation of Authority

The initial determination of permission to act on behalf of an organisation is not part of the card application validation and approval process. Card application for organisations rely on already determined register entries of authorized people.

3.2.6. Criteria for Interoperation

There is no external certificate authority and no interoperating application using cross-certification or unilateral certification in use for the FL-MSCA.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

The Identification and Authentication procedures for re-key requests towards ERCA are defined in the EU Policy [3], section 3.3.

The Identification and Authentication procedures for re-key requests applied by FL-CP towards FL-MSCA shall be the same as those described in section 3.2.

Key generation for tachograph cards is done by FL-CP and therefor tachograph card keys are not subject to key requests.

3.3.2. Identification and Authentication for Re-Key after Revocation

Card certificate revocation is not allowed, see section 3.4.

3.4. Identification and Authentication for Revocation Request

The validation of MSCA certificate revocation requests is defined in the EU Policy [3], section 3.4.

Card certificate revocation is not allowed. Card revocation is handled within the national register of the tachograph cards by the use of card status.

4. CERTIFICATE AND KEY LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a Certificate Application

Certificate Signing Requests (CSR) can only be submitted by MSCAs recognised by their MSA via a compliance statement. The European Authority is responsible for recognising MSAs. Key distribution requests (KDR) towards ERCA are following the same preconditions that are defined for CSRs and therefore KDRs can only be submitted by MSCAs recognised by their MSA.

Card Personalisation Request can only be submitted by the FL-CIA named by the FL-MSA. Card Certificate Signing Requests (Card-CSRs) can only be submitted by the FL-CP named by the FL-MSA.

4.1.2. Enrolment Process and Responsibilities

The enrolment process and responsibilities of the ERCA are described in the EU Policy [3].

The master keys for the tachograph cards shall be handed over from FL-MSCA to FL-CP using the defined and agreed file format and signature rules for master key exchange.

The card personalisation requests data shall be signed by FL-CIA and sent to the FL-CP.

The Card Certificate Signing Requests shall include the untouched and signed personalisation request data and shall contain the card specific keys signed by the FL-CP. The FL-CP shall sign the overall request and sent it to the FL-MSCA.

The FL-MSCA response to the FL-CP Card Certificate Signing Request shall include the requested certificates as part of an overall signed message file.

The FL-MSA is in charge for:

- the naming and if needed contractual binding of the involved parties FL-CIA and FL-CP
- the correct and legal conform implementation and execution of all applicable aspects of the smart tachograph
- the communication towards ERCA in general and the immediate information of the ERCA in case of issues and irregularities in particular

The FL-MSCA is in charge for:

- submitting the Certificate Signing Requests (CSRs) towards ERCA
- submitting the Key Distribution Requests (KDRs) towards ERCA
- the correct and complete data within the CSRs and KDRs
- the transport media for the CSR meeting the ERCA requirements and being readable and in particular not damaged or corrupted

- the CSR and KDR format meeting the ERCA requirements
- the CSR and KDR being duly authorised with an inner and if applicable with an outer signature
- the used Certification Authority Reference within the CSR and KDR being correct and valid
- the used Certificate Holder Reference within a CSR and KDR being correct and valid
- the domain parameters specified in the CSR and KDR meeting the ERCA conditions
- the public point in the CSR meeting the ERCA conditions
- the storage of certificates and keys meeting the ERCA requirements
- the conceptual and implemented key distribution rules meeting the requirements in particular for confidentiality, integrity, and availability
- the key distribution of the master keys for the tachograph cards towards FL-CP
- the receipt and processing of the Card Certificate Signing Request submitted by FL-CP only if the request passed the initial check
- the examination of all incoming Card Certificate Signing Request concerning:
  - correct data format and content completeness
  - order data signature of FL-CIA
  - certification data signature of FL-CP
  - overall request data signature
- the integrity of the overall content of the Card-CSR Response using the agreed DocSigner signature
- the immediate information of the MSA in case of issues and irregularities

The FL-CIA is in charge for:

- the Card Personalisation Request submitting towards FL-CP
- the correctness and completeness of the Card Personalisation Request towards FL-CP
- the authentication of the order information included in the Card Personalisation Request using the FL-CIA signature
- the integrity of the overall content of the Card Personalisation Request using the agreed DocSigner signature
- the immediate information of the MSA in case of issues and irregularities

The FL-CP is in charge for:

- the receipt and processing of the Card Personalisation Request submitted by FL-CIA only if the request passed the initial check
- the examination of all incoming Card Personalisation Request concerning:
  - correct data format and content completeness
  - order data signature of FL-CIA
- the Card Certificate Signing Request submitting towards FL-MSCA
- the correct generation and assignment of the keys used in the Card Certificate Signing Request
- the correct and complete data within the Card Certificate Signing Request
- the authentication of the certification data included in the Card Certificate Signing Request using the FL-CP signature
- the integrity of the overall content of the Card Certificate Signing Request using the agreed DocSigner signature
- the correct card personalisation execution as part of the card creation process including:
  - correct data printed on the cards
  - correct keys and certificates stored on the card chip
- the confirmation of the created cards and used certifications towards FL-CIA
- the immediate information of the FL-CIA in case of issues and irregularities

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. Verification of Key Distribution Message content

For submitter identification and authentication reasons the FL-MSCA examines every incoming Key Distribution Message concerning:

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

4.2.1.2. Verification of Card Personalisation Request content

For submitter identification and authentication reasons the FL-CP examines every incoming Card Personalisation Request concerning:

- the completeness of orderdata
- the correctness and validity of order data signature of FL-CIA
- the absence of error messages

4.2.1.3. Verification of Card Certificate Signing Request content

For submitter identification and authentication reasons the FL-MSCA examines every incoming Card Certificate Signing Request concerning:

- the correctness and validity of order data signature of FL-CIA
- the correctness and validity of certificate signing data signature of FL-CP
- the correctness and validity of the DocSigner signature
- the completeness of key data corresponding to the card type treated in the request
- the correct validity data corresponding to the card type treated in the request
- the absence of error messages

4.2.1.4. Verification of Card CSR Response content

For submitter identification and authentication reasons the FL-CP examines every incoming Card CSR Response concerning:

- the correctness and validity of the order result (certificates)
- the correctness and validity of the DocSigner signature
- the absence of error messages (status)

4.2.2. Approval or Rejection of Certificate Applications

The FL-MSCA shall reject the processing of incoming Key Distribution Message in case verification as described in the section above failed.

The FL-CP shall reject the processing of incoming Card Personalisation Requests in case verification as described in the section above failed.

The FL-MSCA shall reject the processing of incoming Card Certificate Signing Requests in case verification as described in the section above failed.

The FL-CP shall reject the processing of incoming Card CSR Responses in case verification as described in the section above failed.

4.2.3. Time to Process Certificate Applications

A card information module is part of the implementation for the processing of the Card Personalisation Requests and the Card Certificate Signing Requests. The card information module acts as a communication interface between FL-CIA, FL-CP and FL-MSCA. The FL-CIA processes all incoming card applications of the Liechtenstein cardholder and cardholder candidates on a daily business basis. Validated and authenticated applications are summarised into one Card Personalisation Requests and submitted to the card infor-

mation module. The FL-CP receive the Card Personalisation Requests from the card information module and prepare the addressed card personalisation. The FL-CP submits one Card Certificate Signing Request per card. The FL-MSCA receives the Card Certificate Signing Request from the card information module. Validation and processing is completely automated and will be carried out immediately after receipt.

The time to process an incoming card application is part of the FL-MSA service commitment for card applicants. The current valid service commitment is to be found on the internet homepage of the FL-MSA. In example in June 2018 the service commitment for the card delivery of driver cards was three days after receipt of the invoice amount.

Incoming Card Personalisation Request are processed immediately restricted to the working hours. The maximal processing time is contractual ingredient agreed between FL-CP and FL-CIA.

The time to process an incoming Card Certificate Signing Request is part of the service level agreement between FL-CIA and FL-MSCA treating the availability and response times of the involved it systems and components.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

The FL-MSCA validates only once and in general for all requests the validity of the Member State Certificate.

The FL-MSCA validates for every incoming Card Certificate Signing Request:

- the requested card types are valid
- the Begin of Validity (BOV) and End of Validity (EOV) are corresponding to EU requirements concerning the period of validity per card type
- the FL-CIA signature is valid and the authorisation of the personalisation data thus is proofed
- the FL-CP signature is valid and the authorisation of the keys sent is therefore proven
- the request signature is valid and the integrity of the request is therefore proven
- the keys to be signed are cryptographically useable and in particular not damaged or corrupted

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The Card Key Certification is part of the automatically processed reply to the Card Certificate Signing Request. The FL-MSCA sends the reply to the card information module (see section 4.2). The FL-CP uses the reply deposited on the card information module to finish the card creation process.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

4.4.1.1. Certificate Signing Requests (CSRs)

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

- the transport media is readable; i.e. not damaged or corrupted
- the format of the certificate complies with Table 5 in section 7.1 [3]
- all certificate field values match the values requested in the CSR
- the certificate signature can be verified using the ERCA public root key indicated in the CAR field

If any of these checks fail, the MSCA shall abort the process and contact the ERCA. Certificate rejection is managed according to the certificate revocation procedure (see [3] section 4.1.10).

4.4.1.2. Card Certificate Signing Request (Card-CSRs)

The FL-CP shall process the certificate acceptance routine applied to the Card Key Certification Reply before using the delivered certificates for card personalisation and card creation. The FL-CP shall execute the check along the following steps to indicate acceptance:

- the CA Information indicates a trusted reply sender
- the sequence number of the reply pass the check routine
- the reply signature indicates the integrity of the included data
- the keys and certificates are valid and useable, in particular they are not damaged or corrupted
- the received ECC Certificate Constrain match the corresponding field of application of the request

If any of these checks fail, the FL-CP shall abort the process and contact the FL-MSCA. Certificate rejection is managed according to the certificate revocation procedure (see section 4.9).

4.4.2. Publication of the Certificate by the CA

The DocSigner Certificates used for verification of the signatures of the Card Certificate Signing Request are posted to an LDAP repository used by the application handling the requests.

The Card Certificates as part of the Card Key Certification Reply sent to the FL-CP and used for card personalisation are exclusively intended for the usage on the cards. The Card Certificates are not subject of any publication.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The notification of issued Card Certificates is the Card Key Certification Reply passed through the card information module to the FL-CP.

The FL-CP notifies the FL-CIA as soon as a Card Personalisation Request is processed and the associated card is created.

There is no other notification of issued Card Certificates to other entities implemented.

4.5. Key Pair and Certificate Usage

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

The FL-MSCA shall ensure that the FL-MSCA private signing keys are only used for the national Card Certificate Signing Requests for use within the Digital Tachograph system. The FL-MSCA shall ensure that, after certification of the national level keys, the FL-MSCA private signing keys are only used for the production of public key certificates for use within the Digital Tachograph system.

Key escrow is strictly forbidden.

4.5.1. Subscriber Private Key and Certificate Usage

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

The FL-CP shall ensure that master keys, tachograph card keys and tachograph card certificates are only used for tachograph card production as described in the document on hand.

4.5.2. Relying Party Public Key and Certificate Usage

Card user ensure proper application of keys and certificates by ensuring correct usage of their tachograph cards.

Card user shall ensure that the tachograph cards are exclusively used as intended. In particular card user acknowledge that tachograph cards are not transferable and any other usage than for tachograph systems is prohibited.

4.6. Certificate Renewal

Certificate renewal on ERCA and MSCA level, i.e. the extension of the validity period of an existing certificate, is not allowed (see [3] section 4.1.7).

Card Key Certificate renewal is not allowed.

4.6.1. Circumstance for Certificate Renewal

No certificate renewal process implemented.

4.6.2. Who May Request Renewal

No certificate renewal process implemented.

4.6.3. Processing Certificate Renewal Requests

No certificate renewal process implemented.

4.6.4. Notification of New Certificate Issuance to Subscriber

No certificate renewal process implemented.

4.6.5. Conduct constituting acceptance of a renewal certificate

No certificate renewal process implemented.

4.6.6. Publication of the renewal certificate by the CA

No certificate renewal process implemented.

4.6.7. Notification of certificate issuance by the CA to other entities

No certificate renewal process implemented.

4.7. Certificate Re-Key

Certificate re-key means the signing of a new certificate, in replacement of an existing certificate.

MSCA certificate re-key is described in [3] section 4.1.8.

For Card Key Certification no certificate re-key process is in place. Every Card Certificate Signing Request is treated as a new application.

4.7.1. Circumstance for Certificate Re-Key

On a national level, no certificate re-key process is in place.

4.7.2. Who May Request Certification of a New Public Key

On a national level, no certificate re-key process is in place.

4.7.3. Processing Certificate Re-Keying Requests

On a national level, no certificate re-key process is in place.

4.7.4. Notification of New Certificate Issuance to Subscriber

On a national level, no certificate re-key process is in place.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

On a national level, no certificate re-key process is in place.

4.7.6. Publication of the Re-Keyed Certificate by the CA

On a national level, no certificate re-key process is in place.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

On a national level, no certificate re-key process is in place.

4.8. Certificate Modification

Certificate modification is not allowed.

4.8.1. Circumstance for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9. Certificate Revocation and Suspension

Certificates and keys subject to the Certificate Signing Requests and keys subject to the Key Distribution Requests towards ERCA following the revocation process described in [3] section 4.1.10.

Certificates and keys subject to the Card Certificate Signing Request cannot be revoked.

Certificates and keys subject to a compromised or suspected compromised Card Certificate Signing Request shall not be used for card creation and card personalisation.

Provisions in case of key compromise or or suspected key compromise following the national compromise procedure as described in 5.7.3, and may result in at least one of the following provisioning steps:

- issuing of a replacement card containing uncompromised keys
- master key replacement following the ERCA re-key process
- MSCA_Card Certificate replacement following the ERCA certification revocation process

Certificate suspension is not allowed.

4.9.1. Circumstances for Revocation

Not applicable.

4.9.2. Who can Request Revocation

Not applicable.

4.9.3. Procedure for Revocation Request

Not applicable.

4.9.4. Revocation Request Grace Period

Not applicable.

4.9.5. Time within which CA Must Process the Revocation Request

Not applicable.

4.9.6. Revocation Checking Requirement for Relying Parties

Not applicable.

4.9.7. CRL Issuance Frequency (if applicable)

Not applicable.

4.9.8. Maximum Latency for CRLs (if applicable)

Not applicable.

4.9.9. On-Line Revocation/Status Checking Availability

Not applicable.

4.9.10. On-Line Revocation Checking Requirements

Not applicable.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements Re-Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Certificate suspension is not allowed.

4.9.14. Who can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

The FL-MSCA do not offer any certificate status service.

The FL-MSCA certificates used within the tachograph cards are in status "valid" or "expired". The status can be derived directly from the validity date of the certificate. The card validities are managed within the national register of the tachograph cards.

4.10.1. Operational Characteristics

Not applicable.

4.10.2. Service Availability

Not applicable.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

End of Subscription regulations for the ERCA’s certificate signing services are described in [3] section 4.1.12.

An End of subscription on FL-MSCA level is not envisaged.

4.12. Key Escrow and Recovery

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

4.12.1. Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

The FL-MSCA operates its certification infrastructure in an appropriately secured location of the Swiss Federal Office of Information Technology Systems and Telecommunication (FOITT).

5.1.2. Physical Access

Physical access to the certification infrastructure is regulated in Swiss Government PKI access control directive (not publicly available).

Only persons possessing a badge issued by FOITT security administration can enter the secured location with Swiss Government PKI's IT hardware. Access to the location is prohibited for all other persons unless accompanied by an authorized Swiss Government PKI employee.

The secured location is protected by different security mechanisms that are regularly checked.

5.1.3. Power and Air Conditioning

The certification infrastructure is powered through an uninterruptible power supply (UPS) which acts as power conditioner as well.

An air condition system specifically built and run for the secured location ensures constant temperature and humidity control 7x24h.

5.1.4. Water Exposures

The secured location is equipped with water detectors connected to the building's surveillance centre.

5.1.5. Fire Prevention and Protection

The secured location is equipped with smoke and heat detectors connected to the building's surveillance centre.

5.1.6. Media Storage

Not applicable. Data related to the certification infrastructure is backed up in specific servers exclusively (see section 5.1.8).

5.1.7. Waste Disposal

Swiss Government PKI personnel use the appropriate mechanisms depending on the classification of the data held by media for removal, e.g. magnetic and mechanical shredders.

5.1.8. Off-Site Backup

Swiss Government PKI has a backup-site at its disposal from where certification can be continued in case of an emergency. Swiss Government PKI uses an off-site, protected location for storing back-up data.

5.2. Procedural Controls

5.2.1. Trusted Roles

Each of the trusted roles described below is assigned to one person with at least one substitute. All system user rights are restricted according to their role. Role description and role concept are part of non-public documents.

The trusted roles of the responsible Member State Authority FL-MSA are:

- Auditor
- Responsible FL-MSA Representative
- FL-MSA Contact Person
- FL-MSA Trusted courier (delegated to FEDRO)
- FL-MSA Tachograph expert in charge (delegated to FEDRO)

The trusted roles of the Member State Certification Authority FL-MSCA are:

- Head of FL-MSCA
- FL-MSCA PKI Management Board
- FL-MSCA PKI Operations Manager
- FL-MSCA PKI Security Officer
- FL-MSCA PKI Operating
- FL-MSCA PKI Repository Officer
- FL-MSCA Registration Agent

The trusted roles of the Card Personaliser FL-CP are:

- FL-CP Card Personalisation expert in charge
- FL-CP Information Systems Security Officer (ISSO)
- FL-CP Security Administrator
- FL-CP Key Manager
- FL-CP Quality Manager
- FL-CP System Administrator

5.2.2. Number of Persons Required per Task

With the exception of the standard tasks performed by the Operating Team, security critical actions require at least two individuals having different roles (see 5.2.1) to jointly execute the steps.

In particular, the following activities require the presence of two persons in different roles:

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

5.2.3. Identification and Authentication for Each Role

FL-MSCA and FL-CP running a tight access rights management and control for identifying and authenticating its personnel handling the certification processes. The access control uses security mechanisms capable of separating the different trusted roles detailed in 5.2.1 and identifying the specific functions within a role each of the role owners actually fulfils at any time.

5.2.4. Roles Requiring Separation of Duties

The FL-MSCA as well as the FL-CP assign roles to their employees, ensuring that no conflicts regarding the separation of duties arise. In case of FL-MSA e.g. members of the Operating Team shall not be PKI Security Officers and vice versa.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

FL-MSCA and FL-CP are operated by qualified and experienced specialists only. Background checks as specified in 5.3.2 has to be performed for each employee.

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

For FL-MSCA employees the use of PKI hardware and software requires authentication by smartcard with personal PIN. In particular the login to the CA Console application is based on the private Swiss Government Root CA II key stored on the personal smartcard. The access the CA Console application underlies additional password protection.

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

5.3.2. Background Check Procedures

The trusted roles described in section 5.2.1 are in general only given to people:

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

In particular, to get assigned a FL-MSCA or a FL-CP trusted role, staff are subjected to a security review as per the ordinance on security checks for persons (see "Verordnung über die Personensicherheitsprüfungen (PSPV)", only available in German [6]).

5.3.3. Training Requirements

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

5.3.4. Retraining Frequency and Requirements

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

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

5.3.5. Job Rotation Frequency and Sequence

There is no job rotation established.

5.3.6. Sanctions for Unauthorized Actions

Unauthorized actions by FL-MSCA staff are sanctioned as regulated by the federal act on the responsibility of the Swiss confederation, the members of its official bodies and their officers [7].

Unauthorised actions by FL-CP staff are sanctioned according to the labor regulation of FL-CP.

5.3.7. Independent Contractor Requirements

The security requirements for temporary employees or contractor's employees are identical to the ones described in the sections 5.3.1, 5.3.2, 5.3.3, 5.3.4 and 5.3.6.

5.3.8. Documentation Supplied to Personnel

The FL-MSCA staff as well as the FL-CP staff has access to all Liechtenstein Tachograph PKI documents needed to perform their role. In particular, the following documents are available:

- Certificate Policy and Certification Practice Statement (this document)
- Security policies
- Manuals on operation and organization
- Manuals of the hard- and software used by the PKI system and applications.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

All relevant events related to the issuance and maintenance of FKRNG certificate are logged automatically or manually (journals, e.g. for recording entries to/exits from a protected room supervised by SG-PKI) for checking purposes, together with date/time, type, reason for and result of action, name of requester, name(s) of person(s) approving (where applicable).

The specific and detailed list of events that CH-MSCA shall at least log are defined by ERCA within [3] chapter 5.4. In particular, this refers to:

- Initial set up, modification and closure of user accounts,
- system transactions, system starts and system shut downs, system configuration changes
- installation and uninstallation of software, software updates and software components
- data backups and recoveries
- creation of log and transaction data lists
- changes to operational documentation

The specific processes of the FL-CP additionally require the confirmation of the receipt of symmetrical keys according to EU regulation.

The FL-CP is logging window event logs. Log data is archived (live data 3 months / archive data 1 year). Events logged are:

- Initial set up, modification and closure of user accounts,
- system transactions, system starts and system shut downs, system configuration changes

5.4.2. Frequency of Processing Log

Log files are checked as part of a daily verification following the guidelines within the operations manual. The log file check is recorded in a protocol and confirmed by a controller by his signature.

FL-CP log files are checked every three months via logical security audit.

5.4.3. Retention Period for Audit Log

Relevant log files (see section 5.4.1) are retained for at least one year.

5.4.4. Protection of Audit Log

For FL-MSCA log data is signed and stored encrypted on a dedicated server located offsite. For FL-CP log data is protected via access management of the corresponding database.

Only FL-MSCA PKI Security Officers and FL-MSCA PKI Operators can access FL-MSCA log data. Only FL-CP System Administrators and FL-CP Security Administrator can access FL-CP log data.

Auditors get access to log data as part of audits.

5.4.5. Audit Log Backup Procedures

The log files backed up as part of routine backup of the host systems.

The FL-MSCA log files are subject to a daily incremental backup as well as to a weekly full backup.

5.4.6. Audit Collection System (Internal vs. External)

A dedicated server within the FL-MSCA infrastructure resp. within the FL-CP infrastructure collects all log files maintained. A copy of the log files is archived in the security area outside the location of operation. The log data is stored in a way that it can be viewed by authorized persons during the data retention period. The log files are protected against unauthorized access.

5.4.7. Notification to Event-Causing Subject

The log files are monitored by a monitoring system. Serious events shall be reported immediately in writing to the FL-MSA Contact Person and the FL-MSCA PKI Security Officer. The event-causing subject will not be informed.

5.4.8. Vulnerability Assessments

The risk analysis is carried out as part of the creation of the security concepts. The safety requirements concerning the systems of the FL-MSCA and the FL-CP were defined and documented in the respective safety concept and operation manual.

The FL-MSCA security program includes additionally an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Process
- Assesses the sufficiency of the policies, procedures, information systems, and technology in place to counter such threats

A dedicated application analyses FL-MSCA certification infrastructure at least once a week, identifying vulnerabilities and potential attempts at breaching the security of the system. For FL-CP vulnerability scans are performed at least every quarter of a year.

5.5. Records Archival

5.5.1. Types of Records Archived

FL-MSCA all relevant data and log files relating to the issuance and maintenance of certificates. In particular, the following content types are subject to archiving:

- Contractual agreements
- All issued certificates and thus also the public keys of the tachograph cards
- CSR and KDR protocols
- Audit reports

FL-CP archives audit reports.

5.5.2. Retention Period for Archive

Archived data of the FL-MSCA will be kept for at least ten years.

Archived data of the FL-CP will be kept for at least one years.

5.5.3. Protection of Archive

Archived data of the FL-MSCA is stored encrypted on two servers in two separate, secured locations off-site. Access to the archive data is granted to authorized persons in the presence of a second staff member only (four eyes principle).

For FL-CP archived data is protected via access management.

5.5.4. Archive Backup Procedures

For FL-MSCA all data to be archived is copied simultaneously to the off-site back-up servers. For FL-CP data to be archived is copied from time to time to the off-site back-up servers.

5.5.5. Requirements for Time-Stamping of Records

Each event registered, and subsequently archived, gets time-stamped on base of the central date/time reference provided within the local network.

5.5.6. Archive Collection System (Internal or External)

All FL-MSCA data to be archived is integrity protected by hash-values and collected in a specific database running on a server within the operator's central IT infrastructure. The FL-MSCA subsequently archives the DB's contents in a storage area network.

The FL-CP does not operate an archive collection system.

5.5.7. Procedures to Obtain and Verify Archive Information

The archive media are subject of an annual inspection done by the PKI Security Officer in the presence of a second staff member (four eyes principle). The aim of this inspection is to make sure that no damage or loss of data has occured. If any irregularity is detected during the inspection, a new data backup is produced in the shortest possible delay.

5.6. Key Changeover

The EU Policy [3] states concerning "Key Changeover":

"MSCAs shall generate new MSCA key pairs as needed. After a MSCA has generated a new key pair, it shall submit a certificate re-key request as described in section 4.1.8.

The ERCA and MSCAs shall ensure that replacement keys are generated in controlled circumstances and in accordance with the procedures defined in this ERCA certificate policy."

On a national level, for FL-MSA and in particular for FL-MSCA and FL-CP, no certificate re-key process is in place. As a logical consequence, none of the Liechtenstein tachograph PKI participant supports key changeover.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Procedures for incident and compromise handling as well as the business continuity plan are in place. Procedure documentations are not publicly disclosed. These procedures are regularly tested and updated as needed. All backup and recovery systems are tested at least once a year.

5.7.2. Computing Resources, Software, and/or Data are corrupted

All active keys and certificates, exept the card personalisation keys, used by the FL-MSCA and the FL-CP are backed up off-site in at least two backup tokens at all times. All data related to the issuance and maintenance of subscriber certificates is backed up daily as well. Data on the registration and certification processes are backed up incrementally by the CA's databases. A recovery process for backup data in place.

5.7.3. Entity Private Key Compromise Procedures

All key compromise procedures on national level rely on the ERCA master re-key resp. certification revocation process. In the event of compromise or theft of a Liechtenstein private key or a master key, the MSA shall immediately inform the ERCA and the national participants (FL-MSCA / FL-CP). The FL-MSA shall take appropriate measures within a reasonable period of time.

5.7.4. Business Continuity Capabilities after a Disaster

The FL-MSCA is the Swiss federal IT service and data centre operator. The Liechtenstein tachograph PKI services are part of the overall operational continuity management. The continuity management considers handling crisis and restarting as well as restoring services in case of disaster. The continuity management process and role descriptions are not publicly available.

5.8. CA or RA Termination

5.8.1. Final termination - MSA responsibility

Final termination of the FL-MSCA or FL-CP means all service associated to the Liechtenstein tachograph PKI are terminated permanently. It is not applicable for provider changes or re-key processes.

In case of final termination, the FL-MSCA or FL-CP shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the termination of the FL-MSCA's or FL-CP's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

In upfront to the termination of its services the FL-MSCA shall execute at least the following procedures:

- The FL-MSCA or FL-CP shall, without delay, inform the MSA which, without delay, informs all relying parties and the ERCA.
- The FL-MSCA and the FL-CP shall terminate all authorization of subcontractors to act on behalf of the FL-MSCA or FL-CP in the performance of any functions related to the process of issuing certificates or keys.
- The FL-MSCA and the FL-CP shall perform necessary undertakings to transfer obligations for maintaining event log archives for their respective period of time as indicated to the subscriber and relying party.
- The FL-MSCA and the FL-CP shall destroy their private keys and master keys and any backup of these keys.
- The FL-MSCA and the FL-CP shall perform necessary undertakings to maintain and provide continuous access to record archives.

5.8.2. Transfer of FL-MSCA or FL-CP responsibility

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

In this case, the FL-MSA ensures that orderly transfer of responsibilities and assets is carried out. All affected keys and all related backups have to be handed over to the new provider or destroyed in the manner decided by the MSA. After transfer, the old FL-MSCA or FL-CP shall no more be in possession of any key material or backup.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. Member state key pair generation

The FL-MSCA shall generate the member state key pair (MSCA_Card) in accordance with Annex IC Appendix 11 [1].

Member state key pairs are generated by following a key generation script by personnel in trusted roles under (at least) dual person control. The key generation ceremony is documented and logged. Key pair generation is done within a hardware security module (HSM) in which the keys are subsequently stored.

6.1.1.2. Key pair generation for card personalisation

The card personalisation key pairs are exclusively generated by the FL-CP. The FL-CP shall generate the card personalisation key pairs in accordance with Annex IC Appendix 11 [1].

Following the ERCA policy [3], chapter 1.5.3, the FL-MSA requires from FL-CP to use Common Criteria certificated tachograph cards. In particular, the FL-MSA:

- require from FL-CP that any relevant prescription mandated by the Common Criteria security certification of the tachograph card is met during the complete life cycle of the cards.
- require that if equipment private key generation is not done on-board the equipment, private key generation takes place within an HSM that complies with the requirements in section 6.2.

- require that if equipment is capable of generating private or symmetric keys on-board, key generation shall be covered by the security certification of the equipment, ensuring that publicly specified and appropriate cryptographic key generation algorithms are used.

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

6.1.1.3. Key pair generation for transport

The transport key pairs (DocSigner) for the FL-MSCA, the FL-CIA and the FL-CP are provided by the AdminPKI. The handling of these keys corresponds to the specification of the AdminPKI [4] [5].

6.1.2. Private Key Delivery to Subscriber

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

6.1.3. Public Key Delivery to Certificate Issuer

The FL-CP sends card Certificate Signing Requests to the FL-MSCA in order to apply card certificates for driver cards, company cards, workshop cards and control cards (see section 3.1.1.5). The requests are subject of signed files. The FL-MSCA validates the file signature before performing the certification. The request format is agreed between FL-CP and FL-MSCA. The file transfer underlies an encrypted data transfer protocol.

6.1.4. CA Public Key Delivery to Relying Parties

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

6.1.5. Key Sizes

Key sizes are defined in accordance with Annex IC Appendix 11 [1].

In particular the ERCA defined the resulting minimal key length in CSM_50, depending in the length of the European Root Certificate.

The FL-MSCA and FL-CP shall generate keys in the predetermined length.

For the key lengths in specific terms the documentation regarding the "Smart Tachograph Cryptographic keys and digital certificates sample set" states an initial key length (Effective Date is January 1st, 2017, 00:00:00) of the root certificate of 256 bits. As a result of this specification, the initial size of the member state key pair (MSCA_Card.PK / MSCA_Card.SK) and the tachograph key pairs (Card_MA / Card_Sign) has to be as well 256 bit. The initial key size of KM, $K_{M\text{-}WC}$ and KM_{DSRC} is 128 bit.

ERCA decided to extend the key sizes of the European Root Certificate with each new validity period. Starting from 2034 key length of the European Root Certificate will be 384 bit, starting from 2051 key length of the European Root Certificate will be 512 bit.

Key lengths of the FL-MSCA and FL-CP shall grow accordingly.

6.1.6. Public Key Parameters Generation and Quality Checking

All FL-MSCA and FL-CP keys are generated by a HSM conformant to FIPS 140-2 level 3 or EAL 4 augmented.

6.1.7. Key Usage Purposes

The member state key pair is only used for signing the tachograph card certificates.

The tachograph card private keys are used for tachograph card personalisation only.

The tachograph card shall use its Card_MA key pair exclusively to perform mutual authentication and session key agreement towards vehicle units. The Driver cards and workshop cards shall use the private key Card_Sign.SK exclusively to sign downloaded

data files. The Driver cards and workshop cards shall use the corresponding public key Card_Sign.PK exclusively to verify signatures created by the card.

The workshop card motion sensor key is used for workshop cards only.

The DSRC master key is only used for control cards and workshop cards.

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

6.2.1. Cryptographic Module Standards and Controls

All FL-MSCA and FL-CP keys are generated by a HSM conformant to FIPS 140-2 level 3 or EAL 4 augmented (see also section 6.1.6).

6.2.2. Private Key and Symmetric Key Multi-Person Control

All activities on HSMs require the presence of at least two authorized staff members of the FL-MSCA or respectively of the FL-CP.

In particular these are the generation, backup and recovery, activation and deactivation of the keys and the exchange of HSMs.

6.2.3. Key Escrow

Key escrow is strictly forbidden (see also section 4.5).

6.2.4. Private Key Backup

FL-MSCA private keys and symmetric keys are backed up in at least two encrypted backup tokens stored in separate, secure locations off-site. For recovering backup tokens, at least two authorized staff members of the FL-MSCA are required.

6.2.5. Private Key Archival

There aren't any private keys archived.

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

The private Member State keys as well as the DocSigner private keys are not transferred from the cryptographic module, except for the creation of a secure backup on a hardware token.

Master key import and export is only allowed for back-up and recovery purposes. Export of KM_{DSRC} and $K_{M\text{-}WC}$ is allowed in encrypted form only, and only in response to a valid key distribution request from CH-CP by personnel in trusted roles under at least dual person control.

The aspect of transferring private keys from the HSM is not applicable to the private keys of the Card_MA and Card_Sign key pairs. These keys are exclusively stored on the associated tachograph card.

6.2.7. Key Storage on Cryptographic Module

The private Member State keys, master keys and the DocSigner private keys are stored encrypted within the HSMs and are decrypted only when activated.

The aspect of key storage on Cryptographic Module is not applicable to the private keys of the Card_MA and Card_Sign key pairs. These keys are exclusively stored on the associated tachograph card.

6.2.8. Method of Activating Private Key

The private Member State key is activated by the FL-MSA Tachograph expert in charge. The FL-MSA Tachograph expert in charge has to identify himself with the help of a valid Swiss Government Root CA II (resp. the subordinated Swiss Government Regular CA 01 certificate). The login to the CA Console application is based on the private Swiss Government Root CA II key stored on the personal smartcard. The access the CA Console application underlies additional password protection. Key activation is limited to prior certification of the public Member State key by the ERCA.

Beside the FL-MSA Tachograph expert in charge, the FL-MSCA PKI Security Officer and a FL-MSCA PKI Operating role owner (PKI operational staff member) are present at key activation (see also section 5.2 for the procedural controls defined). For CA Console application access PKI operational staff members have to identify themselves as well with the help of their personal smartcard and password.

The private Member State keys are activated for a key usage period of two years, as defined by the ERCA (see [1]).

For activation of DocSigner keys see associated documentation [5].

The aspect of private key activation is not applicable to the private keys of the Card_MA and Card_Sign key pairs.

6.2.9. Method of Deactivating Private Key

Activating a new private Member State key deactivates the former private key. The CA Console supports the use of only one single active private Member State key at any time. FL-MSCA no longer has access to deactivated keys.

For role representatives required for private key activation see section 6.2.8.

6.2.10. Method of Destroying Private Key

As soon as private Member State keys are deactivated, they are to be destroyed on the HSM. Similarly, at the end of their life cycle, symmetric master keys are to be destroyed.

Destruction of the private keys means all copies of the key and information required to regenerate or reconstruct the key have to be deleted from all locations where they ever existed.

6.2.11. Cryptographic Module Rating

For ratings and capabilities, refer to section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The validity periods of all ERCA root certificates, ERCA link certificates and MSCA certificates shall comply with Annex IC Appendix 11 [1]. In Particular, the following validity and usage periods are defined:

Key / Certificate	Additional Information	Validity / Usage period
EUR (root key pair)		17 years
EUR (root certificate)		34 years + 3 months
LinkEUR (link certificate)		17 years
MSCA_Card (private key)		2 years
MSCA_Card (certificate)		7 years + 1 month
Card_MA (certificate)	driver card	5 years
Card_MA (certificate)	company card	5 years
Card_MA (certificate)	control card	2 years
Card_MA (certificate)	workshop card	1 year
Card_Sign (certificate)	driver card	5 years + 1 month
Card_Sign (certificate)	workshop card	1 year + 1 month
$K_{M\text{-}WC}$		17 years*
KM_{DSRC}		17 years**

DocSigner (private key)		2 years
DocSigner (certificate)		3 years

**: Validity starts one year before EUR root key pair validity*

***: Validity starts two years before EUR root key pair validity*

Table 7: Validity and usage periods of certificates and keys

Private keys shall not be used after the private key usage period is over.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Supervised by the FL-MSCA PKI Security Officer, activation data for the HSMs storing the FL-MSCA keys is generated individually by the different authorized FL-MSCA PKI Operating role owner (PKI operational staff members).

Activation data for the HSMs storing the FL-CP keys is as well generated individually by the different authorized FL-CP staff members and in compliance with the four eyes principle.

The passphrases and parameters are then (for FL-MSCA and FL-CP keys) entered as advised by the HSM's provider.

6.4.2. Activation Data Protection

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

6.4.3. Other Aspects of Activation Data

The login to the FL-MSCA Console application is based on the private Swiss Government Root CA II key stored on the personal smart card. The access the FL-MSCA Console application underlies additional password protection.

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

The duration of an authentication session shall not be unlimited.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

FL-MSCA and FL-CP are using mandatory access control with all applications used to operate Liechtenstein Tachograph PKI services.

For all critical processes, segregation of duties is enforced.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

For application development and implementation, the FL-MSCA as well as the FL-CP are following their respective valid processes and standards for systems development and change management.

In addition, FL-MSCA as well as the FL-CP operate a configuration management tool ensuring only approved and tested hardware and software is deployed. In general, all changes are simulated on an acceptance environment before going into production.

6.6.2. Security Management Controls

The Security Officers (FL-MSCA PKI Security Officer / FL-CP Information Systems Security Officer) regularly verify the integrity of the certification service's components.

Appropriate malware countermeasures are established and monitored.

The verification and monitoring results are documented and retained.

6.6.3. Life Cycle Security Controls

The Engineers and Security Officers of the FL-MSCA and the FL-CP shall monitor development, operation, and maintenance of the PKI systems and regularly evaluate the effectiveness through audit.

6.7. Network Security Controls

The FL-MSCA PKI certification infrastructure is operated in a specific network-segment separated from the federal administration's network by a gateway acting as a firewall. Within the network of the FL-CP, the certification system is protected by a firewall. Network connection between FL-MSCA and FL-CP is as well firewall protected. In addition, all PKI communications are protected through integrity checks and encryption mechanisms.

Safety guidelines are set up for all network security components. The security officers (FL-MSCA PKI Security Officer / FL-CP Information Systems Security Officer) are informed before any change in the security configuration.

6.8. Time-Stamping

FL-MSCA and FL-CP are using qualified time-stamping services acting as a Time Stamping Authority (TSA) and supporting electronic signing. The timestamps are used to prove certain data at a certain point in time without the possibility to alter or backdate the timestamps.

All FL-MSCA and FL-CP PKI systems are time synchronized by using Network Time Protocol (NTP), referring the time source provided.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

All FL-MSCA certificates created are based on the profiles defined and provided by the ERCA, as described in [1] Appendix 11 section 9.3.2 and [3] section 7.1.

7.1.1. Version Number(s)

For specification provisions see [1] Appendix 11 section 9.3.2 and [3] section 7.1.

7.1.2. Certificate Extensions

For specification provisions see [1] Appendix 11 section 9.3.2 and [3] section 7.1.

7.1.3. Algorithm Object Identifiers

For specification provisions see [1] Appendix 11 section 9.3.2 and [3] section 7.1.

The algorithm for the DocSigner Certificate is indicated via the Standardised Domain Parameter OID 2.16.756.1.17.3.21.1.

7.1.4. Name Forms

For specification provisions see [1] Appendix 11 section 9.3.2 and [3] section 7.1.

7.1.5. Name Constraints

Not implemented.

7.1.6. Certificate Policy Object Identifier

OID of the document on hand is 2.16.756.1.17.3.82.2

7.1.7. Usage of Policy Constraints Extension

Not implemented.

7.1.8. Policy Qualifiers Syntax and Semantics

Not implemented.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

The FL-MSCA tachograph card certificates described in the document on hand are never revoked or suspended (see section 4.9 for details on certificate revocation). Therefore, no CRL will be kept, and no CRL is to be published.

For the ERCA, the status of all certificates issued can be found on the website https://dtc.jrc.ec.europa.eu/.

7.2.1. Version Number(s)

Not applicable.

7.2.2. CRL and CRL Entry Extensions

Not applicable.

7.3. OCSP Profile

No Online Certificate Status Protocol (OCSP) shall be used.

7.3.1. Version Number(s)

Not applicable.

7.3.2. OCSP Extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstances of Assessment

FL-MSCA and FL-CP are subject to the Liechtenstein national audit.

The national audit shall establish whether the requirements of this Certification Policy and Certification Practice Statement on hand are being maintained. The FL-MSA shall perform the first audit within 12 months of the start of the operations covered by the Certification Policy and Certification Practice Statement on hand.

If an audit finds no evidence of non-conformity, the next audit shall be performed within 24 months. If an audit finds evidence of non-conformity, a follow-up audit shall be performed within 12 months to verify that the non-conformities have been solved.

Before the start of the operations covered by this Certification Policy and Certification Practice Statement on hand, the FL-MSA shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in the Certification Policy and Certification Practice Statement on hand.

8.2. Identity/Qualifications of Assessor

The auditor assigned has to be an independent company carrying out audits in accordance with the statutory and regulatory provisions.

The auditor has to be accredited by the Swiss Accreditation Service to perform the specific audits. In particular, the auditor shall possess significant knowledge of, and preferably be accredited for:

- performance of information system security audits
- PKI and cryptographic technologies
- the operation of PKI software
- the relevant European Commission policies and regulations.

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

8.3. Assessor's Relationship to Assessed Entity

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

In addition to the foregoing prohibition on conflicts of interest, the assessor has a contractual relationship with the FL-MSA or the FL-MSCA for the performance of the audit, but otherwise, the auditor shall be independent. The auditor shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4. Topics Covered by Assessment

The audit shall cover compliance to the Certification Policy and Certification Practice Statement on hand and the associated procedures and techniques documented by the organisation to be audited. The scope of the compliance audit shall be the implementation of the technical, procedural and personnel practices described in these documents.

Some areas of focus for the audits shall be:

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

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

8.5. Actions Taken as a Result of Deficiency

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

In particular, the FL-MSA and FL-MSCA agree with the auditor on the necessary actions and time schedules to correct/eliminate the deficiencies identified. They will jointly see to the initiation and successful completion of the resulting tasks. The Security Officers (FL-MSCA PKI Security Officer / FL-CP Information Systems Security Officer) are responsible to track the necessary actions and report to the FL-MSA the current status of completion.

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

8.6. Communication of Results

The independent auditor shall report the full results of the compliance audit to the organisation that was audited as well as to the FL-MSA. The FL-MSA shall send an audit report covering the relevant results of the audit to the ERCA. This report shall include at least the number of deviations found and the nature of each deviation. If requested by the ERCA, the FL-MSA shall send the full results of the compliance audit to the ERCA.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

The only applicable provision regarding fees charged for certification services are part of the ASTRA fee ordinance (GeBV ASTRA [8]), as card holder resp. card requester have to pay a tachograph card-issuing fee.

Costs for running the certification services are covered by contacts and SLAs agreed among the participants. There are no other fees charged by FL-MSCA or FL-CP.

9.1.1. Certificate Issuance or Renewal Fees

Not implemented.

9.1.2. Certificate Access Fees

Not implemented.

9.1.3. Revocation or Status Information Access Fees

Revocation fees not applicable. Status Information Access fees not implemented.

9.1.4. Fees for Other Services

Not implemented.

9.1.5. Refund Policy

Not implemented.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

FL-CP has to obey the swiss federal law on the electronic signature (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03, [9]) whereafter certification service provider have to be insured to cover liability and the costs that may arise from the measures provided for.

In case of FL-MSCA, the swiss Federal Department of Finance (FDF) has confirmed it is liable for SG PKI's certification services, thereby restricting the need for insurance.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

Not implemented.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following data is considered confidential and treated accordingly:

- any personal or corporate information held by the FL-MSA, FL-MSCA or FL-CP which is not appearing on issued certificates
- all private keys used and handled within the FL-MSCA and FL-CP operation subject to the Certification Policy and Certification Practice Statement on hand
- all master keys used and handled within the CH-MSCA and CH-CP operation subject to the Certification Policy and Certification Practice Statement on hand
- all audit logs generated with the FL-MSCA and FL-CP operation subject to the Certification Policy and Certification Practice Statement on hand, audit reports and any other assessment results as well as all data archived
- all detailed documentation of the FL-MSCA and FL-CP PKI management beyond this Certification Policy and Certification Practice Statement on hand

Dissemination of any information, including audit logs and records, by the FL-MSCA to any party, other than the MSA, shall require written approval by the MSA.

9.3.2. Information Not Within the Scope of Confidential Information

The following data is not considered confidential:

- Identification number of tachograph cards
- Certificates
- Identification information or other personal or corporate information appearing on certificates
- Certificate status information

- FL-MSCA and FL-CP documents intended for subscribers, relying parties and third parties, e.g. this Certification Policy and Certification Practice Statement on hand

9.3.3. Responsibility to Protect Confidential Information

All FL-MSCA and FL-CP staff are responsible for protecting confidential information.

The security officers (FL-MSCA PKI Security Officer / FL-CP Information Systems Security Officer) specify the respective requirements and measures and enforces these in the daily operation.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

All private data shall be treated according to the Swiss laws in particular according to the Federal Act on Data Protection (FADP) (Bundesgesetz über den Datenschutz (DSG), SR 235.1) [10] and related regulations and secondary legal bases.

9.4.2. Information Treated as Private

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

9.4.3. Information not Deemed Private

The provisions defined in point 9.3.2 apply.

9.4.4. Responsibility to Protect Private Information

All FL-MSCA and FL-CP staff must observe the requirements stipulated in the Swiss laws on data protection where applicable.

All FL-MSCA and FL-CP staff shall collect only data necessary for registration and certification and use it for these purposes exclusively. In particular, they must not use private data for any commercial purposes.

9.4.5. Notice and Consent to use Private Information

The relying parties give the FL-MSCA and FL-CP consent to use private information as far as this is required for them to render their services.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The FL-MSCA and FL-CP stores and processes private information as stipulated in swiss legal data protection provisions [10]. Such information is disclosed to government entities only if corresponding decisions are presented that are in line with legal provisions.

9.4.7. Other Information Disclosure Circumstances

No other information disclosure circumstances are envisaged.

9.5. Intellectual Property Rights

FL-MSCA is owner of the intellectual property rights of the following documents:

- Certificates issued by FL-MSCA

Subscribers and relying parties do not acquire ownership of the certificates issued by FL-MSCA; they just obtain the right to use these.

FL-MSA is owner of the intellectual property rights of the following documents:

- Contracts and other agreements concluded between FL-MSA and its clients and partners

The reproduction, presentation (inclusive of publication and distribution) as a whole or in part, by any means, without explicit authorization in writing obtained in advance, is strictly forbidden.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

The FL-MSCA undertakes to follow the provisions of the ERCA Policy [3] as well as of this Certification Policy and Certification Practice Statement on hand.

9.6.2. RA Representations and Warranties

Within the Smart Tachograph PKI, registration authorities are part of the certification authorities (see section 1.3). This document therefore does not contain any specific requirements for registration authorities.

9.6.3. Subscriber Representations and Warranties

The FL-CP undertakes to follow the provisions of the ERCA Policy [3] as well as of this Certification Policy and Certification Practice Statement on hand.

9.6.4. Relying Party Representations and Warranties

The card holder undertake to follow the provisions of the Liechtenstein laws in particular according to the specifications for tachograph card usage.

9.6.5. Representations and Warranties of other Participants

Any service providers, appointed by the FL-MSA, the FL-MSCA or the FL-CP must undertake to comply with the ERCA Policy [3] as well as of this Certification Policy and Certification Practice Statement on hand.

9.7. Disclaimers of Warranties

The FL-MSA disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaim any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

Warranties and obligations of the FL-MSCA and the FL-CP to the FL-MSA are subject to the underlying contracts and agreements. All other warranties by any of these parties identified are excluded.

9.8. Limitations of Liability

The liability of the FL-MSA, the FL-MSCA and the FL-CP is limited to the extent permitted by applicable law.

In particular, the FL-MSA, the FL-MSCA and the FL-CP are not liable for:

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

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

9.9. Indemnities

This document does not provide any additional explicit information on indemnities in addition to the statements in sections 9.6 to 9.8.

9.10. Term and Termination

9.10.1. Term

This Certification Policy and Certification Practice Statement becomes valid the day it is published (see section 2.2).

9.10.2. Termination

This Certification Policy and Certification Practice Statement is valid until:

- the FL-MSA announces it to be no longer valid
- it is replaced by a newer version, or
- FL-MSA stops operating

Note: The case FL-MSA stops operating implies that the Liechtenstein Smart Tachograph system as a whole stops operating. Section 5.8.1 covers the final termination of the FL-MSA responsibility.

9.10.3. Effect of Termination and Survival

Even once the Certification Policy and Certification Practice Statement on hand may no longer be valid, the regulations pertaining to the laws on data protection and on archival of information are still observed.

9.11. Individual Notices and Communications with Participants

Communication between FL-MSA, CHMSCA and FL-CP takes place via signed mails or by letter. General information or announcements are published on the FEDRO tachograph website (http://www.dfs.astra.admin.ch).

Notice of severance or merger may result in changes to the scope, management and/or operation of the FL-MSA. In such an event, this Certification Policy and Certification Practice Statement on hand may require modification as well. Changes to these documents shall be made in a manner consistent with the administrative requirements stipulated in the following section (section 9.12) of the document on hand.

9.12. Amendments

This Certification Policy and Certification Practice Statement is issued under responsibility of the Liechtenstein Member State Authority. The FL-MSA, in cooperation with the FL-MSCA, may revise this Certification Policy and Certification Practice Statement if it deems necessary. The FL-MSA will in all cases consult the ERCA with respect to the necessity of renewal of the approval as result of the changes in the FL-MSA Certification Policy and Certification Practice Statement.

9.12.1. Procedures for Amendment

9.12.1.1. Items that may change without notification

The only changes that may be made to this policy and practice statement without notification are:

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

9.12.1.2. Changes with notification

Changes to any item in this policy and practice statement shall be advertised 90 days in advance.

Changes to items that, by the judgment of the MSA, will not materially affect a substantial majority of the users using this policy and practice statement may be advertised only 30 days in advance.

9.12.1.3. Comment period

Impacted users may place comments concerning a proposed MSA policy and practice statement change to the FL-MSA within 15 days of original notice.

9.12.1.4. Whom to inform

Information about changes to this policy and practice statement shall be sent to:

- ERCA,
- FL-MSCA (=Liechtenstein MSCA)
- FL-CP (=Liechtenstein Card Personalisers of the tachograph cards)
- FL-CIA (=Liechtenstein Card Issuing Authority)

9.12.1.5. Period for final change notice

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

9.12.1.6. Changes requiring a new ERCA approval

If a Certification Policy and Certification Practice Statement change is determined by the FL-MSA to have a material impact on a significant number of users of the Policy, the FL-MSA shall submit the revised policy to the ERCA for approval.

9.12.2. Notification Mechanism and Period

Notification mechanisms are part of the amendment procedures described in 9.12.1.

9.12.3. Circumstances under which OID must be changed

The only changes that may be made to this policy and practice statement without change to the document version number are:

- Editorial or typographical corrections.

Any other type of document change (see amendment procedures described in 9.12.1) leads to document version number change.

9.13. Dispute Resolution Provisions

Any dispute related to key and certificate management between the FL-MSA resp. the FL-MSCA and an organisation or individual outside shall be resolved using an appropriate dispute settlement mechanism. The dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the Liechtenstein Authority.

It is up to the FL-MSA resp. the FL-MSCA to decide whether a matter is subject to arbitration.

9.14. Governing Law

This Certification Policy and Certification Practice Statement on hand is subject to the applicable Liechtenstein federal laws. In addition, it is subject to the Swiss Federal Act on Data Protection (FADP) [10]. The place of jurisdiction depends on the concerned law: Bern (for Swiss law) and Vaduz (for Liechtenstein law).

9.15. Compliance with Applicable Law

The introduction and operation of the smart tachograph system in Liechtenstein is based on the associated European and national laws and regulations. Compliance with these regulations is monitored by the FL-MSA. In case of discrepancies between all the related regulations, the EU 165/2014 and the EU 799/2016 amended by the EU 502/2018 shall prevails.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

All regulations in this Certification Policy and Certification Practice Statement on hand apply to all participants and subscribers. Every new published version of this Certification Policy and Certification Practice Statement on hand replaces all previous versions. There are no additional verbal or subsidiary agreements in place.

9.16.2. Assignment

The assignment of rights, contrary to the underlying laws, regulations and the Certification Policy and Certification Practice Statement on hand, is prohibited.

9.16.3. Severability

If individual provisions of this Certification Policy and Certification Practice Statement on hand are or become invalid, this shall not affect the remaining provisions of this Certification Policy and Certification Practice Statement. Likewise, if a provision is missing, this shall not affect the validity of the Certification Policy and Certification Practice Statement on hand. In place of the ineffective provision, an effective provision shall be deemed to be agreed that comes closest to the original intention or that would have been determined in line with the meaning and purpose of the Certification Policy and Certification Practice Statement had this point been covered therein.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

Any legal disputes arising from the FL-MSA operations are subject to the laws of the Liechtenstein Authority. The place of enforcement and jurisdiction is Vaduz.

Any legal disputes arising from the FL-MSCA and FL-CP operations are subject to the laws of the Swiss Authority. The place of enforcement and jurisdiction is Bern.

9.16.5. Force Majeure

The FL-MSA accepts no liability for the violation of an obligation, for default or for non-fulfilment under this Certification Policy and Certification Practice Statement if this results from an underlying event that is beyond its control (e.g. force majeure, war, network outage, fire, earthquake or other catastrophes).

9.17. Other Provisions

No stipulation.

REFERENCES

[1] Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.139.01.0001.01.ENG

[2] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997

[3] Smart Tachograph, European Root Certificate Policy and Symmetric Key Infrastructure Policy, Version 1.0, June 2018: https://dtc.jrc.ec.europa.eu/iot_doc/Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy v1.0.pdf

[4] Swiss Government Root CA II - Certificate: https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki/rootzertifikate/swiss-government-root-ca-ii.html

[5] Swiss Government Root CA II - Certification Policy and Certification Practice Statement: https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki/cp-und-cps/cp-cps-root-ca-ii.html

[6] Ordinance on security checks for persons - "Verordnung über die Personensicherheitsprüfungen (PSPV)", only available in German: https://www.admin.ch/opc/de/classified-compilation/20092321/index.html

[7] Federal Act on the Responsibility of the Swiss Confederation, the Members of its Official Bodies and their Officers - "Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördenmitglieder und Beamten (Verantwortlichkeitsgesetz, VG)", only available in German: https://www.admin.ch/opc/de/classified-compilation/19580024/index.html

[8] GebV ASTRA, Gebührenverordnung-ASTRA (SR 172.047.40): https://www.admin.ch/opc/de/classified-compilation/20071953/index.html

[9] Federal law on the electronic signature (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03): https://www.admin.ch/opc/de/classified-compilation/20131913/index.html

[10] Federal Act on Data Protection (FADP) (Bundesgesetz über den Datenschutz (DSG), SR 235.1): https://www.admin.ch/opc/de/classified-compilation/19920153/index.html

[11] Regulation (EU) No 165/2014: https://publications.europa.eu/en/publication-detail/-/publication/fe086399-a04f-11e3-8b87-01aa75ed71a1

[12] Commission Implementing Regulation (EU) 2018/502 amending Implementing Regulation (EU) 2016/799: https://dtc.jrc.ec.europa.eu/iot_doc/EU%202018-502.pdf

[13] The Liechtenstein MSA-Policy for the Digital Tachograph according EU Council Regulation 2135/98: https://www.astra.admin.ch/dam/astra/de/dokumente/digitaler_fahrtschreiber/liechtensteinischezertifizierungspolitikfuerdassystemdesdigitale.pdf.download.pdf/liechtensteinischezertifizierungspolitikfuerdassystemdesdigitale.pdf

[14] Agreement on the European Economic Area (EEA Agreement): http://www.efta.int/Legal-Text/EEA-Agreement-1327

LIST OF FIGURES

Figure 1: Legal Hierarchy and PKI roles for Liechtenstein 10
Figure 2: Liechtenstein specific certificates of the Tachograph PKI 11
Figure 3: Liechtenstein specific key generation responsibilities of the Tachograph PKI 11
Figure 4: Liechtenstein specific requests and responses of the Tachograph PKI 12

LIST OF TABLES

Table 1: Necessary keys on the respective card type 17
Table 2: Acronyms and meanings 20
Table 3: Identifiers for certificate issuers and subjects 22
Table 4: Identifiers of the DocSigner certificate 22
Table 5: Identifier of the Card Personalisation Request 23
Table 6: Identifier of the Card Certification Request 23
Table 7: Validity and usage periods of certificates and keys 43