Second Generation Digital Tachograph

(Smart Tachograph)

Kingdom of Belgium

Member State Authority (MSA)

Certificate Policy and

Symmetric Key Infrastructure Policy

Version 1.2

Version Control

Version	Date	Comment
Official Version 1.0	01/02/2019	Approved by the European Authority
Official Version 1.1	01/04/2022	Updates requested by external 2021 audit.
Official Version 1.2	15/03/2023	Updated section “1.8.4. Component Personalizer (CP)” to include new organization names and contact details information.

Contents

1. INTRODUCTION

1.1. OVERVIEW

The Smart Tachograph is the second generation of the Digital Tachograph, a control device for recording drivers' activities, such as driving and rest periods in commercial vehicles. The use of the digital tachograph is required by law in the European Union. The Smart Tachograph has been introduced by Regulation (EU) No 165/2014 [2] of the European Parliament and of the Council.

Similar to the Digital Tachograph system (Gen-1), the Smart Tachograph system (Gen-2) is a three-layered hierarchic Public Key Infrastructure (PKI) system. A Root Certification Authority is established at the European level (European Root Certification Authority or ERCA) and is connected to the different Member State Certification Authorities (MSCAs) to create a consistent and secure system. The role of ERCA is to securely certify the public keys of the MSCAs to establish a trusted certification chain. Moreover, the ERCA also distributes a number of symmetric master keys to the MSCAs.

At the national level, the role of the MSCAs is to securely certify the public keys of Smart Tachograph equipment issued under their accountability: Vehicle Units (VU), Tachograph Cards (TC), Motion Sensors (MS) and/or External GNSS Facilities (EGF). Moreover, MSCAs are responsible for distributing master keys and/or cryptographic data derived from master keys to the component personalizers (CP) that are responsible for issuing this equipment.

At the equipment level, equipment personalizers are responsible for creating equipment key pairs and inserting equipment keys and certificates securely into their equipment. For some types of equipment, personalizers also insert symmetric keys into the equipment. Personalizers obtain these keys from the ERCA or from the MSCA.

To ensure compatibility with existing first-generation equipment, second-generation equipment shall be equipped both with first generation (TDES and RSA) keys and certificates as well as second-generation (AES and ECC) keys and certificates. This means that for the foreseeable future, tachograph cards will contain two applications, as specified in Appendix 2 to Annex 1C of EU 799/2016 [3].

For more details, the reader is referred to the Implementing Regulation (EU) 799/2016 [3], and especially to Appendix 11 of Annex 1C thereof. Note that this Regulation has been amended by Commission Implementing Regulation (EU) 502/2018. Every reference to EU 799/2016 [3] in this MSA certificate policy is supposed to include these amendments.

Part A of Appendix 11 defines the security mechanisms for the first-generation tachograph system (digital tachograph) based on RSA public-key cryptographic systems and Triple-DES based symmetric cryptographic systems.

Part B of Appendix 11 describes how elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems are used to realize this for the second-generation tachograph system.

A Public Key Infrastructure (PKI) has been designed to support the public-key cryptographic systems, while the symmetric cryptographic systems rely on master keys that have to be delivered to the relevant actors. An infrastructure consisting of three layers has been set up. At the European level, the European Root Certification Authority (ERCA) is responsible for the generation and management of root public-private key pairs, with the respective certificates, and symmetric master keys. ERCA issues certificates to Member State Certification Authorities (MSCAs) and distributes symmetric master keys to the MSCAs. The MSCAs are responsible for the issuance of Smart Tachograph equipment certificates, as well as for the distribution of symmetric master keys and other data derived from the master keys to be installed in Smart Tachograph equipment.

This document follows the framework for Certificate Policies described in RFC 3647 [4]. The Symmetric Key Infrastructure policy has been added to this document, preserving the lay-out of RFC 3647 [4]. How MSCA itself complies with this Certificate and Symmetric Key Infrastructure Policy is described in the MSCA Certification Practice Statement (CPS).

The key words “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC 2119 [5].

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is named “Second Generation Digital Tachograph (Smart Tachograph) Kingdom of Belgium Member State Authority (MSA) Certificate Policy and Symmetric Key Infrastructure Policy”. This Certificate Policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the certificates used in the Smart Tachograph system do not contain a reference to this policy.

The current version is 1.2.

1.3. APPROVAL

This policy was endorsed by the European Root Certification Authority – ERCA

Digital Tachograph Root Certification Authority
Digital Citizen Security Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)
in
April 2023.

1.4. SCOPE AND APPLICABILITY

This certificate policy is valid for the Smart Tachograph System only.

The smart cards and digital certificates issued by the MSCA are only for use within the Smart Tachograph system.

1.5. DOCUMENT OBJECTIVE

The Certificate Policy for the MSA at the national level for the first generation of Digital Tachograph is "Belgian MSA Policy for the Tachograph System (B-MSA)" version 1.17 approved by ERCA. It lays down the policy at national level for key generation, key management and certificate signing for the Digital Tachograph system (first-generation tachograph system).

The objective of this document is to form the Certificate Policy for the MSA at the Kingdom of Belgium level for elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems: "Second Generation Digital Tachograph (Smart Tachograph) Kingdom of Belgium Member State Authority (MSA) Certificate Policy and Symmetric Key Infrastructure Policy" version 1.2. It lays down the policy at Kingdom of Belgium level for key generation, key management and certificate signing for elliptic curve-based public-key cryptographic systems and AES-based symmetric cryptographic systems for the Smart Tachograph system.

1.6. TACHOGRAPH SYSTEM ORGANIZATION

An illustration of the Tachograph system organization is shown in the figure below:

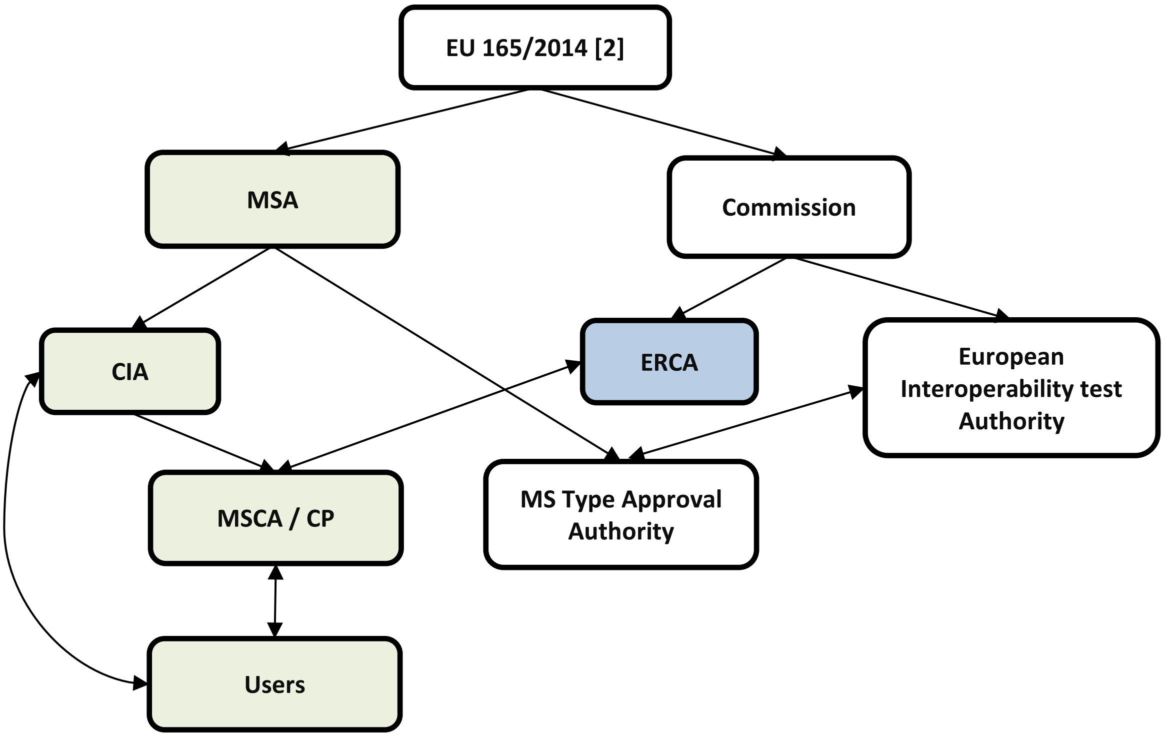
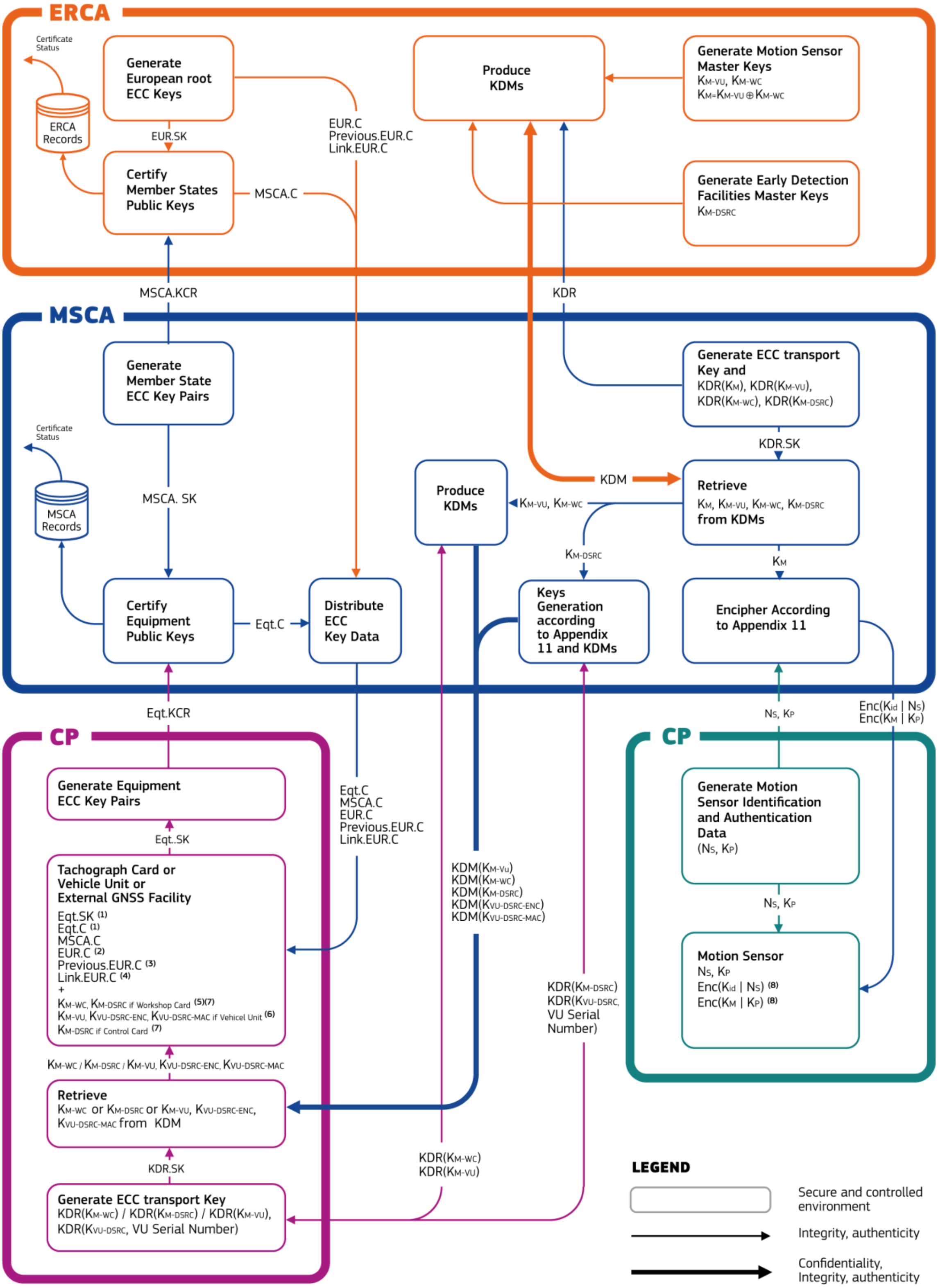

EU 165/2014 [2]
MSA
Commission
CIA
ERCA
European Interoperability test Authority
MSCA / CP
MS Type Approval Authority
Users

Figure 1 **Tachograph system organization (colored boxes are covered in this document)**

1.7. PARTICIPANTS

The participants in the Smart Tachograph PKI and in the Symmetric Key Infrastructure are described here and represented in ***Figure 1*** **Tachograph system organization (colored boxes are covered in this document)**.

Figure 1 **Tachograph system organization (colored boxes are covered in this document)** (Participants in the Smart Tachograph PKI and symmetric key infrastructure) also represents the exchanges between the participants, namely ERCA, MSCAs and component personalizers (CPs).


ERCA
Certificate Status
ERCA Records
Generate European root ECC Keys
EUR.SK
Certify Member States Public Keys
MSCA.C
EUR.C
Previous.EUR.C
Link.EUR.C
Produce KDMs
Generate Motion Sensor Master Keys
$K_{M\text{-}VU}$, $K_{M\text{-}WC}$
$K_M = K_{M\text{-}VU} \oplus K_{M\text{-}WC}$
Generate Early Detection Facilities Master Keys
$K_{M\text{-}DSRC}$
MSCA.KCR
KDR
MSCA
Generate Member State ECC Key Pairs
Certificate Status
MSCA Records
MSCA. SK
Certify Equipment Public Keys
Eqt.C
Distribute ECC Key Data
Produce KDMs
$K_{M\text{-}VU}$, $K_{M\text{-}WC}$
Generate ECC transport Key and
$KDR(K_M)$, $KDR(K_{M\text{-}VU})$,
$KDR(K_{M\text{-}WC})$, $KDR(K_{M\text{-}DSRC})$
KDR.SK
KDM
Retrieve
K_M, $K_{M\text{-}VU}$, $K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$
from KDMs
$K_{M\text{-}DSRC}$
K_M
Keys Generation according to Appendix 11 and KDMs
Encipher According to Appendix 11
Eqt.KCR
N_S, K_P
$Enc(K_{id} | N_S)$
$Enc(K_M | K_P)$
CP
Generate Equipment ECC Key Pairs
Eqt..SK
Tachograph Card or Vehicle Unit or External GNSS Facility
Eqt.SK (1)
Eqt.C (1)
MSCA.C
EUR.C (2)
Previous.EUR.C (3)
Link.EUR.C (4)
+
$K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$ if Workshop Card (5)(7)
$K_{M\text{-}VU}$, $K_{VU\text{-}DSRC\text{-}ENC}$, $K_{VU\text{-}DSRC\text{-}MAC}$ if Vehicel Unit (6)
$K_{M\text{-}DSRC}$ if Control Card (7)
Eqt.C
MSCA.C
EUR.C
Previous.EUR.C
Link.EUR.C
$K_{M\text{-}WC}$ / $K_{M\text{-}DSRC}$ / $K_{M\text{-}VU}$, $K_{VU\text{-}DSRC\text{-}ENC}$, $K_{VU\text{-}DSRC\text{-}MAC}$
Retrieve
$K_{M\text{-}WC}$ or $K_{M\text{-}DSRC}$ or $K_{M\text{-}VU}$, $K_{VU\text{-}DSRC\text{-}ENC}$, $K_{VU\text{-}DSRC\text{-}MAC}$ from KDM
KDR.SK
Generate ECC transport Key
$KDR(K_{M\text{-}WC})$ / $KDR(K_{M\text{-}DSRC})$ / $KDR(K_{M\text{-}VU})$,
$KDR(K_{VU\text{-}DSRC}$, VU Serial Number)
$KDM(K_{M\text{-}VU})$
$KDM(K_{M\text{-}WC})$
$KDM(K_{M\text{-}DSRC})$
$KDM(K_{VU\text{-}DSRC\text{-}ENC})$
$KDM(K_{VU\text{-}DSRC\text{-}MAC})$
$KDR(K_{M\text{-}DSRC})$
$KDR(K_{VU\text{-}DSRC}$,
VU Serial Number)
$KDR(K_{M\text{-}WC})$
$KDR(K_{M\text{-}VU})$
CP
Generate Motion Sensor Identification and Authentication Data
(N_S, K_P)
N_S, K_P
Motion Sensor
N_S, K_P
$Enc(K_{id} | N_S)$ (8)
$Enc(K_M | K_P)$ (8)
LEGEND
Secure and controlled environment
Integrity, authenticity
Confidentiality, Integrity, authenticity

NOTES

1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Figure 2 Participants in the Smart Tachograph PKI and symmetric key infrastructure

1.7.1. National Authority

Responsible for the National policy is the Member State Authority (MSA).

MSA certificate policy, this document, shall comply with all applicable requirements in the ERCA certificate policy [1].

The Kingdom of Belgium Member State Authority (MSA), referred to hereinafter as B-MSA appoints the organization which implements this policy at the national level.

1.7.2. Certification Authorities

1.7.2.1. European Root Certification Authority (ERCA)

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

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 Smart Tachograph European Root Certificate Policy and Symmetric Key [1] is available on the JRC website at:

https://dtc.jrc.ec.europa.eu/iot_doc/Smart%20Tachograph%20-%20European%20Root%20Certificate%20Policy%20and%20Symmetric%20Key%20Infrastructure%20Policy%20v1.0.pdf

1.7.2.2. Foreign MSCAs

Foreign MSCAs (non B-MSCA) are out of scope of this policy, as there will be no direct interaction between the B-MSCA and any other MSCAs.

1.7.2.3. B-MSCA

The Kingdom of Belgium Member State Certification Authority (MSCA), referred to hereinafter as B-MSCA is appointed by the B-MSA.

The B-MSCA shall operate in conformance with all applicable requirements in

- this B-MSA certificate policy,
- the ERCA certificate policy for the Digital Tachograph;
- the ERCA certificate policy for the Smart Tachograph;
- the EU Regulation 799/2016 [3] in particular Annex 1C.

In particular, the responsibilities of the B-MSCA are:

- to have available an B-MSCA system for Production as well as an B-MSCA system for Interoperability Testing purposes, according to the (EU) Regulation 799/2016 [3];

- to securely generate, store and manage Generation-1 (RSA) Member State key pairs, in accordance with the requirements in section 3 of Appendix 11 to Annex 1C, and in “Chapter 6 Technical Security Controls” of this policy.
- to create Key Certification Requests for these RSA keys conform the Digital Tachograph ERCA certificate policy, and send those to the ERCA to obtain the corresponding Member State certificates;
- to securely generate, store and manage Generation-2 (ECC) MSCA_Card key pairs, in accordance with the requirements in section 9.1.3 of Appendix 11 to Annex 1C, and in “Chapter 6 Technical Security Controls” of this policy.
- to create Certificate Signing Requests for these ECC keys conform the Smart Tachograph ERCA certificate policy, and send those to the ERCA to obtain the corresponding MSCA_Card certificates;
- to issue certificates for first-generation tachograph card public keys and second-generation tachograph card public keys upon request of the B-CP;
- to send the Gen-1 and Gen-2 B-MSCA certificates to the B-CP;
- to keep traceable records of all of issued card certificates;
- to receive a Key Distribution Request conform the ERCA certificate policy from the B-CP and forward that request to the ERCA to obtain a Key Distribution Message containing a master key;
- to securely manage the Key Distribution Message and send it to the B-CP.

Moreover, the MSCA shall:

- explain how the MSCA complies with all applicable requirements in this MSA certificate policy;
- review its CPS to make sure it still accurately describes the actual systems and processes of the B-MSCA, and notify the B-MSA about any necessary changes;
- establish an information security management system (ISMS), based on a risk assessment for all the operations involved. The ISMS shall cover all processes related to the issuing of tachograph cards and the management of personal data on these cards. The implementation of the ISMS shall be certified according to ISO 27001 [19];
- maintain adequate organizational and financial resources to operate in conformity with the requirements laid down in this B-MSA certificate policy.

1.7.3. Registration Authorities

The B-MSCA comprises only a certification authority. Functionality associated with a registration authority (RA) is performed by the Card Issuing Authority (CIA). The Kingdom of Belgium Card Issuing Authority (CIA), referred to hereinafter as B-CIA is appointed by the B-MSA.

The B-CIA shall operate in conformance with all applicable requirements in:

- this B-MSA certificate policy;
- the ERCA certificate policy for the Digital Tachograph;
- the ERCA certificate policy for the Smart Tachograph;
- the EU Regulation 799/2016 [3] in particular Annex 1C.

The B-CIA is responsible for

- verifying whether a tachograph card was already issued to the applicant in another EU-member state;
- informing all users about the requirements of this policy in an appropriate manner;
- issuing a (Production) tachograph card on request of a Card Holder;
- providing correct and complete personalization data (including card certificate(s) data) to the B-CP for each tachograph card to be issued;
- performing tachograph card (certificate) life cycle management;
- issuing tachograph cards as needed by the European Digital Tachograph Laboratory for Interoperability Testing, as specified in the Smart Tachograph Equipment Interoperability Test Specification;
- immediately informing the B-MSA and the B-MSCA or one of its authorized agencies about all security-relevant incidents.

1.7.4. Component Personalizer

The Kingdom of Belgium Component Personalizer (CP), referred to hereinafter as B-CP is appointed by the B-MSA.

The Card Personalizer shall operate in conformance with all applicable requirements in:

- this B-MSA certificate policy;
- the ERCA certificate policy for the Digital Tachograph;
- the ERCA certificate policy for the Smart Tachograph;
- the Regulation 799/2016 [3], in particular Annex 1C.

In particular, the responsibilities of the B-CP are:

- to have available an B-CP system for Production as well as a CP system for Interoperability Testing purposes, according to the Regulation 799/2016 [3];

- to generate Key Distribution Requests for all each of the currently valid versions of the Motion Sensor Master Key – Workshop Card part (KM-WC) and the DSRC Master Key (KDSRC) conform the ERCA certificate policy, and send these requests to the B-MSCA to be forwarded to the ERCA;
- to receive the resulting Key Distribution Messages from the ERCA via the B-MSCA and decrypt and securely store the KM-WC and the KDSRC;
- to store, use and manage the KM-WC and KDSRC in accordance with the requirements in "Chapter 6 Technical Security Controls" of this policy;
- to handle tachograph card personalization data in accordance with applicable data protection rules and regulations;
- to provision and personalize smart tachograph cards on request of the B-CIA;
- to ensure and verify the consistency of all electronic and visual personalization data on each card;
- to package and label the personalized tachograph cards;
- to keep the B-CIA informed of the personalization status of each tachograph card
- establish an information security management system (ISMS), based on a risk assessment for all the operations involved. The ISMS shall cover all processes related to the issuing of tachograph cards and the management of personal data on these cards. The implementation of the ISMS shall be certified according to ISO 27001 [19];
- maintain adequate organizational and financial resources to operate in conformity with the requirements laid down in this B-MSA certificate policy.

Requirements regarding vehicle unit and motion sensor manufacturers are currently not covered by this policy. This policy must be adapted if the need arises.

1.7.5. Subscribers

The subscribers to the B-MSCA certificate signing service are the Card Holders: drivers, control officers, transporting companies and workshop employees. These parties use the Generation-1 Card certificate or the Generation-2 Card_MA certificate on their cards to interact with a vehicle unit.

Card Holders are responsible for:

- requesting an initial tachograph card at the B-CIA;
- when expiry of their tachograph card is imminent, timely requesting a renewal at the B-CIA;
- providing accurate and complete information to the B-CIA, in particular during registration and when requesting a tachograph card;
- using their tachograph card and the certificate(s) on that card only for the purposes specified in Annex 1C;
- exercising reasonable care to avoid unauthorized use of the card;
- notifying the B-CIA without delay and requesting a replacement card if:

  - the card is lost, stolen, or malfunctioning;
  - the personalization data of the card is, or becomes, inaccurate;
  - the PIN code of a workshop card is compromised (i.e. becomes known to a third party);
  - the Card Holder forgot the PIN code of their workshop card.
- returning cards that are malfunctioning, inaccurately personalized or whose PIN is compromised or forgotten to the B-CIA on request.

Regarding the number of cards that can be requested:

- Card Holders of a driver card or control card may request and possess at most one valid driver card or control card;
- Card Holders of workshop card may request and possess at most one valid workshop card for each accredited workshop on whose behalf the Card Holder performs tachograph-related duties;
- Card Holders of a company card may request and possess multiple valid company cards.

1.7.6. Relying Parties

Parties relying on the public key certification services of the B-MSCA are primarily the national and international authorities (control bodies) tasked with enforcing the rules and regulations regarding driving times and rest periods. These parties use the certified public key in the Gen-1 Card certificate and the Gen-2 Card_Sign certificate on driver and workshop cards to validate the authenticity and integrity of data downloaded from such cards, by verifying the signature over these data.

1.8. Responsible Organizations

1.8.1. Member State Authority (MSA)

In Kingdom of Belgium, the Member State Authority (hereinafter, B-MSA), which is in charge of this certificate policy, is:

Federale Overheidsdienst Mobiliteit en Vervoer
Directoraat-generaal Wegvervoer en Verkeersveiligheid
Dienst Wegvervoer
Vooruitgangstraat 56 B-1210 Brussel
Belgium

Service Public Fédéral Mobilité et Transport
Direction générale Transport routier et sécurité routière
Direction Transport par Route
Rue du Progrès 56 B-1210 Bruxelles
Belgium

The contact address of the B-MSA is:
Rue du Progrès 56
B-1210 Bruxelles, Belgiums
Email:
info@mobilit.fgov.be

1.8.2. Member State Certification Authority (MSCA)

The appointed Member State Certification Authority for Kingdom of Belgium (hereinafter, B-MSCA) is:

S.C. CERTSIGN S.A.

The contact address of the B-MSCA is:

Oltenitei Avenue Nr. 107 A, Building C1, ground floor, CP 041303, Sector 4, Bucharest, Romania

Using the infrastructure at the following branch address:

29A Tudor Vladimirescu Blvd., 2nd floor, District 5, Bucharest, Romania

Email:

cards.helpdesk@certsign.ro

1.8.3. Card Issuing Authority (CIA)

The appointed Card Issuing Authority for Kingdom of Belgium (hereinafter, B-CIA) is:

Instituut Wegtransport en Logistiek België, vzw
Archimedesstraat 5
B-1000 Brussel

Institut Transport Routier et Logistique, asbl
Rue Archimède 5
B-1000 Bruxelles

The contact address of the B-CIA is:

Rue Archimède 5

B-1000 Bruxelles, *Belgium*

Email: digitach@itlb.be

1.8.4. Component Personalizer (CP)

The appointed Component Personalizer for Kingdom of Belgium (hereinafter, B-CP) is:

The contact address of the B-CP:

Thales DIS France S.A.

6, rue de la Verrerie

92190 Meudon, France

Using the infrastructure at the following branch addresses:

Thales DIS Finland

Oy Myllynkivenkuja 4

FI-01620 Vantaa, Finland

1.9. KEY AND CERTIFICATE USAGE

1.9.1. Appropriate Certificate Uses

Certificates issued by the B-MSCA may be used as card certificates in the Smart Tachograph system, as specified in Appendix 11 of Annex 1C of EU Regulation 799/2016 [3].

1.9.2. Prohibited Certificate Uses

All other uses of certificates issued by the B-MSCA are prohibited.

1.10. POLICY ADMINISTRATION

1.10.1. National Authority

Responsible for this National CA policy for Kingdom of Belgium Tachograph System is the B-MSA.

The B-MSA appoints the organization which implements this policy at the national level and provides key certification and key distribution services to the component personalizers (CPs).

1.10.2. Appointed MSCA

B-MSCA is responsible for implementation of this policy at the national level and for the provision of key certification and key distribution services to the component personalizers (CPs) and is referred to hereinafter as the Kingdom of Belgium Member State Certification Authority (B-MSCA).

B-MSA shall ensure that the B-MSCA has the resources required to operate in conformity with this policy.

The B-MSCA shall document its implementation of this policy in a Certification Practice Statement (CPS).

The B-MSCA CPS is the B-MSCA’s procedural document, which details how the B-MSA certificate policy is enforced in day-to-day management. The document is developed by the B-MSCA. The B-MSCA CPS is owned by the B-MSCA. The B-MSCA CPS shall be treated as restricted information. The B-MSCA shall make the contents of its CPS available to Member State Authorities and its auditors on a need-to-know basis.

The B-MSCA CPS shall be managed, reviewed, and modified following document control procedures.

The B-MSA shall be responsible to determine whether the B-MSCA CPS complies with this B-MSA certificate policy. The B-MSA's statement of compliance is based on a security review performed by the B-MSA or an B-MSA’s appointed auditor.

The B-MSCA shall maintain records of its operations as appropriate to demonstrate conformity with this policy, and shall make these records available to the B-MSA on demand.

Complaints from component personalizers (CP) about the services provided by the B-MSCA shall be addressed to the B-MSA to be dealt with.

1.11. DEFINITIONS AND ACRONYMS

1.11.1. Definitions

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

Cardholder: A person or an organization that is a holder and user of a Tachograph card. Included are drivers, company representatives, workshop workers and control body staff.

Certificate: In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.

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

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual certificate policy.

Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.

Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.

Private key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called Secret key.

Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.

Tachograph cards/Cards: Four different type of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.

User: Users are equipment users and are either Card Holders for card or manufacturers for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

1.11.2. Acronyms

AES	Advanced Encryption Standard
CAR	Certification Authority Reference
CHR	Certificate Holder Reference
CIA	Card Issuing Authority
CP	Component Personaliser
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSRC	Dedicated Short Range Communication
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
EC	European Commission
ECC	Elliptic Curve Cryptography
EGF	External GNSS Facility
EA	European Authority
ERCA	European Root Certification Authority
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ISMS	Information Security Management System
JRC	Joint Research Centre
KCR	Key Certificate Request
KDR	Key Distribution Request
KDM	Key Distribution Message
KID	Key Identifier
K_M	Motion Sensor Master Key
K_{M-VU}	VU part of K_M
K_{M-WC}	WC part of K_M
K_{ID}	Motion Sensor Identification Key
K_P	Motion Sensor Pairing Key
K_{DSRC}	DSRC Master Key
MA	Mutual Authentication
MoS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority

NCP	Normalised Certificate Policy
PKI	Public Key Infrastructure
RA	Registration Authorities
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman
TLV	Type-Length-Value
VU	Vehicle Unit
WC	Workshop Card

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

The B-MSA is responsible for the public website www.digitach.be which is repository for B-MSA public documents.

The certificates signed by the B-MSCA are also be maintained in a stand-alone database which does not need to be public.

B-MSCA is responsible for storing all issued equipment certificates in a repository. This repository does not need to be public.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The B-MSA publishes the following information on its website:

- B-MSA Certificate Policy for Digital Tachograph System;
- B-MSA Certificate Policy for Smart Tachograph System, MSA Certificate Policy and Symmetric Key Infrastructure Policy (this document);
- B-MSA Certificate Policy change proposal information;
- A compliance statement by the ERCA for the B-MSA certificate policy;
- A compliance statements by the B-MSA for B-CIA, B-MSA and B-CP Certification Practice Statements.

The B-CIA Certification Practices Statement is not public, but shall be communicated on request and on a need to know basis to the relevant parties.

The B-MSCA Certification Practices Statement is not public, but shall be communicated on request and on a need to know basis to the relevant parties.

The B-CP Certification Practices Statement is not public, but shall be communicated on request and on a need to know basis to the relevant parties.

The B-MSA certificate policy compliance statements shall be issued by ERCA on completion of the B-MSA certificate policy review process defined in ERCA policy.

By publishing the B-MSCA certificate information in B-MSA repository, B-MSA certifies that:

- ERCA has issued the B-MSCA;
- the information stated in the certificate was verified in accordance with this policy and the CPS;
- The B-MSCA has accepted the certificate.

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 9.13 of this policy.

Similarly, information relating to the changes in the B-MSA certificate policies and the B-CIA, B-MSCA and B-CP CPSs shall be published according to the schedules defined by the change (amendment) procedures laid down in ERCA CPS and the B-MSA certificate policy, respectively.

Changes to the B-CIA, B-MSCA and B-CP CPSs shall not be public, but shall only be communicated to the relevant parties following the need to know principle.

2.4. ACCESS CONTROLS ON REPOSITORIES

All information available via the MSA website repository shall have read-only access.

All information published on the MSA website repository shall be available via a secure Internet connection.

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 name

3.1.1.1. Certificate subject and issuer

The Certification Authority Reference (CAR) and Certificate Holder Reference (CHR) 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
MSCA	Certification Authority Key Identifier (KID)	Nation numeric Nation alpha Key serial number Additional info CA identifier ('01')
Card Certificates	ExtendedSerialNumber	Serial Number Month Year Type Manufacturer Code

Table 1 Identifiers for MSCA certificate and subjects

Test key certificates, test certificate requests, test key distribution requests and test key distribution messages for the purpose of Interoperability Tests, shall contain the values '54 4B' ("TK") in the additionalInfo field.

The value of the additionalInfo field in the CHR of B-MSCA certificates for Production shall have the value 'FF FF'.

3.1.1.2. Key Distribution Requests and Key Distribution Messages

Key Distribution Requests and Key Distribution Messages are identified by the key identifier of the ephemeral public key generated by the B-MSCA, see section 4.2.1 of this policy. The key identifier value is determined according to section 3.1.1.1 of this policy with the following modifications:

- NationNumeric:	as appropriate for the requesting entity
- NationAlpha:	as appropriate for the requesting entity
- keySerialNumber:	unique for the requesting entity
- additionalInfo:	‘4B 52’ (“KR”, for Key Request), unless it concerns a test KDR. In that case, ‘54 4B’ (“TK”, for Test Key) shall be used.
- CA identifier:	‘01’

3.1.2. Need for names to be meaningful

The meaning of the possible values for the CHR and CAR fields in a card certificate is explained in the Smart Tachograph ERCA certificate policy and in Annex 1C of EU Regulation 799/2016 [3].

3.1.3. Anonymity or pseudonymity of subscribers

The relation between the CHR field in a card certificate issued by the B-MSCA and the legal person (i.e. the Card Holder) holding that certificate is registered by the B-CIA. It cannot be established from the contents of the certificate itself.

Subscriber anonymity is not allowed.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to Prove Possession of Private Key

When submitting a Key Certification Request (KCR) to the B-MSCA, the B-CP shall prove it is in possession of the private key corresponding to the public key in the certificate. It shall do so by signing the KCR contents with that private key. In other words, the KCR shall be self-signed.

The full KCR format, including the signature, is specified in the “B-MSCA - B-CP Interface Requirement Specification” documentation.

3.2.2. Authentication of Organization Identity

As described in section 1.7 of this policy, the Smart Tachograph PKI and in the Symmetric Key Infrastructure participants consists of:

- a single B-MSA, identified in section 1.8.1 of this policy;
- a single B-MSCA, identified in section 1.8.2 of this policy;
- a single B-CIA, identified in section 1.8.3 of this policy;
- a single B-CP, identified in section 1.8.4 of this policy.

Since all of these organizations are directly appointed and no other organizations will need to connect to the Kingdom of Belgium Smart Tachograph system, it is not necessary to authenticate any organization's identity.

3.2.3. Authentication of Individual Identity

3.2.3.1. During Card Application

The B-CIA shall ensure that evidence of a Card Holder's identification and accuracy of the names and associated data are properly examined as part of the registration service during card application.

In particular:

- B-CIA shall inform the Card Holder of the terms and conditions regarding the use of the certificates;
- B-CIA shall communicate this information through a durable means of communication in readily understandable language;
- B-CIA shall collect adequate evidence, from an appropriate and authorized source, of the identity and any specific attributes of the Card Holder. Submitted evidence may be in the form of either paper of electronic documentation. Verification of the Card Holder's identity shall be by appropriate means and in accordance with national law;
- If the Card Holder is a physical person, B-CIA shall check evidence of the identity against a nationally recognized identity document, e.g. a driver's license;
- If the Card Holder is a physical person who is identified in association with a legal person or organizational entity (i.e. a workshop), B-CIA shall check evidence of the Card Holder's identity against a nationally recognized identity document, e.g. a national ID card, and evidence that the Card Holder is indeed associated with the legal person or organizational entity;
- if the Card Holder is an organizational entity (i.e. a transport company), B-CIA shall check the Card Holder's identity against a recognized registration.

3.2.3.2. During Card Delivery

The B-CIA shall authenticate the individual identity of a Card Holder before delivering a tachograph card:

- For driver cards, workshop cards or control cards, the B-CIA shall verify the identity of the person receiving the card in person by means of a check of a valid identity document containing a photograph. The person receiving the card shall be same person as the Card Holder of that card;
- For company cards, the company requesting the card shall communicate the identity of the person receiving the card on behalf of the company to B-CIA prior to distribution. During distribution, B-CIA shall verify the identity of this person in person by means of a check of a valid.

3.2.4. Validation of Authority

No stipulation.

3.2.5. Criteria for interoperation

B-MSCA shall not rely on any external certificate authority for the certificate signing and key distribution services they provide to the smart tachograph system.

If the B-MSCA must rely on an external PKI for any other service or function, they shall review and approve the Certificate Policy and/or CPS of the external certification service provider prior to applying for certification services as a subject.

3.3. I&A FOR RE-KEY REQUESTS

The Identification and Authentication (I&A) procedures for re-key requests (see sections 4.1.7 and 4.2.9 of this policy) shall be the similar to those described in section 3.2 of this policy with the addition of an outer signature.

3.4. I&A FOR REVOCATION REQUESTS

B-MSCA does not allow certificate revocation.

4. LIFE-CYCLE OPERATIONAL REQUIREMENTS FOR CERTIFICATES AND MASTER KEYS

This chapter specifies the message formats, cryptographic mechanisms and procedures for the application and distribution of certificate signing request, certificates and symmetric master keys between the ERCA and the B-MSCA.

Furthermore, this chapter describe the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates and symmetric keys for cards and for the application and distribution of encrypted data for motion sensors between the B-MSCA and B-CP.

The cryptographic strength of the security mechanisms shall be at least as strong as the strength of the transported keys and encrypted data.

4.1. PUBLIC KEY CERTIFICATE APPLICATION AND ISSUANCE

4.1.1. Certificate Application

B-MSCA certificate signing requests (CSR) can only be submitted by B-MSCA recognised by B-MSA via a compliance statement.

Key Certification Requests (KCR) can only be submitted to the B-MSCA by the B-CP.

Continuation of key certification services from the B-MSCA shall depend on timely receipt by the B-MSA of the audit reports for all PKI participants, demonstrating that all of these parties are continuing to fulfil their obligations as laid down in this B-MSA certificate policy.

As there is only one B-CP appointed party that can submit a key certification request, there is no enrolment process for such parties.

The responsibilities of the B-CP regarding an application for a card certificate are:

- to securely generate an RSA or ECC key pair (as applicable. For an ECC key pair, the B-CP shall use standardized domain parameters having the same key strength as those used in B-MSCA certificate indicated in the CAR field of the Key Certification Request;
- to create a Key Certification Request (KCR) message and send it to the B-MSCA. The format and contents of the KCR shall be identical to the tachograph card certificate to be signed by the B-MSCA. However, the KCR signature shall be verifiable with the public key contained in the KCR. For RSA certificates, the signature shall be created as specified in section 3.3.2 of Appendix 11 to Annex 1C of EU Regulation 799/2016 [3]. For ECC certificates, the signature shall be created as specified in CSM_150 in section 9.3 of Appendix 11 of EU Regulation 799/2016 [3].
- to digitally sign the KCR.

A CSR shall be in TLV-format. *Table 2* Certificate signing request format shows the CSR encoding, including all tags. For the lengths, the DER encoding rules specified in shall be used. The values are specified in the remainder of this section.

Data Object	**Req**	**Tag**
Authentication	c	‘67’
ECC (CV) Certificate	m	‘7F 21’
Certificate Body	m	‘7F 4E’
Certificate Profile Identifier	m	‘5F 29’
Certification Authority Reference	m	‘42’
Certificate Holder Authorisation	m	‘5F 4C’
Public Key	m	‘7F 49’
Standardised Domain Parameters OID	m	‘06’
Public Point	m	‘86’
Certificate Holder Reference	m	‘5F 20’
Certificate Effective Date	m	‘5F 25’
Certificate Expiry Date	m	‘5F 24’
Inner Signature	m	‘5F 37’
Certification Authority Reference of Outer Signature Signatory	c	‘42’
Outer Signature	c	‘5F 37’

Table 2 **Certificate signing request format**

m: require; c: conditional

4.1.1.1. Verification of CSR contents

B-MSCA shall ensure that a CSR originating from a B-CP is complete, accurate, and duly authorized. B-MSCA shall only sign a certificate if this is the case.

Checks for correctness, completeness and authorization shall be performed automatically by the B-MSCA. If the request is correct and complete, the B-MSCA authorizes the signing of the certificate.

For each CSR it receives, B-MSCA shall verify that:

- the CSR format complies with *Table 2* Certificate signing request format;
- the CAR contained in the request indicates the B-MSCA private key currently valid for signing the certificates;
- the CHR is unique across the entire Smart Tachograph system;
- the domain parameters specified in the request are listed in Table 1 of Annex 1C, Appendix 11, and the strength of these parameters matches the strength of the B-MSCA key indicated in the CAR;

- the public point in the request has not been certified by the B-MSCA previously and has not been used as an ephemeral key for symmetric key distribution previously (see section 4.2.3 of this policy), even for interoperability test purposes;
- the public point in the request is on the curve indicated in the request;
- the inner signature can be verified using the public point and the domain parameters indicated in the request. This proves that the component personalizer is in possession of the private key associated with the public key;

If any of these checks fails, the B-MSCA shall reject the CSR. The B-MSCA shall communicate the rationale for any request rejection to the B-CP in an appropriate error coding message.

4.1.1.2. Certificate generation, distribution and administration

If all checks succeed, the B-MSCA shall proceed to sign the certificate signing request and generate the certificate. The format of the certificate complies with *Table 5 Certificate profile* in section 7.1 of this policy.

The following information shall be recorded in the B-MSCA database for each certificate signing request received:

- the complete KCR originating from the B-CP;
- the Certificate Holder Reference (CHR);
- the Certificate Authority Reference (CAR);
- the certified public key;
- the EOV (for Gen-1 certificates) or CEfD and CExD (for Gen-2 certificates);
- the complete resulting tachograph card certificate, if any;
- the certificate status “Valid” if the certificate is issued or “Rejected” in case the CSR is rejected;
- a timestamp.

4.1.2. Certificates

The format of the public key certificates can be found in section 7.1 of this policy.

B-MSCA shall create the signature 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, as specified in Annex 1C, Appendix 11, CSM_50. The signature format shall be plain as specified in BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28 [8].

Validity period of certificates:

- MSCA_card certificates **shall be valid for no more than seven years and one month from** issuance.
- MSCA_VU-EGF certificates **shall be valid for no more than seventeen years and three months from** issuance.
- Card_MA Workshop cards certificates **shall be valid for no more than one year** from issuance.
- Card_MA Driver cards certificates **shall be valid no more than five years** from issuance.
- Card_MA Company cards certificates **shall be valid no more than five years** from issuance.
- Card_MA Control cards certificates **shall be valid no more than two years** from issuance.
- VU_MA certificates **shall be valid no more than fiteen years and 3 months** from issuance.
- VU_Sign certificates **shall be valid no more than fiteen years and 3 months** from issuance.
- EGF_MA certificates **shall be valid no more than fiteen years** from issuance.
- Card_Sign driver certificates **shall be valid no more than five years and one month** from issuance.
- Card_Sign workshop certificates **shall be valid no more than one year and one month** from issuance.

4.1.3. Exchange of Requests and Responses

For transportation of certificate signing requests and certificates, a trusted curier and CD-R media should be used between B-MSCA and the ERCA. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

The B-MSCA shall write one to three copies of each certificate signing requests to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (txt file), Base64 (.pern file) or binary (.bin file) format.

For transportation of certificate signing requests and certificates a secure connection between B-MSCA and the B-CP shall be used.

4.1.4. Certificate Acceptance

The courier signs for receipt of the B-MSCA certificate at the ERCA premises.

Upon reception of the certificates from ERCA, the B-MSCA shall check that:

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

If any of these checks fail, the B-MSCA shall abort the process and contact the ERCA.

Certificate rejection is managed according to the certificate revocation procedure as described in section 4.1.9 of this policy.

Upon reception of the certificates from B-MSCA, the B-CP shall check that:

- the format of the certificate complies with *Table 5 Certificate profile* in section 7.1 of this policy;
- all certificate field values match the values requested in the CSR;
- the certificate signature can be verified using the B-MSCA public key indicated in the CAR field.

If any of these checks fail, the B-CP shall abort the process and contact the B-MSCA.

4.1.5. Key Pair and Certificate Usage

B-MSCA shall maintain a database containing certificate status information for all card certificates issued.

B-MSCA shall communicate the symmetric master keys, the keys derived from these master keys or the data encrypted with these master keys to B-CP by appropriately secured means for the sole purpose for which the keys and data are intended, as specified in Annex IC Appendix 11 [3].

The B-MSCA shall use any key pair and the corresponding certificate in accordance to section 6.2 of this policy.

4.1.6. Certificate Renewal

Renewal of certificates, issued by B-MSCA, i.e. the extension of the validity period of an existing certificate, is not allowed.

4.1.7. Certificate Re-key

Certificate re-key for all certificates issued by the B-MSCA is not allowed.

Certificate application, processing, issuance, acceptance and publication is the same as for the initial key pair.

For B-MSCAcertificates, the certificate re-key means the signing of a new B-MSCA certificate, in replacement of an existing B-MSCA certificate. The B-MSCA certificate re-key shall take place either:

- when an B-MSCA is nearing the end of the usage period of (one of) its private key(s). In this case, re-key shall be done in a timely manner to ensure that the B-MSCA can continue operations after the end of this period;
- following certificate revocation.

Certificate application, processing, issuance, acceptance and publication is the same as for the initial key pair.

The B-MSCA is allowed to use multiple MSCA private key concurrently, with overlapping validity periods of the corresponding certificates. In the CPS, the B-MSCA shall specify how many MSCA certificates it will hold concurrently, and at which moments these certificates will be renewed.

4.1.8. Certificate Modification

Certificate modification is not allowed.

4.1.9. Certificate Revocation and Suspension

4.1.9.1. Circumstances for equipment certificates revocation

Revocation of equipment and card certificates issued by B-MSCA is not allowed.

4.1.9.2. Circumstances for MSCA certificates revocation

B-MSCA certificates shall be revoked by ERCA in the following circumstances:

- rejection on receipt of a newly issued certificate;
- compromise or suspected compromise of the B-MSCA private key;
- loss of the B-MSCA private key;
- B-MSCA termination;
- B-MSA or B-MSCA failure to meet obligations under the Regulation and ERCA certificate policy.

4.1.9.3. Who can request revocation

B-MSCA certificate revocation (if the case) shall originate from the following entities as authoritative:

- ERCA;
- B-MSA;
- B-MSCA;

4.1.9.4. Procedure for revocation request

The B-MSCA certificate revocation procedure is described in B-MSCA CPS.

4.1.9.5. Revocation request grace period

The grace period for the B-MSCA certificate revocation by ERCA is five working days from the start of the circumstances for revocation when any of the authoritative entities in section 4.1.9.3 Who can request revocation have submitted a revocation request.

4.1.9.6. Revocation checking requirements for relying parties

Relying parties shall be responsible for checking the certificate status information published in ERCA repository.

4.1.9.7. Certificate status issuance frequency

The status of the B-MSCA public key certificates shall be retrievable online from https://dtc.jrc.ec.europa.eu/.

Status of equipment certificates issued by B-MSCA is kept in the B-MSCA internal repository. This repository does not need to be public.

B-MSCA shall maintain certificate status information and make this information available to parties having a legitimate interest upon request.

4.1.9.8. Maximum latency for CRLs

Not applicable.

4.1.9.9. On-line revocation / status checking availability

B-MSCA revocation / status information published in ERCA repository is only guaranteed to be available during ERCA normal working hours.

B-MSCA does not maintain revocation status for the issued certificates.

4.1.9.10. On-line revocation / status checking requirements

No stipulation.

4.1.9.11. Other forms of revocation advertisements available

None.

4.1.9.12. Special requirements concerning key compromise

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

All private keys and master keys shall immediately be deactivated as described in section 6.2.9 of this policy (such that they cannot be used) if a compromise is suspected.

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

If the master key is compromised, or suspected to be compromised, the B-CP shall notify the incident to ERCA and to the B-MSA without unnecessary delay and at least within 8 hours of detection.

In their notification, the B-MSCA and B-CP shall indicate the circumstances under which the compromise occurred.

If a compromise is confirmed or cannot be ruled out, the keys shall be destroyed as described in section 6.2.10 of this policy, including all (backup) copies of it.

B-MSA and B-CP shall perform a follow-up security investigation according to their security incident handling procedures and the results shall be reported to ERCA and B-MSCA.

If a compromise can be ruled out, the keys shall be activated again as described in section 6.2.8 of this policy.

4.1.9.13. Certificate suspension

Equipment certificate, issued by B-MSCA suspension is not allowed.

4.1.9.14. Certificate Status Service

The B-MSCA revocation / status information published in ERCA repository is only guaranteed to be available during ERCA normal working hours.

B-MSCA does not maintain revocation status for the issued certificates.

4.1.9.15. End of Subscription

Subscription for the B-MSCA's certificate signing services ends when the B-MSA and/or B-MSCA decides for B-MSCA termination. Such a change is notified to ERCA by the B-MSA as a change to the B-MSA certificate policy.

In the case of subscription ending, the decision to submit a certificate revocation request for any valid B-MSCA certificates, or to allow all B-MSCA certificates to expire, is the responsibility of the B-MSA.

B-CP are responsible for ensuring the equipment is provided with the appropriate keys and certificates.

End of subscription for the equipment manufacturers ends when B-CP subscription for the B-MSCA's certificate signing services ends.

4.1.9.16. Key Escrow and Recovery

Key escrow is expressly forbidden, meaning that B-MSCA private keys shall not be exported to or stored in any system apart from the B-MSCA systems.

B-MSCA shall use the appropriate security controls and backup the B-MSCA private keys in order to support its business continuity in case of its systems hardware or software failure. B-MSCA private keys must never leave the hardware module security environment in plain text and strong encryption must be used for the backup and storage operations.

4.2. MASTER KEY APPLICATION AND DISTRIBUTION

4.2.1. Master Key Application

As specified in Annex 1C of EU Regulation 799/2016 [3], workshop cards shall be equipped with the Motion Sensor Master Key – Workshop Card part (KM-WC). This key is needed to allow a workshop to perform pairing of Motion Sensor to a Vehicle Unit.

Annex 1C also specifies that control cards and workshop cards shall be equipped with the DSRC Master Key. This key is needed to allow a control officer to decrypt a message received from a VU over a DSRC link and to verify its authenticity. Workshops need this key to verify that a VU is able to send such messages.

These master keys are generated by the ERCA. Distribution of these keys can be requested by B-MSCA as specified in the ERCA certificate policy.

In order to be able to store these master keys in the corresponding cards, the B-CP shall have these keys at its disposal.

As the B-MSCA does not use the the symmetric keys for its operation, in order to increase the overall security of the process, the Key Distribution Requests (KDR) are generated by B-CP, validated by B-MSCA and afterwards transferred to ERCA by the trusted courier. The the Key Distribution Messages (KDM) are generated by ERCA and are transferred directly to B-CP by the trusted courier.

In this process B-MSCA does not generate or store any ephemeral communication keys.

Therfore, the process for exchanging the Key Distribution Requests (KDR) and Key Distribution Messages (KDM) is as follows:

1. B-MSA nominates the trusted courier;
2. B-CP generates a Key Distribution Request (KDR) for a master key conforming to ERCA certificate policy, including the generation of an ephemeral key pair for key agreement in their HSM;
3. B-CP sends over the KDRs to the B-MSCA by means of the trusted courier;
4. B-MSCA verifies the correctness of the KDRs as specified in section 4.2.2.1 of ERCA certificate policy;
5. B-MSCA sends the KDRs to the ERCA by the trusted courier, as specified in the ERCA certificate policy and the ERCA CPS;
6. ERCA creates the Key Distribution Messages (KDM) as specified in the ERCA certificate policy;
7. ERCA sends over the KDMs to B-CP by means of the trusted courier;
8. B-CP verifies the correctness of the KDMs as specified in section 4.2.6 of ERCA certificate policy;
9. B-CP processes the KDMs as specified in section 4.2.6 of ERCA certificate policy.

A KDR shall be in TLV-format. *Table 3 Key distribution request format* shows the KDR encoding, including all tags. For the lengths, the DER encoding rules shall be used. The values are specified in the remainder of this section.

Data Object	Req	Tag
Key Distribution Request	m	'A1'
Request Profile Identifier	m	'5F 29'
Message Recipient Authorisation	m	'83'
Key Identifier	m	'84'
Public Key (for ECDH key agreement)	m	'7F 49'
Standardised Domain Parameters OID	m	'06'
Public Point	m	'86'

Table 3 Key distribution request format

m: require;

4.2.2. Master Key Application Processing

4.2.2.1. Verification of KDR contents

Before forwarding the Key Distribution Request received from the B-CP to the ERCA, the B-MSCA shall verify that:

- the KDR format complies with the specification in section 4.2.1 of the ERCA certificate policy;
- the type of master key requested in the KDR is the KM-WC or the KDSRC;
- the version number of the master key corresponds with (one of) the version number(s) published by the ERCA;
- the key identifier of the ephemeral public has not been used before, even for Interoperability Test purposes;
- the ephemeral domain parameters specified in the request are the same as the domain parameters of the currently used B-MSCA certificate(s);
- the ephemeral public point in the request has not been certified by the B-MSCA in a tachograph card certificate. It also has not been used for key distribution previously, even for Interoperability Test purposes;
- the ephemeral public point specified in the request is on the curve specified in the request;
- If any of these checks fail, the B-MSCA shall not send the KDR to the ERCA, but shall notify the B-CP of the problem. The B-CP shall then generate a new KDR.

If all checks pass, the B-MSCA shall calculate and store a hash over the complete KDR, using the hashing algorithm linked to the key size of the requested master key, as specified in Annex 1C of EU Regulation

799/2016 [3], Appendix 11, CSM_50. This hash will be used by the ERCA to verify the authenticity of the KDR, see section 4.2.2.1 of the ERCA certificate policy.

Next, the B-MSCA shall send the KDR to the ERCA by means of a courier.

4.2.2.2. KDM generation, distribution and administration

If all checks succeed, ERCA shall proceed to prepare the key distribution message (KDM) by determining the symmetric key requested by the B-MSCA and following the steps as described in section 4.2.3 of this policy (from step 2).

4.2.3. Protection of Confidentiality and Authenticity of Symmetric Keys

The confidentiality and authenticity of symmetric keys distributed by ERCA to B-MSCA shall be protected via an Elliptic Curve Integrated Encryption Scheme (ECIES). This scheme allows for agreement between ERCA and B-MSCA on encryption keys and MAC keys to be used to protect the master symmetric keys during distribution. The ECIES has been standardized in ISO/IEC 18033-2 [9]. The ECIES variant to be used by ERCA to B-MSCA for symmetric key distributions uses the following cryptographic algorithms, in accordance with Appendix 11 of Annex 1C of the Commission Implementing Regulation (EU) 799/2016 [3], amended by the European Commission in 2018:

- Key derivation function: KDF2;
- Message authentication code algorithm: AES algorithm in CMAC mode;
- Symmetric encryption algorithm: AES in the Cipher Block Chaining (CBC) mode of operation.

On a high level, the ECIES consists of the following steps. More details are given for each step below:

1. The B-MSCA generates a unique ephemeral ECC key pair for Diffie-Hellman key agreement and sends the public key to ERCA in the Key Distribution Request, see *Table 3 Key distribution request format*.
2. ERCA similarly generates a unique ephemeral ECDH key pair, and uses the Diffie-Hellman key agreement algorithm together with its own private key and the B-MSCA's ephemeral public key to derive a shared secret.
3. Using the key derivation function, the shared secret and additional information detailed below, ERCA derives an encryption key and a MAC key.
4. ERCA uses the encryption key to encrypt the symmetric key to be distributed.
5. ERCA uses the MAC key to calculate a MAC over the encrypted key, the Message Recipient Authorization and the Key Identifier.

Any operations with the ephemeral private key, with the shared secret and with the derived keys KENC and KMAC shall take place in an HSM complying with the requirements in section 6.2 of this policy.

The ephemeral private key shall never leave the HSM.

ERCA shall record the value of the MAC. As described in section 4.2.6 of this policy, the B-MSCA will use these values to verify the authenticity of the key distribution message.

4.2.4. Key Distribution Messages

After performing the Master Key application processing (see section 4.2.2 of this policy), ERCA shall construct a key distribution message as shown in *Table 4 Key distribution message format*. For the lengths, the DER encoding rules shall be used. The values are specified in the remainder of this section.

Data Object	Req	Tag
Key Distribution	m	‘A1’
Request Profile Identifier	m	‘5F 29’
Message Recipient Authorisation	m	‘83’
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement	m	‘84’
Public Point of ERCA for ECDH key agreement	m	‘86’
Encrypted symmetric key	m	‘87’
MAC	m	‘88’

Table 4 Key distribution message format

4.2.5. Exchange of Requests and Responses

For transportation of key distribution requests and key distribution messages, CD-R media should be used. The CD-R shall be 12 cm media in single-session mode (ISO 9660:1988 formatted).

The B-MSCA shall write one to three copies of each key distribution request to the transport medium for transport to the ERCA. Copies shall be in hexadecimal ASCII (txt file), Base64 (.pern file) or binary (.bin file) format.

For both KDRs and KDMs, the transport media and the printouts shall be handed over between the courier and the B-MSCA employee in the B-MSCA area.

4.2.6. Master Key Acceptance

The courier signs for receipt of the key distribution message at ERCA premises.

Upon reception of the key distribution message at the B-MSCA premises, the B-MSCA shall check that:

- the transport media is readable; i.e. not damaged or corrupted;
- the format of the message complies with *Table 4 Key distribution message format*;
- the message is genuine. The B-MSCA shall do this by contacting ERCA as described in ERCA CPS and verifying that the MAC in the received KDM matches the MAC in the KDM sent by ERCA;
- the master key type and version in the message matches the requested type and version;

- the public point specified in the message is on the curve specified by the key distribution request sent by the B-MSCA to ERCA.

If any of these checks fail, the B-MSCA shall abort the process and contact ERCA. If all of these checks succeed, the B-MSCA shall:

- use the ECKA-DH algorithm to derive a shared point (Kx, Ky), as described in step 3 in section 4.2.3 of this policy, using the B-MSCA's ephemeral private key indicated by the key identifier in the message and ERCA's ephemeral public key. The B-MSCA shall verify that the shared point is not the infinity point; if it is, the B-MSCA shall abort the process and contact ERCA. Else, the B-MSCA shall form the shared secret K by converting Kx to an octet string (Conversion between Field Elements and Octet Strings);
- derive the keys KENC and KMAC as described in step 4 in section 4.2.3 of this policy,
- verify the MAC over the encrypted symmetric key, as described in step 5 in in section 4.2.3 of this policy. If this verification fails, the B-MSCA shall abort the process and contact ERCA;
- decrypt the symmetric key as described in step 4 in section 4.2.3 of this policy. The B-MSCA shall verify that the padding of the decrypted key, if any, is correct. If this verification fails, the B-MSCA shall abort the process and contact ERCA.

Any operations with the ephemeral private key, with the shared secret and with the derived keys K_{ENC} and K_{MAC} shall take place in an HSM complying with the requirements in section 6.2 of this policy.

After successful recovery of the master key, or when the key distribution process is aborted and no KDM renewal (see section 4.2.8 of this policy) is initiated, the B-MSCA shall securely destroy its ephemeral private key for key agreement in the HSM, as well as the encryption key K_{ENC} and the MAC-ing key K_{MAC}.

In its CPS the B-MSCA shall describe the message formats, cryptographic mechanisms and procedures for the application and distribution of equipment certificates and symmetric keys for cards and for the application and distribution of encrypted data for motion sensors between the B-MSCA and B-CP.

4.2.7. Master Key Usage

The B-CP shall use any received master key in accordance to section 6.2 of this policy.

4.2.8. KDM Renewal

KDM renewal means the issuance of a copy of an existing KDM to B-MSCA without changing the ephemeral public key or any other information in the KDM.

KDM renewal may take place only if the original transport media received at the B-MSCA are damaged or corrupted. Damage or corruption of transport media is a security incident which shall be reported by B-MSCA to the B-MSA and ERCA.

Subsequent to this report, the B-MSCA may send a KDM renewal request to ERCA, referring to the original key distribution request. This procedure is described in B-MSCA CPS.

ERCA shall only accept KDM renewal request endorsed by the B-MSA which approved the B-MSCA.

Note: In case the B-MSCA needs to send a request to re-distribute a master key that was already successfully distributed to the B-MSCA, it shall generate a new key distribution request, using a newly generated ephemeral key pair. Such a request may lead ERCA to initiate an investigation of the possibility of key compromise.

4.2.9. Master Key Re-key

To receive the new version of a master key, B-MSCAs shall submit a new KDR. Requesting a new master key shall take place in a timely manner so that the key (or derived keys or encrypted data for motion sensors) can be placed in time in newly issued components.

Key application, processing, distribution and acceptance is the same as for the initial key.

4.2.10. Symmetric Key Compromise Notification

If the B-MSCA detects or is notified of the compromise or suspected compromise of a symmetric master key, the B-MSCA shall notify this to ERCA and the B-MSA without unnecessary delay and at least within 8 hours of detection. In their notification, the B-MSCA shall indicate the circumstances under which the compromise occurred. B-MSA shall perform a follow-up security investigation according to its security incident handling procedure and the result shall be reported to ERCA and B-MSCA subscribers.

4.2.11. Master Key Status Service

The status of symmetric master keys shall be retrievable online from https://dtc.jrc.ec.europa.eu/. The ERCA shall maintain the integrity of the status information.

Master key status information published in the ERCA repository shall be updated on the first working day of each week.

The availability of the website mentioned above shall be guaranteed during normal working hours.

4.2.12. End of Subscription

Subscription for ERCA's key distribution services ends when B-MSA decides for B-MSA termination. Such a change is notified to ERCA by the B-MSA as a change to the national policy.

In the case of subscription ending, the B-MSCA shall securely destroy all copies of any symmetric master key in its possession.

4.2.13. Key Escrow and Recovery

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

B-MSCA shall use the appropriate security controls and backup the symmetric master key in order to support its business continuity in case of its systems hardware or software failure. The symmetric master key must never leave the hardware module security environment in plain text and strong encryption must be used for the backup and storage operations.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL SECURITY CONTROLS

5.1.1. Site location and construction

The key management and certificate generation and revocation services of the B-MSCA and the B-CP shall be housed in a secure area, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorized access, damage, and interference. Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

The B-CIA, the B-MSCA, and the B-CP shall provide continuous monitoring and alarm facilities to detect and register any unauthorized or irregular attempts to access its resources, and to react upon them in a timely manner.

5.1.2. Physical access

The B-CIA, B-MSCA, and B-CP shall ensure that physical access to trustworthy systems and critical services is controlled and registered. Physical access to facilities concerned with key generation, certificate generation and revocation management shall be limited to adequately identified and authorized individuals, i.e. persons in a trusted role as described in section 5.2.1 of this policy.

5.1.3. Power and air conditioning

In their CPSs, the B-CIA, B-MSCA, and B-CP shall investigate the possible consequences of an interruption of electric power to their critical services. If necessary, they shall install electrical power backup systems to mitigate any unacceptable consequences.

5.1.4. Water exposures

The B-CIA, B-MSCA, and B-CP shall take measures to minimize the risk of exposure to water of their critical systems, especially key management and certificate generation systems.

5.1.5. Fire prevention and protection

The B-CIA, B-MSCA, and B-CP shall take measures to minimize the risk of fire in the facilities housing their systems.

5.1.6. Media storage

The B-CIA, B-MSCA, and B-CP shall take measures to protect any storage media used to store confidential data, such as hard disks, smart cards and HSMs, against unauthorized or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).

Confidential data shall be protected to safeguard data integrity and confidentiality when stored, in use and when exchanged over networks. Confidential data that is deleted shall be permanently destroyed, e.g. by overwriting multiple times with random data.

5.1.7. Waste disposal

The B-CIA, B-MSCA, and B-CP shall control waste disposal in such a way that the risk of compromise of confidential data is minimized. Information stored on digital media to be disposed shall be permanently destroyed by overwriting it.

5.1.8. Off-site backup

In their CPSs, the B-MSCA and the B-CP shall consider the use of an off-site backup of all critical information, especially B-MSCA private keys and master keys, in order to ensure disaster recovery.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted roles and the responsibilities of each role

In their Certification Practice Statement (CPS), the B-CIA, B-MSCA, and B-CP shall identify the trusted roles on which the security of the operations is dependent, as well as the responsibilities of each trusted role. These trusted roles shall be used in secure operating procedures. The trusted roles and the associated responsibilities shall be documented in job descriptions. These job descriptions shall be defined from the viewpoint of separation of duties and least privilege.

B-CIA, B-MSCA, and B-CP personnel shall be formally appointed to a trusted role by senior management of the respective organization.

5.2.2. Number of persons required per task

The B-CIA, B-MSCA, and B-CP shall identify in their CPSs which tasks are considered critical and consequently need multiple-person control. Such tasks shall at least include key pair generation, use or export of private keys and symmetric key import or export. For each critical task, the CPSs shall list the number of persons in a trusted role that are needed to carry out that task.

5.2.3. Identification and authentication for each role

The B-CIA, B-MSCA, and B-CP systems shall ensure effective user administration and access management. Access to critical systems shall be limited to individuals who are properly authorized and on a need-to-know basis. Access to information and applications shall be restricted, only allowing access to resources as necessary for carrying out the role allocated to a user.

All users shall be identified, authenticated and authorized by assignment of a role before using any systems.

5.2.4. Roles requiring separation of duties

No single person shall be allowed to simultaneously assume more than one of the trusted roles identified according to section 5.2.2 of this policy.

B-CIA, B-MSCA, and B-CP shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved. B-CIA, B-MSCA, and B-CP shall ensure that the ISMS policies address personnel training, clearances and roles. B-CIA, B-MSCA, and B-CP ISMS implementations should conform to the requirements described in ISO 27001 [19].

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, experience, and clearance requirements

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

All personnel in trusted roles shall have appropriate background screening with positive result. Detailed clearance requirements for personnel in trusted roles shall be discussed in the B-CIA, B-MSCA, and B-CP CPSs.

5.3.2. Background check procedures

Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the CPSs. Personnel in trusted roles shall have no conflicts of interest that might prejudice the impartiality of the B-CIA, B-MSCA, and B-CP operations.

5.3.3. Retraining frequency and requirements

Retraining of personnel shall take place at least in case of changes to documented policies, procedures, or operations.

5.3.4. Job rotation frequency and sequence

No stipulation.

5.3.5. Sanctions for unauthorized actions

B-CIA, B-MSCA, and B-CP personnel shall be held accountable for their activities, which shall be logged in event logs as described in section 5.4 of this policy. Possible consequences of unauthorized actions should be defined in personnel employment contracts.

5.3.6. Independent contractor requirements

Tasks may be outsourced to a specialized company, or personnel from independent contractors may be hired to carry out the responsibilities. However, in such cases the personnel controls defined in this section 5.3 and in the CPS shall be maintained.

The B-CIA, B-MSCA, and B-CP shall retain responsibility for all aspects of the provision of their services as described in this policy, even if some functions are outsourced to subcontractors. Responsibilities of any subcontractors shall be clearly defined by the respective PKI participant and appropriate arrangements made to ensure that third parties are bound to implement any controls specified in this policy.

5.3.7. Documentation supplied to personnel

The B-CIA, B-MSCA, and B-CP shall provide their personnel with up-to-date versions of the documentation necessary for carrying out their role. In their B-CIA, B-MSCA, and B-CP CPSs, each of these parties shall identify the documentation to be provided to each role.

5.3.8. Training requirements

B-CIA, B-MSCA, and B-CP personnel training shall be managed according to a training plan described in the B-CIA, B-MSCA, and B-CP CPSs.

5.3.9. Screening, Background and Qualification

Trusted personnel should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

Personnel appointment to trusted roles shall be managed in accordance with a screening process established in the B-CIA, B-MSCA and B-CP CPSs.

5.4. AUDIT LOGGING PROCEDURES

All significant security events in B-CIA, B-MSCA and B-CP software shall be automatically time-stamped and recorded in the system log files. These include at least the following:

- Successful and failed attempts to create, update, remove or retrieve status information about accounts of personnel, or to set or revoke the privileges of an account;
- Successful and failed attempts to set or change an authentication method (e.g. password, biometric, cryptographic certificate) associated to a personal account;
- Successful and failed attempts to log-in and log-out on an account;
- Successful and failed attempts to change the software configuration;
- Software starts and stops;
- Software updates;
- System start-up and shut-down;
- Successful and failed interactions with the database(s) containing data on critical processes, including connection attempts and read, write and update or removal operations.

Furthermore, the B-CIA software shall log the following events:

- Reception of a request to issue to tachograph card from a Card Holder;
- Sending a card application request to the B-CP;
- Sending a certificate revocation request to the B-MSCA (if applicable).

Furthermore, the B-MSCA software shall log the following events:

- Reception of key certification requests;
- Reception of a certificate revocation request from the B-CIA or the B-MSA (if applicable);
- Successful and failed attempts to process a key certification request and sign a certificate;
- Successful and failed attempts to connect to or disconnect from an HSM;
- Successful and failed attempts to authenticate a user to an HSM;
- Successful and failed attempts to generate or destroy a key pair inside an HSM;
- Successful and failed attempts to import or export a private key to or from an HSM;
- Successful and failed attempts to change the life cycle state of any key pair;
- Successful and failed attempts to use a private key inside an HSM for any purpose.

Furthermore, the B-CP software shall log the following events:

- Reception of a card application message from the B-CIA;
- Sending of a key certification request to the B-MSCA;
- Reception of a tachograph card certificate;
- Generation of a key distribution request, including generation of an ephemeral key pair for key agreement inside an HSM;

- Reception and processing of a key distribution message, including import of the master key into an HSM;
- Personalization of a tachograph card;
- Successful and failed attempts to connect to or disconnect from an HSM;
- Successful and failed attempts to authenticate a user to an HSM;
- Successful and failed attempts to import or export a master key to or from an HSM;
- Successful and failed attempts to destroy a master key inside an HSM;
- Successful and failed attempts to generate a card key pair inside an HSM;
- Successful and failed attempts to export a card key pair from an HSM;
- Successful and failed attempts to destroy a card key pair inside an HSM;
- Successful and failed attempts to change the life cycle state of any key;
- Successful and failed attempts to use a master key inside an HSM for any purpose.

In order to be able to investigate security incidents, where possible the system log shall include information allowing the identification of the person or account that has performed the system tasks.

The integrity of system event logs shall be maintained and shall be protected from unauthorised inspection, modification, deletion or destruction. B-CIA, B-MSCA and B-CP system events logs shall be backed-up and stored in accordance with procedures described in the respective CPSs.

The B-CIA, B-MSCA and B-CP shall process system event logs at least following an alarm or anomalous event, in order to establish its probable cause.

Furthermore, the B-CIA, B-MSCA and B-CP shall periodically inspect system logs for integrity.

Inspection of system event logs shall take place at least annually.

5.4.1. Audit Log Retention

Audit log retention period for B-CIA, B-MSCA and B-CP shall be indefinite.

5.4.2. Audit Log Backup

Two copies of the consolidated log shall be made and stored in separate physically secured locations.

The audit log shall be stored in a way that makes it possible to examine the log during its retention period.

The audit log shall be protected from unauthorized access.

5.5. RECORDS ARCHIVAL

5.5.1. Types of records archived

The B-CIA, B-MSCA and B-CP shall provide in their CPSs an overview of all records which shall be archived.

5.5.2. Retention period for archive

For all archived information, archival periods shall be indefinite. The B-CIA, B-MSCA and B-CP shall take measures to ensure that the record archive is stored in such a way that loss is reasonably excluded.

5.5.3. Protection of archive

The B-CIA, B-MSCA and B-CP shall put in place measures and procedures to ensure that:

- only persons in authorized roles can view the archive;
- the integrity, authenticity and confidentiality of archived records is protected;
- the archive is protected against deletion;
- the archive is protected against deterioration of the media on which it is stored;
- the archive is protected against (future) obsolescence of hardware, operating systems and software.

The B-CIA, B-MSCA and B-CP shall document these measures and procedures in their CPSs.

5.5.4. Archive backup procedures

The B-CIA, B-MSCA and B-CP shall document appropriate back-up and recovery procedures for all relevant data.

5.5.5. Requirements for time-stamping of records

Archived records shall be time-stamped as necessary to ensure the usefulness of the archive.

5.5.6. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

The B-CIA, B-MSCA and B-CP shall document procedures to retrieve information from the archive and verify the correctness of such data.

5.6. KEY CHANGEOVER

5.6.1. MSCA key pairs

B-MSCA shall use a MSCA private key for a period of two years. In order to guarantee the continuation of its services, the B-MSCA shall generate a new MSCA key pair in time. The B-MSCA shall request the ERCA to sign a new MSCA certificate for the new public key by sending a certificate signing request, using the procedure specified in section 4.1 of the ERCA certificate policy. The MSCA shall take into account the guaranteed turnaround time of the ERCA of one month.

5.6.2. Master key

In case the ERCA has generated a new version of a master key, as specified in Appendix 11 sections 9.2.1.2 and 9.2.2.2, the availability of a new key shall be published on the ERCA website, together with its version number and length.

To receive the new version, B-MSCA shall submit a new KDR in order to receive the new version of a master key, using the procedure specified in section 4.2 of the ERCA certificate policy. The MSCA shall take into account the guaranteed turnaround time of the ERCA of one month.

5.6.3. Tachograph card key pairs

Tachograph card key pairs shall never be changed.

5.7. KEY BACKUP

5.7.1. MSCA Keys

B-MSCA private key and symmetric key may be backed up, using a key recovery procedure requiring at least dual control. The procedure used shall be stated in the B-MSCA CPS. It is allowed to backup private signing keys in encrypted format; if decrypting requires HSM and at least dual control and requirements in section 6.2 of this policy are fulfilled.

Back-up and recovery procedures for all relevant data shall be described in the B-MSCA Back-up and Recovery Plan and/or B-MSCA Back-up and Recovery Procedure.

5.7.2. CP Keys

B-CP key may be backed up, using a key recovery procedure requiring at least dual control. The procedure used shall be stated in the B-CP CPS. It is allowed to backup private signing keys in encrypted format; if decrypting requires HSM and at least dual control and requirements in section 6.2 of this policy are fulfilled.

Back-up and recovery procedures for all relevant data shall be described in the B-CP Back-up and Recovery Plan and/or B-CP Back-up and Recovery Procedure.

5.8. COMPROMISE AND DISASTER RECOVERY

5.8.1. Incident and compromise handling procedures

The B-CIA, B-MSCA and B-CP shall define security incidents and compromise handling procedures in a Security Incident Handling Procedure manual, which shall be issued to administrators and auditors. All incidents within the B-CIA, B-MSCA and B-CP operations shall be reported to the B-MSA within 4 hours after the incident.

On detection of an incident, operations shall be suspended until the level of compromise has been established. In the event of possible compromise or theft of a B-MSCA private key and / or a master key, the B-MSCA or B-CP (as applicable) shall immediately inform the B-MSA. The B-MSA shall inform the ERCA and shall take appropriate measures within a reasonable time period.

Furthermore, the B-CIA, B-MSCA and B-CP shall assume that technological progress will render their IT-systems obsolete over time and shall define measures to manage obsolescence.

5.8.2. Computing resources, software, and/or data are corrupted

In their CPSs, the B-CIA, B-MSCA and B-CP outline the procedures for recovering a secure environment after computing resources, software and/or data get corrupted.

5.8.3. Entity private key compromise procedures

B-MSCA shall specify recovery procedures to be used if a B-MSCA private key is (suspected to be) compromised. These procedures shall describe how the affected private key is deactivated (such that it cannot be used) until the compromise has been confirmed or reasonably ruled out:

- If a compromise is confirmed or cannot be ruled out, the key shall be destroyed as described in section 6.2.10 of this policy, including all (backup) copies of it. The CPS shall also specify how a secure environment is re-established in this case, which card certificates are revoked (if any), how a new B-MSCA key pair is generated, and how a new B-MSCA certificate will be requested and be provided to the B-CP. The B-MSCA shall immediately inform the B-CIA, B-CP and the B-MSA. The B-CIA shall inform the relying parties.
- If a compromise can be ruled out, the key shall be activated again as described in section 6.2.8 of this policy..

If a card private key is (suspected to be) compromised, the B-CP shall immediately inform the B-CIA, B-MSCA and the B-MSA. The B-CIA shall inform the relevant relying parties. The B-CIA and B-CP shall collaborate to find out the cause of the compromise and take adequate measures to avoid a repeat.

5.8.4. Business continuity capabilities after a disaster

The following incidents are considered to be disasters:

- compromise or theft of a private key and / or a master key;
- non-availability of a private key and / or a master key;
- IT hardware failure.

The B-CIA, B-MSCA and B-CP draft and maintain a Business Continuity Plan, detailing how they will maintain their services in the event of a disaster. This plan shall describe their capabilities to ensure business continuity following a natural or other disaster.

The B-CIA, B-MSCA and B-CP shall ensure that in the event of a disaster, operations are restored within 48 hours. These recovery mechanisms used to restore operations shall not depend on the ERCA response times.

The B-CIA, B-MSCA and B-CP shall take adequate steps to limit the consequences of the disaster and, if possible, avoid repetition of the disaster.

Protection against IT hardware failures shall be provided by redundancy, i.e. availability of duplicate IT hardware, possibly located at multiple sites.

5.9. CIA, MSCA OR CP TRANSFER AND TERMINATION

5.9.1. CIA Transfer and Termination

In the event of termination of B-CIA activity by the currently appointed organization (section 1.8.3 of this policy), the B-MSA shall appoint a new organization responsible for the implementation of the applicable requirements in this policy. The current organization shall transfer its CIA-related assets to the new organization or to the B-MSA, while ensuring that confidentiality and integrity are maintained.

5.9.2. MSCA Transfer and Termination

In the event of termination of B-MSCA activity by the currently appointed organization (section 1.8.2 of this policy), the B-MSA shall notify the European Authority, the ERCA and B-CP.

B-MSA shall appoint a new organization responsible for the provision of key certification services to the B-CP and for the implementation of the applicable requirements in this policy.

B-MSA shall inform B-CP about the newly appointed B-MSCA organization and optionally the European Authority and the ERCA.

The current B-MSCA organization shall transfer its MSCA-related assets, including records required to provide evidence of certification for the purposes of legal proceedings, to the new organization or to the B-MSA, while ensuring that confidentiality and integrity are maintained.

In particular, before the B-MSCA terminates its services the following procedures shall be executed as a minimum:

- B-MSCA shall inform the B-MSA, B-CIA, the B-CP and the ERCA;

- B-MSCA shall terminate all authorization of subcontractors to act on behalf of the B-MSCA in the performance of any functions related to the process of issuing certificates;
- B-MSCA shall perform necessary undertakings to transfer obligations for maintaining event log archives for their respective period of time as indicated in the CPS;
- B-MSCA shall perform necessary undertakings to transfer certification status information of issued certificates to the B-CIA;
- B-MSCA shall destroy its private keys;
- B-MSCA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the B-MSCA becomes bankrupt or for other reasons is unable to cover the costs by itself;
- B-MSCA shall state in its practices the provisions made for termination of service. This shall include:
  - the notification of affected entities;
  - the transfer of its obligations to other parties;
  - the handling of the status information for certificates that have been issued.

5.9.3. CP Transfer and Termination

In the event of termination of B-CP activity by the currently appointed organization (section 1.8.4 of this policy), the B-MSA shall appoint a new organization responsible for the personalization of tachograph cards and for the implementation of the applicable requirements in this policy. The current organization shall transfer its CP-related assets to the new organization or to the B-MSA, while ensuring that confidentiality and integrity are maintained.

In their CPSs, the B-CIA, B-MSCA and B-CP shall identify the assets that shall be transferred to another organization in case of termination.

The party being terminated shall ensure that potential disruptions to subscribers and relying parties due to the termination are minimized.

5.10. CROSS CERTIFICATES

No cross certificates shall be used.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation and Master Key Import

6.1.1.1. By the MSCA

The B-MSCA shall generate B-MSCA key pairs for Production in accordance with Appendix 11 to Annex 1C of EU Regulation 799/2016 [3]. Generation of key pairs shall be undertaken in a HSM that complies with the requirements in section 6.2 of this policy. The HSM shall be located in a physically secured environment. B-MSCA key pair generation shall be performed in a manual or automatic process that is under (at least) dual person control, where all controlling persons have a trusted role. The B-MSCA shall use publicly specified and appropriate cryptographic algorithms for key pair generation. The B-MSCA shall document a secure operation procedure for generating key pairs.

The B-MSCA shall have the necessary key pairs and associated signing certificates to ensure continuity.

6.1.1.2. By the CP

The B-CP shall generate tachograph card key pairs for Production in accordance with Appendix 11 to Annex 1C of EU Regulation 799/2016 [3]. The B-CP shall also generate ephemeral key pairs for key agreement, as specified in the Smart Tachograph ERCA certificate policy. Generation of key pairs shall be undertaken in a physically secured environment in a manual or automatic process that is under (at least) dual person control, where all controlling persons have a trusted role. The B-CP shall use publicly specified and appropriate cryptographic algorithms for key pair generation.

Ephemeral key pairs for key agreement with the ERCA during master key distribution shall be generated in the HSM into which the key distribution message containing the encrypted master key will be imported.

The B-CP shall import a master key for Production as specified in chapter 4 of this policy. Master key import shall be undertaken in a physically secured environment by personnel in trusted roles under (at least) dual person control.

The B-CP shall document a secure operation procedure for generating tachograph card pairs, as well as for importing a master key (including the generation of an ephemeral key pair).

6.1.2. Private key and master key delivery to subscriber

6.1.2.1. By the MSCA

The B-MSCA shall not create key pairs for subscribers. Consequently, there is no need to distribute private keys to subscribers.

6.1.2.2. By the CP

The B-CP creates key pairs for subscribers. Private keys are delivered to subscribers stored in the secure memory of the tachograph card.

Tachograph card key pair generation may be done either on-board the card (with the public key being exported by the card), or outside the card (with the private key being inserted into the card). In the CPS, the B-CP shall indicate which of these two methods is used.

If card key pair generation is done on-board the card, the card shall comply with the requirements in section 6.2 of this policy. The card private key(s) shall never leave the card, throughout its lifetime.

If card key pair generation is not done on-board the card, it shall take place within an HSM that complies with the requirements in section 6.2 of this policy. Transport of the private key from the HSM into the secure memory of the smart card shall take place in a physically secured environment. Moreover, the confidentiality, authenticity and correctness of the private key shall be ensured at all times. Any relevant prescription related to key loading, mandated by the Common Criteria security certification of the tachograph card, shall be met during the personalization process. After finishing the personalization process of the card, the B-CP shall destroy any copies of the private key that exist outside the card.

For workshop cards and control cards, the B-CP also needs to transfer KM-WC and/or KDSRC from the HSM to the card’s secure memory. Insertion of a master key into a tachograph card shall take place in such a way that the confidentiality, authenticity and correctness of the key is ensured at all times. The process shall be in compliance with the relevant prescriptions mandated by the card’s Common Criteria security certification.

6.1.3. Public key delivery to certificate issuer

6.1.3.1. By the MSCA

The B-MSCA shall deliver the B-MSCA public keys to be certified to the ERCA using the procedure described in section 4.1 of the ERCA certificate policy.

6.1.3.2. By the CP

The B-CP shall deliver the card public keys to be certified to the B-MSCA using a key certification request.

6.1.4. Public key delivery to relying parties

6.1.4.1. ERCA Public Key Delivery

The B-MSCA and the B-CP shall download the ERCA root public key from the ERCA repository mentioned in the ERCA certificate policy. When the ERCA publishes a new ERCA root certificate, the B-MSCA and the B-CP shall download the new certificate along with the link certificate, and shall verify the link certificate with the previous ERCA root key.

The B-MSCA shall use the ERCA root public keys to validate the signature over any MSCA certificate it receives from the ERCA.

The B-CP shall insert the first-generation ERCA certificate containing the public key as a trust point in the Gen-1 application of each tachograph card. Moreover, the B-CP shall insert one, two or three Gen-2 ERCA certificates containing public keys as trust points in the Gen-2 application of each tachograph card, as specified in requirement CSM_91 in Appendix 11 to Annex 1C of EU Regulation 799/2016 [3].

Finally, if available, the B-CP shall personalize a link certificate in EF Link_Certificate on each card, as specified in requirement CSM_91 and in Appendix 2 to Annex 1C.

6.1.4.2. MSCA Public Key Delivery

B-MSCA shall provide the B-CP with the Gen-1 and Gen-2 MSCA certificates containing the public keys that can be used to verify the signature over each card certificate sent by the B-MSCA to the B-CP.

The B-CP shall include the Gen-1 MSCA certificate into the Gen-1 application of each card and the Gen-2 MSCA certificate into the Gen-2 application of each card.

6.1.4.3. Card Public Key Delivery

The B-CP shall include all card certificates containing the card public keys into the relevant application on each tachograph card, as specified in Appendix 2 of Appendix 11 to Annex 1C of EU Regulation 799/2016 [3].

6.1.5. Key sizes

B-MSCA and the B-CP shall choose the key sizes of the key pairs they generate in accordance with the requirements in Appendix 11 of Annex 1C of EU Regulation 799/2016 [3].

6.1.6. Public key parameters generation and quality checking

In their CPSs, the B-MSCA and the B-CP shall indicate whether they will use the Brainpool or NIST family of standardized domain parameters for their Gen-2 key pairs, in accordance with requirement CSM_48 in Annex 1C of EU Regulation 799/2016 [3].

To ensure sufficient quality (i.e. randomness) of the generated key, any random value required for key generation shall be generated by a random bit generator that is implemented within the certified HSM (or tachograph card) that generates the key.

6.1.7. Key usage purposes

The B-MSCA shall use the B-MSCA private keys only for digitally signing issued tachograph card certificates, as detailed in chapter 3 of this policy.

The B-CP shall not use the tachograph card private keys it generates for any purpose, except inserting them into tachograph cards (if they are not generated inside the card). A tachograph card shall use its private key(s) for mutual authentication towards VUs and (possibly) digitally signing downloaded data, as specified in Appendix 11 to Annex 1C of EU Regulation 799/2016 [3].

6.2. PRIVATE KEY AND SYMMETRIC KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

To protect the confidentiality, integrity and availability of private keys, the B-MSCA and the B-CP shall generate and use any private keys exclusively in a Hardware Security Module (HSM) or tachograph card. Similarly, the B-CP shall request, import and store any master key exclusively in a HSM or smart card. For both purposes, the HSM shall

- be certified to EAL 4 or higher in accordance with ISO/IEC 15408 [10] using a suitable Protection Profile; or
- meet the requirements in ISO/IEC 19790 level 3 [13]; or
- meet the requirements in FIPS PUB 140-2 level 3 [14]; or
- offer an equivalent level of security according to equivalent nationally or internationally recognized evaluation criteria for IT security.

In case card key pair generation is done on-board the card, key generation shall be covered by the Common Criteria security certification of the card. The card shall use publicly specified and appropriate cryptographic algorithms for key pair generation.

Private key operations and symmetric key operations shall take exclusively place internally in the HSM or smart card where the keys used are stored.

The above requirements apply only to keys used for Production. Keys used for Interoperability Testing may be generated and used outside a HSM.

6.2.2. Private key and master key multi-person control

6.2.2.1. By the MSCA

The B-MSCA shall make sure that B-MSCA private keys for Production are used only in a manual or automatic process that is under (at least) dual person control, where all controlling persons have a trusted role. This requirement does not apply for private keys used for Interoperability Testing.

In its CPS, B-MSCA shall specify the number and trusted role of persons needed to carry out the following operations on B-MSCA private keys in an HSM:

- generation;
- activation for use (see section 6.2.8 of this policy);
- export for backup purposes;
- import (recovery) from a backup;
- destruction.

Each of these operations shall only be possible if the number of trusted persons specified in the CPS for the specific task have authenticated themselves towards the HSM, using the activation data described in section 6.4 of this policy.

6.2.2.2. By the CP

If tachograph card private keys are generated on-board the card (see section 6.1.1.2 of this policy) then private key management is not necessary, as it never leaves the card.

If tachograph card private keys for Production are generated in an HSM, then the B-CP shall make sure that they are used only in a manual or automatic process that is under (at least) dual person control, where all controlling persons have a trusted role. This requirement does not apply for private keys used for Interoperability Testing.

In its CPS, the B-CP shall specify the number and trusted role of persons needed to carry out the following operations on tachograph card private keys in an HSM:

- generation;
- export for inserting into tachograph cards;
- destruction.

Moreover, the CPS shall specify the number and trusted role of B-CP employees needed to carry out the following operations on a master key in an HSM:

- import;
- export for insertion into workshop cards;
- export for backup purposes;
- import (recovery) from a backup;
- destruction.

Each of these operations shall only be possible if the number of trusted persons specified in the CPS for the specific task have authenticated themselves towards the HSM, using the activation data described in section 6.4 of this policy.

6.2.3. Private key and master key escrow

Key escrow of B-MSCA private keys is expressly forbidden: such keys shall not be exported to or stored in any system apart from the B-MSCA systems.

Key escrow of card private keys is expressly forbidden: after personalization is finished, such keys shall not be stored in any system apart from the tachograph card itself.

Key escrow of a master key is expressly forbidden: master keys shall not be exported to or stored in any system apart from the B-CP systems and in tachograph workshop cards and control cards.

6.2.4. Private key and master key backup

In its CPSs, the B-MSCA and the B-CP shall describe backup and restore procedures for the B-MSCA private keys and the master keys, respectively. These secure operating procedures shall be appropriate to minimise the chance of loss of these keys. Key backups shall be regularly verified to make sure that keys can still be restored from them.

Any copies of the B-MSCA private keys and the master keys shall be subject to the same level of security controls as the keys in use.

Tachograph card private keys shall not be backed up.

6.2.5. Private key and master key archival

No stipulation.

6.2.6. Private key and master key transfer into or from a cryptographic module

B-MSCA private key import and export into or from an HSM shall only take place for back-up and recovery purposes. B-MSCA private keys shall be exported only in encrypted form, preferably using the default backup and restore mechanisms of the HSM.

Tachograph card private key import is forbidden. Tachograph card private key export shall only take place for insertion into tachograph cards, if necessary (section 6.1.2.2 of this policy).

Master key import shall only take place during the initial import of the Key Distribution Message received from the ERCA (section 4.1 of this policy), and for recovery purposes from a backup. Master key export shall only take place for backup purposes.

6.2.7. Private key and master key storage on cryptographic module

Keys shall be stored in the HSM in encrypted form.

6.2.8. Method of activating private key and master key

For activation of private key or a master keys stored inside a HSM for use, the B-MSCA and the B-CP should use two-factor authentication mechanisms (e.g. a smart card or other token combined with a PIN) to authenticate the HSM operators towards the HSM.

6.2.9. Method of deactivating private key and master key

The duration of an authentication session shall not be unlimited. At regular intervals, to be specified in the CPS, re-authentication of the HSM operator(s) shall be necessary. If re-authentication does not take place in time, the keys inside the HSM shall be automatically deactivated for use.

6.2.10. Method of destroying private key and master key

At the end of the two-year private key usage period of a B-MSCA private key (as specified in Appendix 11 of Annex 1C of EU Regulation 799/2016 [3], the B-MSCA shall destroy all copies of the key, such that it cannot be retrieved.

At the end of the life cycle of a master key (as specified in Appendix 11 of Annex 1C), the B-CP shall destroy all copies of the key in its possession, such that it cannot be retrieved.

When an HSM containing a B-MSCA private key or a master key is replaced, the keys stored in it shall be destroyed before the HSM leaves the secure environment.

Destruction of private keys or a master key stored in an HSM shall be done by using the function of the HSM for key destroying. Destruction of back-up keys shall be done by physical destruction of the data carriers on which the backups are stored.

6.2.11. Cryptographic Module Rating

Refer to section 6.2.1 of this policy.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

B-MSCA public key certificates and hence the public keys shall be archived indefinitely, as discussed in section 5.5 of this policy.

All B-MSCA certificates and tachograph card certificates shall have the validity period specified for them in Appendix 11 to Annex 1C of EU Regulation 799/2016 [3].

As specified in Appendix 11, the B-MSCA shall use a B-MSCA private key for maximum two years, starting from the effective date in the corresponding certificate.

The private usage period of a tachograph card private key shall be the same as the validity period of the corresponding certificate.

6.4. ACTIVATION DATA

B-MSCA and the B-CP shall describe in their CPSs all credentials, such as passwords, PINs, authentication smart cards or other tokens, that are necessary to bring the HSM(s) containing the B-MSCA private key(s) or the master keys and the HSM(s) used to generate card key pairs (as appropriate) in an operational state or to activate a private key or master key for use.

B-MSCA and the B-CP shall document requirements regarding the length and complexity of these credentials, as well as regarding the trusted role responsible for generating them and the circumstances and frequency under which they shall be changed. The B-MSCA and the B-CP shall document the secure operating procedures to be followed to set each of the credentials to their initial value and to change them.

A credential shall be changed periodically, and at least whenever a person that is in possession of or has knowledge of that credential leaves their function or is assigned another trusted role.

B-MSCA and the B-CP shall describe the measures taken to protect the availability, confidentiality and integrity of all activation data.

6.5. COMPUTER SECURITY CONTROLS

Computer security controls shall be implemented to ensure secure operations. The B-CIA, B-MSCA and B-CP shall describe the specific technical security measures taken to harden their systems. A proven system security checklist appropriate for the relevant operating system shall be applied.

6.6. LIFE CYCLE SECURITY CONTROLS

6.6.1. System development controls

The B-CIA, B-MSCA and B-CP shall describe the practices and controls used during the development or sourcing of their systems. A risk analysis shall be carried out during the design and requirements specification of any systems development project undertaken by these parties or on behalf of these parties, to ensure that an adequate level of security is built into the developed systems.

The functionality and security of hardware and software shall be tested properly before being taken into production.

6.6.2. Security management controls

Security management controls shall include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures shall include checking the integrity of the security software, firmware, and hardware to ensure their correct operation. In their CPSs, the B-CIA, B-MSCA and B-CP shall specify the tools and procedures used for integrity checking, as well as the scope and frequency of such checks.

6.6.3. Life cycle security controls

The B-CIA, B-MSCA and B-CP shall describe their CPSs regarding updates of hardware, operating systems and software. Change control procedures shall exist for modifications and releases for any operational software. A separation between Acceptance (or Pre-Production) and Production systems shall be maintained. Change procedures and security management procedures shall guarantee that the required security level is maintained in the Production system.

Change control procedures shall be documented and used for releases, modifications and (emergency) software fixes for any operational software.

6.7. NETWORK SECURITY CONTROLS

The B-CIA, B-MSCA and B-CP shall document their network architecture, including the use of firewalls and IDS/IPS, if any.

The B-MSCA and the B-CP shall segregate and implement their network architecture in such a way that access from the internet to their internal network domain, and from the internal network domain to the systems used to generate, manage and store cryptographic keys (including the HSMs), can be effectively controlled.

6.8. TIMESTAMPING

The time and date of an event shall be included in every audit trail entry. In their CPSs, the B-CIA, B-MSCA and B-CP shall describe how time is synchronized and verified.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

All certificates shall have the profile specified in Annex 1C, Appendix 11 and Appendix 1 of the Commission Implementing Regulation (EU) 799/2016 [3], amended by the European Commission in 2018:

Data Object	Req	Field ID	Tag	Length (bytes)	ASN.1 data type
ECC (CV) Certificate	m	C	‘7F 21’	var	
Certificate Body	m	B	‘7F 4E’	var	
Certificate Profile Identifier	m	CPI	‘5F 29’	‘01’	INTEGER (0…255)
Certification Authority Reference	m	CAR	‘42’	‘08’	KeyIdentifier
Certificate Holder Authorisation	m	CHA	‘5F 4C’	‘07’	Certificate Holder Authorisation
Public Key	m	PK	‘7F 49’	var	
Standardised Domain Parameters OID	m	DP	‘06’	var	OBJECT IDENTIFIER
Public Point	m	PP	‘86’	var	OCTET STRING
Certificate Holder Reference	m	CHR	‘5F 20’	‘08’	KeyIdentifier
Certificate Effective Date	m	CEfD	‘5F 25’	‘04’	TimeReal
Certificate Expiration Date	m	CExD	‘5F 24’	‘04’	TimeReal
ECC Certificate Signature	m	S	‘5F 37’	var	OCTET STRING

Table 5 Certificate profile

The algorithm is indicated via the Standardized Domain Parameters OID as specified in Table 1 of Appendix 11, Annex 1C of the Commission Implementing Regulation (EU) 799/2016 [3], amended by the European Commission in 2018. The options are:

Name	Object Identifier reference	Object identifier value
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
Brainpool P384r1	brainpoolP384r1	1.3.36.3.3.2.8.1.1.11
Brainpool P512r1	brainpoolP512r1	1.3.36.3.3.2.8.1.1.13
NIST P-521	Secp521r1	1.3.132.0.35

Table 6 Allowed Standardized Domain Parameters OIDs

7.2. CRL PROFILE

Revocation of equipment and card certificates issued by B-MSCA is not allowed.

No CRL shall be published.

B-MSCA certificates (issued by ERCA) status can be found on ERCA website https://dtc.jrc.ec.europa.eu.

7.3. OCSP PROFILE

No OCSP shall be used.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The first full and formal audit on the B-CIA, B-MSCA and B-CP operation shall be performed within 12 months of the start of the operations covered by the B-MSA certificate policy. The B-MSA may also order a compliance audit by an auditor at any time at its discretion.

The B-CIA, B-MSCA, B-CP audits shall establish whether the requirements on the B-MSA described in this document are being maintained.

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 the B-MSA certificate policy, the B-MSA shall carry out a pre-operational assessment to obtain evidence that the B-CIA, B-MSCA and B-CP organizations is able to operate in conformance to the requirements in the B-MSA certificate policy.

As a minimum, the following shall be assessed:

- that the facilities housing the operations covered by this policy comply with the requirements in section 5.1 of this policy;
- that all systems (hardware and software) are in place and are functioning according to specification;
- that all systems (hardware and software) comply with the requirements in “Chapter 6 Technical Security Controls” of this policy, such that the required level of physical and logical protection of cryptographic keys and other confidential information is ensured;
- that all necessary trusted roles have been assigned in accordance with section 5.3 of this policy.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The audit shall be performed by an independent auditor.

Any person selected or proposed to perform the B-CIA, B-MSCA and B-CP compliance audit shall first be approved by the B-MSA.

The names of the auditors which will perform the audits shall be registered. Such auditors shall comply with the following requirements:

- ***Ethical behavior***: trustworthiness, uniformity, confidentiality regarding their relationship to the organization to be audited and when handling its information and data;
- ***Fair presentation***: findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit;

- ***Professional approach***: has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in information technologies, PKI and the related technical norms and standards.

The auditor shall possess significant knowledge of, and preferably be accredited for:

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

B-CIA, B-MSCA and B-CP audits shall cover compliance to the current B-MSA certificate policy, their respective CPSs, the B-CIA CPS, B-MSCA CPS and B-CP CPS and associated procedures and techniques 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 ("Chapter 3 Identification and Authentication");
- operational functions/services ("Chapter 4 Life-Cycle Operational Requirements for Certificates and Master Keys");
- physical, procedural and personnel security controls ("Chapter 5 Facility, management and Operational Controls");
- key management ("Chapter 4 Life-Cycle Operational Requirements for Certificates and Master Keys" and "Chapter 6 Technical Security Controls");
- technical security controls ("Chapter 6 Technical Security Controls").

During the audit, the auditor shall assess the audit logs (section 5.4 of this policy) to determine whether weaknesses are present in the security of the systems of the organization to be audited.

Possible weaknesses determined as a result of the audit shall be mitigated. The assessment results and possible weaknesses determined 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 organization (B-CIA, B-MSCA, B-CP) that was audited. After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.6. COMMUNICATION OF RESULTS

For the B-CIA, B-MSCA and B-CP audits, the independent auditor shall report the full results of the compliance audit to the organization that was audited and to B-MSA in English language.

The B-MSA shall send a summary of the audit report covering the relevant results of the audit to ERCA in English language.

This summary of the audit report shall include at least the number of deviations found and the nature of each deviation.

If requested by ERCA, the B-MSA shall send the full results of the compliance audit to ERCA.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

The B-CIA, B-MSCA and B-CP shall have adequate arrangements to cover liabilities arising from their operations and/or activities.

No other stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

Confidential data shall comprehend at least:

- Private keys;
- Symmetric master keys;
- Audit logs;
- Detailed documentation regarding the PKI management;

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

Certificates are not considered to be confidential.

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

9.4. PRIVACY OF PERSONAL INFORMATION

The B-CIA, B-MSCA and B-CP shall treat all personal information, especially information provided by Card Holders in the course of their application for a tachograph card, according to the General Data Protection Regulation 679/2016 [22]. Appropriate technical and organizational measures shall be taken to prevent unauthorized or unlawful processing of personal data and to prevent accidental loss or destruction of, or damage to, personal data.

Personally identifiable information, contact information, and authorizations of B-CIA, B-MSCA and B-CP staff are private.

Personally identifiable or corporate information and contact information of Card Holders that does not appear in a certificate issued by the B-MSCA, is private.

9.5. INTELLECTUAL PROPERTY RIGHTS

No stipulation.

9.6. REPRESENTATIONS AND WARRANTIES

The B-CIA organization guarantees that the B-CIA shall operate according to ERCA certificate policy, B-MSA certificate policy and the B-CIA CPS.

The B-MSCA organization guarantees that the B-MSCA shall operate according to ERCA certificate policy, B-MSA certificate policy and the B-MSCA CPS.

The B-CP organization guarantees that the B-CP shall operate according to ERCA certificate policy, B-MSA certificate policy and the B-CP CPS.

9.7. DISCLAIMERS AND WARRANTIES

B-MSCA 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 authorized source), and further disclaim any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

9.8. OBLIGATIONS

This section contains provisions relating to the respective obligations of:

- B-MSA;
- B-CIA;
- B-MSCA;
- B-CP;
- Cardholders.

9.8.1. B-MSA Obligations

With regard to this certificate policy, the B-MSA has the following obligations:

a) Maintain the certificate policy;

b) Submit this certificate policy to ERCA for approval;

c) Appoint the B-CIA, B-MSCA and a B-CP;

d) Audit the appointed B-CIA, B-MSCA and B-CP;

e) Approve the B-CIA, B-MSCA and B-CP Practice Statements;

f) Publish the B-MSA policy;

9.8.2. B-CIA Obligations

With regard to this certificate policy, the appointed B-CIA has the following obligations:

a) Follow this B-MSA certificate policy;

b) Publish the B-CIA Practice Statement (B-CIA CPS) that includes a reference to this certificate policy, to be approved by the B-MSA;

c) Ensure that correct and relevant user information from the application process is passed to the component personalizers (CPs);

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

For more comprehensive description of B-CIA responsibilities see section 1.7.3 of this policy.

9.8.3. B-MSCA Obligations

With regard to this certificate policy, the appointed B-MSCA has the following obligations:

a) Follow this B-MSA certificate policy;

b) Publish the B-MSCA Practice Statement (B-MSCA CPS) that includes a reference to this certificate policy, to be approved by the B-MSA;

c) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this certificate policy;

d) Oversee that ERCA Root Certificate Policy requirements will be implemented in B-MSCA systems;

e) Maintain confidentiality of the B-MSCA private keys and symmetric master leys;

f) establish an information security management system (ISMS), based on a risk assessment for all the operations involved. The ISMS shall cover all processes related to the issuing of tachograph cards and the management of personal data on these cards. The implementation of the ISMS shall be certified according to ISO 27001 [19].

For more comprehensive description of B-MSCA responsibilities see section 1.7.2.3 of this policy.

9.8.4. B-CP Obligations

With regard to this certificate policy, the appointed component personalizer has the following obligations:

a) Follow this B-MSA certificate policy;

b) Publish the CP Practice Statement (CP CPS) that includes a reference to this certificate policy, to be approved by the B-MSA;

c) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this certificate policy;

d) Maintain confidentiality of the cardholder private keys and symmetric master leys;

e) establish an information security management system (ISMS), based on a risk assessment for all the operations involved. The ISMS shall cover all processes related to the issuing of tachograph cards and the management of personal data on these cards. The implementation of the ISMS shall be certified according to ISO 27001 [19].

For more comprehensive description of B-CP responsibilities see section 1.7.4 of this policy.

9.8.5. Cardholder Obligations

With regard to this certificate policy, the cardholders have the following obligations:

All cards:

a) accurate and complete information is submitted to the B-CIA in accordance with the requirements of this policy;
b) the keys and certificate are only used in the Smart Tachograph system;
c) the card is only used in the Smart Tachograph system;
d) reasonable care is exercised to avoid unauthorized use of the equipment private key and card;
e) a user shall not use a damaged or expired card;
f) a user shall not tamper with or attempt to modify cards in any way;
g) the user shall notify the B-CIA without any reasonable delay if any of the following occurs up to the end of the validity period indicated in the certificate:
    - the equipment private key or card has been lost, stolen or potentially compromised;
    - the certificate content is, or becomes, inaccurate.

Driver card:

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

Workshop card:

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

For more comprehensive description of card holder responsibilities see section 1.7.5 of this policy.

9.9. LIMITATIONS OF LIABILITY

No stipulation.

9.10. INDEMNITIES

No stipulation.

9.11. TERM AND TERMINATION

B-MSA Certificate Policy is valid from the moment it is approved by ERCA and it shall be valid until further notice.

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

9.12. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.13. AMENDMENTS

This Certificate Policy is issued under responsibility of the B-MSA. The B-MSA, in cooperation with ERCA, may revise this Certificate Policy if it deems this necessary. It is allowed to make editorial or typographical corrections to this policy without notification without an increase in version number.

For all other changes of this Certificate Policy, the procedure for change proposals and approvals shall be as follows:

1. B-MSA (and ERCA) may submit proposals for change to the B-MSA certificate policy to ERCA at any time.
2. ERCA shall set an appropriate period for comments. The B-MSA and ERCA may comment on the proposed changes within the defined period for comments.
3. B-MSA shall consider the comments and shall decide which, if any, of the notified changes to implement.
4. ERCA shall notify the B-MSA about its decision, and shall set an appropriate period for the changes to be implemented.
5. B-MSA shall publish a new version of the B-MSA certificate policy including all implemented changes, accompanied by an increase in the version number of the document.

9.13.1. Changes without notification

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

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

9.13.2. Changes with notification

9.13.2.1. Notice

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

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

9.13.2.2. Comment period

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

9.13.2.3. Notified entities

Information about changes to this policy shall be sent to:

- ERCA;
- B-CIA;
- B-MSCA;
- B-CP.

9.13.2.4. Period for Final Change Notice

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

9.13.3. Changes Requiring a New MSA Policy Approval

If a policy change is determined by the B-MSA organization to have a material impact on a significant number of entities affected by this policy, the B-MSA shall submit the revised B-MSA policy to ERCA for approval.

9.14. DISPUTE RESOLUTION PROCEDURES

The B-CIA, B-MSCA and B-CP shall have policies and procedures for the resolution of complaints and disputes received from Card Holders or other parties about the provisioning of their services as described in this MSA certificate policy.

Any dispute related to key and certificate management between the B-MSA, B-MSCA, service agencies and equipment manufacturers 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 B-MSA.

9.15. GOVERNING LAW

European regulations shall govern the enforceability, construction, interpretation, and validity of this B-MSA Certificate Policy.

9.16. COMPLIANCE WITH APPLICABLE LAW

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 [2] of the European Parliament and of the Council and with Commission Implementing Regulation (EU) 799/2016 [3], amended Commission Implementing Regulation (EU) 502/2018. In case discrepancies exist between this document and the Regulation or Implementing Regulation, the latter shall prevail.

9.17. MISCELLANEOUS PROVISIONS

No stipulation.

9.18. OTHER PROVISIONS

No stipulation.

10. REFERENCES

1. Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy, version 1.0, June 2018 [1]
2. Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014, Official Journal of the European Union L60 [2]
3. Commission Implementing Regulation (EU) 799/2016, amended by the European Commission in 2018, Official Journal of the European Union L 139 [3]
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 [4]
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997 [5]
6. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0, Month year [6]
7. Smart Tachograph - Equipment Interoperability Test Specification, JRC, version 1.0, Month year [7]
8. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28 [8]
9. ISO/IEC 18033-2, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, first edition, 2006-05-01 [9]
10. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 – 2014 [10]
11. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15 [11]
12. CEN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services [12]
13. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15 [13]
14. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001 [14]
15. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013 [15]
16. ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01 [16]
17. ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an n-bit block cipher. Third edition, 2006-02-01 [17]

18. National Institute of Standards and Technology (NIST), Special Publication 800- 38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005 [18]
19. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01 [19]
20. Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission, Adopted 29/05/2009 [20]
21. Commission Decision 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission [21]
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [22]