Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

The Netherlands' Member State Authority (MSA) Certificate Policy

for the Digital Tachograph and Smart Tachograph systems

Date	January, 2024
Version	1.1
Status	Final

Colophon	ILT Afdeling ICT, team CIO office Den Haag

Contact persons	F.G. van Wijnen Operational TSP manager Ferry.van.Wijnen@ILenT.nl
	J. van Ginderen Operational TSP manager Joep.van.ginderen@ilent.nl
Version	
Principal	
Author	David Bakker - UL

Contents

1 INTRODUCTION

1.1 Overview

1.1.1 Document background: The Smart Tachograph PKI system

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 (among others) heavy goods 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 of the European Parliament and of the Council, [1].

Like the Digital Tachograph system, the Smart Tachograph system 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 (MSCA) to create a consistent and secure system. The role of the ERCA is to securely certify the public keys of the MSCAs to establish a trusted certification chain. Next to that, the ERCA also distributes a number of symmetric master keys to the MSCAs.

At the MSCA 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 personalisers that are responsible for issuing this equipment.

At the equipment level, equipment personalisers are responsible for creating equipment key pairs and inserting equipment keys and certificates securely into their equipment. For some types of equipment, personalisers also insert symmetric keys into the equipment. Personalisers 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[1]. This means that for the foreseeable future, tachograph cards will contain two applications, as specified in Appendix 2 to Annex 1C [2].

For more details, the reader is referred to the Implementing Regulation (EU) 2016/799, [2], and especially to Appendix 11 of Annex 1C thereof. Note that this Regulation has been amended by Commission Implementing Regulation (EU) 2018/502, [3]. Every reference to [2] in this MSA certificate policy is supposed to include these amendments.

1.1.2 Document scope

1.1.2.1 DUTCH SMART TACHOGRAPH CARDS ONLY

This document is the certificate policy (CP) of the Dutch Member State Authority (MSA) for both the Digital Tachograph and Smart Tachograph PKI. It complies with

[1] Until the moment the EC formally decides to request workshops to switch off support for first-generation cards in VUs.

all requirements for MSA certificate policies in the ERCA certificate policy, [5], and lays down the policy at the Dutch national level for the key generation, key management and certificate signing for the Dutch Smart Tachograph cards. The scope of this document includes only the MSCA level and the equipment personaliser level in The Netherlands.

Currently no VU, Motion Sensor or EGF manufacturers are present in The Netherlands. Therefore, this Certificate Policy only describes key and certificate management for Tachograph Cards and requirements regarding Vehicle Unit and Motion Sensor manufacturers are currently not covered by this policy. This policy must be adapted if VUs, Motion Sensors or EGFs were to be produced in The Netherlands in the future.

1.1.2.2 Both first and second-generation keys and certificates

This Smart Tachograph MSA certificate policy applies both to the first-generation (TDES and RSA) and the second-generation (AES and ECC) keys and certificates. This is because for the foreseeable future Smart Tachograph cards will contain both types of keys and certificates. The systems and processes used for the issuance of Dutch tachograph cards shall therefore be capable of securely handling both types of keys and certificates.

It is not desirable having two different certificate policies that are applicable for the same systems. Therefore, the existing The Netherlands MSA Policy [10] shall be terminated at the moment that this document becomes valid.

1.1.2.3 keys and certificates for Production and Interoperability Testing

Next to the production keys and certificates, the Dutch MSCA also issues Interoperability Testing certificates to the Card Personaliser (CP), to be used for interoperability testing purposes as documented in [9]. The MSCA also assists in the distribution of the Interoperability Testing master keys ($K_{M\text{-}WC}$ and K_{DSRC}) from the ERCA to the Card Personaliser. The CP inserts these keys and certificates into the tachograph cards that the CP must send to the Digital Tachograph Laboratory (run by the JRC) for interoperability testing purposes. These activities are in scope of this document as well.

1.1.3 Document audience

This document is intended for

- Management and employees of the Dutch MSA who are accountable and/or responsible for the contents of this Policy,
- Management and employees of the Dutch MSCA, Card Issuing Authority (CIA), Card Personaliser (CP) and Card Distributor (CD), who are accountable and/or responsible for the systems and operations described in this document,
- Auditors responsible for auditing the systems and operations of the Dutch MSCA, Card Issuing Authority, Card Personaliser and Card Distributor,
- Employees of the ERCA responsible for approving this document,
- Any other stakeholders in the Dutch Digital Tachograph and Smart Tachograph ecosystems, including the general public.

Readers of this document are supposed to be familiar with the contents of references [1] - [5].

1.1.4 Document structure

This document follows the framework for CPS described in RFC 3647, [7]. Please note that RFC 3647 deals only with certificates, whereas the security of the Smart

Tachograph system also depends on the security of a number of master keys. To clearly distinguish the requirements for both the certificate lifecycle and the master key lifecycle, this document contains a separate paragraph for each. Paragraph 4.1 describes the lifecycle operational requirements for certificates and paragraph 4.2 describes the same for master keys. Both of these paragraphs have the same outline and follow the requirements in section 4.4 (Certificate Life-Cycle Operational Requirements) of RFC 3647.

1.1.5 Key words

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, [8].

1.2 Document name and identification

This document is named "The Netherlands' Member State Authority (MSA) Certificate Policy for the Digital Tachograph and Smart Tachograph systems". This certificate policy does not have an ASN.1 object identifier. Such an identifier is not needed, as the Smart Tachograph card certificates do not contain a reference to this (or any other) policy.

The current version of this document is 1.0.

This Dutch MSA certificate policy was approved by the ERCA (see section 1.5.1) on DATE.

1.3 PKI participants

1.3.1 Overview

The participants in the Smart Tachograph PKI, as well as the data flows between them, are represented in Figure 1 in the Smart Tachograph ERCA Certificate Policy, [5]. For the Digital Tachograph PKI, the participants are the same, but there are small differences in the data flows.

In the case of The Netherlands, the Component Personaliser level can be represented in more detail as shown in Figure 1.

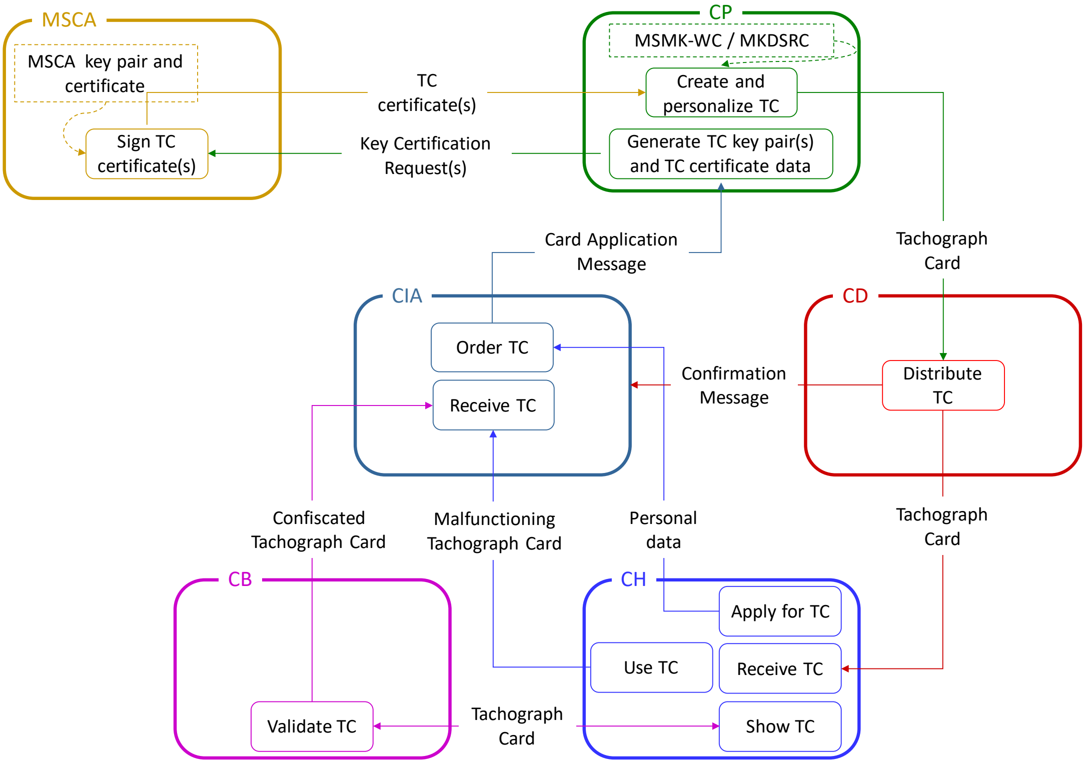

Figure 1 Roles and interactions in the Dutch Smart Tachograph system

Figure 1 shows the following roles:

- the Member State Certification Authority (MSCA) – discussed in section 1.3.2.
- the Card Personaliser (CP) – a PKI participant discussed in section 1.3.6.2.
- the Card Issuing Authority (CIA) – a PKI participant discussed in section 1.3.6.1.

- the Card Distributor (CD) – a PKI participant discussed in section 1.3.6.3.
- the Card Holder (CH) –the subscriber to the MSCA's services, discussed in section 1.3.4.
- the Control Body (CB) – both a PKI participant and a party relying on the MSCA's services, discussed in sections 1.3.5 and 1.3.6.4.

Notes:

- The interaction of the MSCA with the ERCA in order to obtain the MSCA certificate(s) (see section 1.3.2) is not shown in the figure.
- Similarly, the figure does not show the interaction of the CP with the ERCA (via the MSCA) to obtain the K_{M-WC} or K_{DSRC}; see section 1.3.6.2.

1.3.2 Certification authorities

The Certification Authorities participating in the Smart Tachograph and Digital Tachograph PKI systems are the ERCA, foreign MSCAs and the Dutch MSCA. These are discussed in the next subsections.

1.3.2.1 ERCA

This document assumes that the ERCA complies with all applicable requirements in the Smart Tachograph ERCA certificate policy, [5], and the Digital Tachograph ERCA certificate policy, [4].

1.3.2.2 Foreign MSCAs

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

1.3.2.3 Dutch MSCA

The Dutch MSCA is appointed by the Card Issuing Authority and can be contacted at the address specified in the CPS.[2] The MSCA shall operate in conformance with all applicable requirements in

- this MSA certificate policy,
- the ERCA certificate policy for the Digital Tachograph [4],
- the ERCA certificate policy for the Smart Tachograph [5],
- the Regulation 2016_799 [2], in particular Annex 1C.

In particular, the responsibilities of the Dutch MSCA are:

- to have available a MSCA system for Production as well as an MSCA system for Interoperability Testing purposes, according to the Regulation 2016_799 [2]:
    - The Production MSCA system shall have sufficient capacity to fulfil the KPIs set in the contract with the CIA. The MSCA shall monitor capacity demands and make projections of future capacity requirements to ensure that adequate processing power and storage are available at all times.
    - The Interoperability Test MSCA system shall be a (logically) separate system. It shall use the Interoperability Testing root keys and master keys made available by the ERCA, as specified in the Smart Tachograph Equipment Interoperability Test Specification, [9], and shall have its own MSCA private keys.
    - Adequate measures shall be taken to ensure that keys and certificates for Interoperability Testing are not generated, used or

[2] The Certification Practices Statement (CPS) is drafted by the Card Issuing Authority, see section 1.3.6.1. It contains information regarding all participants in the Dutch tachograph PKI.

stored in the Production system, and keys and certificates for Production are not generated, used or stored in the Interoperability Test system.

- 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, [2], and in chapter 7 of this policy.
- to create Key Certification Requests for these RSA keys conform the Digital Tachograph ERCA certificate policy [4], and send those, via the CIA, 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, [2], and in chapter 7 of this policy.
- to create Certificate Signing Requests for these ECC keys conform the Smart Tachograph ERCA certificate policy [5], and send those, via the CIA, to the ERCA to obtain the corresponding MSCA_Card certificates.
- to let the CIA and the CP know the Certificate Holder Reference of the first-generation and second-generation MSCA certificate(s) that are available for certificate signing at any given moment.
- to issue certificates for first-generation tachograph card public keys and second-generation tachograph card public keys upon request of the Card Personaliser, but only after approval from the Card Issuing Authority, as specified in chapter 4 of this policy.
- to send the Gen-1 and Gen-2 MSCA certificates to the Card Personaliser.
- to keep traceable records of all of issued card certificates.
- to revoke card certificates upon request from the CIA or the MSA.
- to keep traceable records of all revocations.
- to maintain a list of revoked certificates, in such a way that the status of each certificate can be verified by other Dutch Smart Tachograph PKI participants, as discussed in section 4.9.
- to receive a Key Distribution Request conform the ERCA certificate policy [5] from the Card Personaliser, as specified in the Interface Requirement Specification [13], 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 Card Personaliser, as specified in [13].

Moreover, the MSCA shall:

- upon request of the CIA, deliver input for writing the Certification Practices Statement; see section 1.3.6.1. The input shall explain how the MSCA complies with all applicable requirements in this MSA certificate policy.
- upon request of the CIA, review the CPS to make sure it still accurately describes the actual systems and processes of the MSCA, and notify the CIA 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 [14].
- be certified according to ISO 9001.
- maintain adequate organisational and financial resources to operate in conformity with the requirements laid down in this MSA certificate policy.

1.3.3 Registration authorities

The Dutch MSCA comprises only a certification authority. Functionality associated with a registration authority is performed by the Card Issuing Authority. This document does not contain any specific requirements for the registration authority. In the Certification Practices Statement (CPS), the CIA and MSCA shall explain how the Registration Authority and Certificate Authority are managed.

1.3.4 Subscribers (Card Holders)

The subscribers to the 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 CIA.
- when expiry of their tachograph card is imminent, timely requesting a renewal at the CIA.
- providing accurate and complete information to the 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, [2].
- exercising reasonable care to avoid unauthorised use of the card.
- notifying the CIA without delay and requesting a replacement card if:
    - the card is lost, stolen, or malfunctioning.
    - the personalisation 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 personalised or whose PIN is compromised or forgotten to the 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[3].
- Card Holders of a company card may request and possess multiple valid company cards.

1.3.5 Relying parties (Control Bodies)

Parties relying on the public key certification services of the 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.

Control bodies are responsible for:

- verifying the authenticity and temporal validity of any tachograph card certificate, as specified in Appendix 11 to Annex 1C, [2].
- verifying the authenticity and integrity of usage data downloaded from an authentic tachograph card, by verifying the signature created by the card.
- accepting authentic usage data and the information in authentic card certificates in enforcement processes and in legal procedures.

[3] Note that the relevant workshop is mentioned on each workshop card.

- using data downloaded from tachograph cards in accordance with all applicable requirements in this MSA certificate policy, the ERCA certificate policies [4] and [5], and Annex 1C [2].
- taking any other precautions as prescribed in agreements, this policy or elsewhere.

1.3.6 Other participants

1.3.6.1 Card Issuing Authority

The Card Issuing Authority (CIA) is appointed by the MSA and can be contacted at the address specified in the CPS. The Card Issuing Authority shall operate in conformance with all applicable requirements in

- this MSA certificate policy,
- the ERCA certificate policy for the Digital Tachograph [4],
- the ERCA certificate policy for the Smart Tachograph [5],
- the Regulation 2016_799 [2], in particular Annex 1C.

The Card Issuing Authority is responsible for

- issuing a (Production) tachograph card on request of a Card Holder, including:
  - registering the Card Holder and their tachograph card personalisation data, in accordance with applicable data protection rules and regulations.
  - requesting the issuance and personalisation of a tachograph card for the Card Holder from the Card Personaliser, by sending a Card Application Message as specified in the Interface Requirement Specification [12].
  - requesting the distribution of personalized tachograph cards by the Card Distributor.
- providing correct and complete personalisation data (including card certificate(s) data) to the CP for each tachograph card to be issued.
- performing tachograph card (certificate) life cycle management, including
  - monitoring and analyzing
    - all cards that are malfunctioning, as reported by the Card Holder.
    - the repeated reporting of loss or stolen cards by Card Holders or transport companies.
    - cards of which the PIN was lost or (possibly) compromised, as reported by the Card Holder.
    - all cards that was confiscated by a Control Body and returned to the CIA.
  - possibly requesting card certificate revocation by the MSCA, by sending a revocation message.
- issuing tachograph cards as needed by the European Digital Tachograph Laboratory for Interoperability Testing, as specified in the Smart Tachograph Equipment Interoperability Test Specification, [9].

Moreover, the CIA shall

- appoint the MSCA, CP and CD.
- ensure that the appointed parties comply with all applicable requirements in this MSA certificate policy.
- provide accurate status information about each tachograph card to the respective Card Holder.
- notify all Card Holders about their obligations and oblige them to keep these.

- issue a Certification Practices Statement (CPS), written in Dutch or English. The CPS shall cover the activities of the CIA, the CP, the MSCA and the CD with regard to the Digital Tachograph and Smart Tachograph. The CIA will get the necessary input about the processes of the MSCA, the CP and the CD from these parties, as required elsewhere in this document. The CPS shall comply with the following requirements:
    - The CPS shall explain how the MSCA, the CP, the CIA and the CD comply with all applicable requirements in this MSA certificate policy.
    - The CPS shall follow the framework for certificate policies described in RFC 3647 [7].
    - The CPS may consist of or refer to a collection of documents, as appropriate to the organisation of its component services.
    - The CPS shall have to be approved by the MSA.
    - The CIA shall periodically review the CPS to make sure it still accurately describes the actual systems and processes of the CIA. The CIA shall invite the CP, MSCA and CD to likewise review the CPS and notify the CIA about any necessary changes. The CIA shall send the changed CPS to the MSA for approval.
    - The CIA is not required to make the CPS public.
- 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 [14].
- be certified according to ISO 9001.
- maintain adequate organisational and financial resources to operate in conformity with the requirements laid down in this policy.

1.3.6.2 Card Personaliser

The Card Personaliser is appointed by the Card Issuing Authority and can be contacted at the address specified in the CPS. The Card Personaliser shall operate in conformance with all applicable requirements in

- this MSA certificate policy,
- the ERCA certificate policy for the Digital Tachograph [4],
- the ERCA certificate policy for the Smart Tachograph [5],
- the Regulation 2016_799 [2], in particular Annex 1C.

In particular, the responsibilities of the Card Personaliser are:

- to have available a CP system for Production as well as a CP system for Interoperability Testing purposes, according to the Regulation 2016_799 [2]:
    - the Production CP system shall have sufficient capacity to fulfil the KPIs set in the contract with the CIA. The CP shall monitor capacity demands and make projections of future capacity requirements to ensure that adequate processing power and storage are available at all times.
    - The Interoperability Test CP system shall be a (logically) separate system. It shall use the Interoperability Testing master keys made available by the ERCA, as specified in Smart Tachograph Equipment Interoperability Test Specification, [9].
    - Adequate measures shall be taken to ensure that keys and certificates for Interoperability Testing are not generated, used or stored in the Production system, and keys and certificates for Production are not generated, used or stored in the Interoperability Test system.
- to generate Key Distribution Requests for all of the currently valid versions[4] of the Motion Sensor Master Key – Workshop Card part (K_{M-WC}) and the DSRC Master Key (K_{DSRC}) conform the ERCA certificate policy [5], and send these requests to the MSCA to be forwarded to the ERCA.
- to receive the resulting Key Distribution Messages from the ERCA via the MSCA as specified in chapter 5, and decrypt and securely store the K_{M-WC} and the K_{DSRC}.
- to store, use and manage the K_{M-WC} and K_{DSRC} in accordance with the requirements in chapter 7 of this policy.
- to handle tachograph card personalisation data in accordance with applicable data protection rules and regulations.
- to provision and personalise smart tachograph cards on request of the CIA, including
    - providing the card body, the chip module and the chip itself.
    - securely generating and managing first-generation and second-generation tachograph card key pair(s), in accordance with the requirements in chapter 7 of this policy.
    - requesting the corresponding first-generation and second-generation public key certificate(s) from the MSCA, as specified in section 4.1 of this policy.
    - personalising the electronic data into the card, as specified below,
    - printing visual personalisation data on the card.
- to ensure and verify the consistency of all electronic and visual personalisation data on each card.
- to package and label the personalised tachograph cards.
- to keep the CIA informed of the personalisation status of each tachograph card.

The following requirements apply to the personalisation of each card:

- The exact personalisation data is dependent on the type of card and shall comply with the requirements in Appendix 2 of Annex 1C, [2]:
    - The Generation-1 application on the card shall contain the necessary first-generation card private keys and certificates,
    - The Generation-2 application on the card shall contain the necessary second-generation card private keys and certificates,

[4] Refer to Annex 1C [2], Appendix 11, sections 9.2.1.2 and 9.2.2.2 for details.

  - The Generation-1 application on the card shall contain the first-generation ERCA public key as a trust point,
  - The Generation-2 application on the card shall contain one, two or three ERCA root certificates as trust points and zero or one link certificates, as specified in Appendix 11 of Annex 1C.
- The electronic personalisation data of the Generation-1 and Generation-2 applications on the card shall be consistent,
- The electronic personalisation data of the card shall be consistent with the visual personalisation,
- The validity period of the card and of the card's certificates shall be consistent. The effective date of the card's certificate(s) shall be equal to the begin of the validity of the tachograph card itself, as encoded in EF Identification.
- The time part of the effective date of the card's certificates shall be set to 00:00:00.
- The time part of the expiry date of the card's certificates shall be set to 00:00:00; e.g. a Driver Card_MA certificate with effective date 01-07-2019 00:00:00 shall have its expiry date set to 01-07-2024 00:00:00.
- The expiry date printed on the outside of the card shall be equal to the date part of the expiry date of the card's MA certificate (01-07-2024 in the example above). This date shall be interpreted as the first date on which the card is no longer valid.
- Issuance of replacement cards shall be possible, in accordance with clause (420) in Annex 1C. [2]. This means that both the CP and MSCA shall be able to handle card certificates with a validity period shorter than those specified in Appendix 11.

Note regarding the last three bullets: the CIA is responsible for setting the certificate EOV (for Gen-1 card certificates) or the certificate effective date and the expiry date (for Gen-2 card certificates) correctly. The CIA includes these data elements in the Card Application Message to the Card Personaliser.

Moreover, the Card Personaliser shall:

- upon request of the CIA, deliver input for writing the Certification Practices Statement; see section 1.3.6.1. The input shall explain in detail how the CP complies with all applicable requirements in this MSA certificate policy.
- upon request of the CIA, review the CPS to make sure it still accurately describes the actual systems and processes of the CP, and notify the CIA 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 [14].
- be certified according to ISO 9001.
- maintain adequate organisational and financial resources to operate in conformity with the requirements laid down in this policy.

1.3.6.3 CARD DISTRIBUTOR

The Card Distributor is appointed by the Card Issuing Authority and can be contacted at the address specified in the CPS. The Card Distributor shall operate in conformance with all applicable requirements in this MSA certificate policy.

The Card Distributor is responsible for:

- upon request of the CIA, collecting personalised tachograph cards from the Card Personaliser and distributing them to the intended card holders.
- reliably verifying the identity of the intended card holder prior to handing over a tachograph card, according to the requirements in section 3.2.3 of this policy.
- informing the CIA of either the success or the failure[5] of the distribution of each tachograph card.

Moreover, the Card Distributor shall:

- upon request of the CIA, deliver input for writing the Certification Practices Statement; see section 1.3.6.1. The input shall explain how the CD complies with all applicable requirements in this MSA certificate policy.
- upon request of the CIA, review the CPS to make sure it still accurately describes the actual systems and processes of the CD, and notify the CIA 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 [14].
- be certified according to ISO 9001.
- maintain adequate organisational and financial resources to operate in conformity with the requirements laid down in this policy.

1.3.6.4 CONTROL BODIES

Apart from their duties as a party relying on the Dutch MSCA's services (see section 1.3.5), the control bodies are also responsible for returning any confiscated tachograph cards to the Card Issuing Authority.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by the Dutch Smart Tachograph MSCA may be used as card certificates in the Smart Tachograph system, as specified in Appendix 11 of Annex 1C [2].

1.4.2 Prohibited certificate uses

All other uses of certificates issued by the Dutch Smart Tachograph MSCA are prohibited.

[5] In case of failure of distribution, the CIA is responsible for solving the issue.

1.5 Policy administration

1.5.1 Organisation administering the document

The organisation responsible for drafting, maintaining and updating of this The Netherlands’ MSA certificate policy in accordance with the ERCA certificate policy [5] is The Netherlands’ Smart Tachograph Member State Authority, which can be reached at the following address:

Inspectie Leefomgeving en Transport
Ministerie van Verkeer en Waterstaat
Postbus 16191
2500 BD Den Haag
The Netherlands

The MSA shall:

- ensure that the appointed CIA correctly implements the requirements in this document,
- verify the compliance to this Policy of the Certificate Practice Statement (CPS) written by the CIA.

1.5.2 Contact person

Questions about this The Netherlands’ MSA certificate policy should be addressed to the contact person identified in the CPS.

1.5.3 Person determining CP suitability

This document shall be approved by the ERCA, as specified in the ERCA certificate policy [5].

1.5.4 CP approval procedures

The approval procedure for this MSA certificate policy is documented in the ERCA certification practices statement (CPS), [6].

1.6 Definitions and acronyms

Acronym	*Definition*
AES	Advanced Encryption Standard (algorithm)
CB	Control Body
CD	Card Distributor
CIA	Card Issuing Authority
CH	Card Holder
CP	Certificate Policy
CP	Card Personaliser
CPS	Certification Practice Statement
DSRC	Dedicated Short Range Communication
EC	European Commission
ECC	Elliptic Curve Cryptography (algorithms)
EGF	External GNSS Facility
ERCA	European Root Certification Authority
EU	European Union
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
IDS/IPS	Intrusion Detection System / Intrusion Protection System
JRC	Joint Research Centre
KCR	Key Certification Request
K_{DSRC}	DSRC Master Key

KDR	Key Distribution Request
KDM	Key Distribution Message
K_M	Motion Sensor Master Key
$K_{M\text{-}WC}$	WC part of K_M
KPI	Key Performance Indicator
MA	Mutual Authentication
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman (algorithm)
TDES	Triple Data Encryption Standard (algorithm)
VU	Vehicle Unit
WC	Workshop Card

2 Publication and repository responsibilities

2.1 Repositories

The Dutch MSA shall be responsible for a public website, which shall be the repository for public documentation regarding the Dutch Smart Tachograph system, as listed in the next section. The URL of this website shall be listed in the CPS.

The Card Issuing Authority shall be responsible for a public website, which shall be the repository for public documentation regarding the process to apply for a Smart Tachograph card. This website shall also offer (future) Card Holders the possibility to start the application process, to upload the necessary information and to view the progress. The URL of this website shall be listed in the CPS.

The MSCA does not need to keep up a public website regarding the Smart Tachograph system. There is no need for the general public to be informed about issued tachograph card certificates and their current status. For participants in the Dutch Smart Tachograph PKI, the MSCA shall make available certificate status information as described in section 4.10.

2.2 Publication of certification information

2.2.1 Information published in the MSA repository

The Dutch MSA shall publish the following information on its website:

- The Netherlands’ MSA Certificate Policy for the Digital Tachograph and Smart Tachograph (this document),
- MSA certificate policy change proposals (see section 10.12),
- A compliance statement by the ERCA for the MSA certificate policy,
- A compliance statements by the MSA for the Certification Practice Statement.

2.2.2 Information visible on Dutch smart tachograph cards

Clause (230) in Annex 1C [2] leaves a number of decisions regarding the visible information shown on a smart tachograph card to the discretion of the national authorities. On Dutch tachograph cards, the following information will (and will not) be printed:

- Workshop cards will contain a photograph of the fitter,
- Workshop cards will not contain a signature of the fitter,
- Workshop cards and control cards will contain the surname of the fitter or control officer, but it may be identical to the workshop name or control body name,
- Workshop cards and control cards may optionally contain the first name of the fitter or control officer,
- Control cards will not contain a photograph of the control officer,
- Control cards will not contain a signature of the control officer,
- Company cards will not contain a photograph or signature, since these cards are not bound to a natural person,
- Driver cards will not contain a signature of the driver,
- Driver cards will not contain the normal place of residence or postal address of the holder,
- Field 4d may contain an additional number for administrative purposes. For Dutch workshop cards, field 4d will contain the ‘keuringsinstantienummer’ (inspection body number) of the workshop. For other types of cards, this field will not be used.

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 10.12 of this document.

2.4 Access controls on repositories

All information available via the websites mentioned in section 2.1 shall have read-only access. The MSA and the CIA shall designate staff having write or modify access to the information.

All information published on these websites shall be available via a secure Internet connection.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject of a certificate issued by the Dutch MSCA is a tachograph card. The subject is identified by the Certificate Holder Reference (CHR) field in the certificate.

The issuer of the certificate (i.e. the MSCA) is identified by the Certificate Authority Reference (CAR) field in the certificate. Section 3.1.1 of the Smart Tachograph ERCA certificate policy [5] describes how these identifiers are formed.

The value of the `additionalInfo` field in the CHR of Dutch MSCA certificates for Production shall have the value ‘FF FF’. In MSCA certificates for Interoperability Testing, `additionalInfo` shall have the value ’54 4B’.

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 [5] and in Annex 1C [2].

3.1.3 Anonymity or pseudonymity of subscribers

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

Subscriber anonymity is not allowed.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The Card Issuing Authority is responsible for deriving a unique Certificate Holder Reference for each card[6] and communicating this to the Card Personaliser.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

When submitting a Key Certification Request (KCR) to the MSCA, the Card Personaliser 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.

[6] See section 4.2.2. The same CHR shall be used for all certificates on a given card, and this CHR shall not be used for any other certificate.

The full KCR format, including the signature, is specified in the Interface Requirement Specification [11].

3.2.2 Authentication of organisation identity

As described in section 1.3, the Dutch Digital Tachograph and Smart Tachograph PKI consists of

- a single Member State Authority, identified in section 1.5.1,
- a single Card Issuing Authority, identified in section 1.3.6.1,
- a single Member State Certificate Authority, identified in section 1.3.2.3,
- a single Card Personaliser, identified in section 1.3.6.2,
- a single Card Distributor, identified in section 1.3.6.3.

Since all of these organisations are directly appointed and no other organisations will need to connect to the Dutch Smart Tachograph system, it is not necessary to authenticate any organisation’s identity.

3.2.3 Authentication of individual identity

3.2.3.1 DURING CARD APPLICATION

The 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:

- The CIA shall inform the Card Holder of the terms and conditions regarding the use of the certificates.
- The CIA shall communicate this information through a durable means of communication in readily understandable language.
- The CIA shall collect adequate evidence, from an appropriate and authorised 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, the CIA shall check evidence of the identity against a nationally recognised 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 organisational entity (i.e. a workshop), the CIA shall check evidence of the Card Holder's identity against a nationally recognised identity document, e.g. a driver's license, and evidence that the Card Holder is indeed associated with the legal person or organisational entity.
- If the Card Holder is an organisational entity (i.e. a transport company), the CIA shall check the Card Holder's identity against a recognised registration.

3.2.3.2 DURING CARD DELIVERY

The Card Distributor shall authenticate the individual identity of a Card Holder before delivering a tachograph card:

- For driver cards, workshop cards or control cards, the Card Distributor 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 the Card Distributor prior to distribution. During distribution, the Card

Distributor shall verify the identity of this person in person by means of a check of a valid identity document containing a photograph.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

The MSCA shall not rely on any external certificate authority for the certificate signing services they provide to the Dutch Smart Tachograph system.

Participants in the Dutch Smart Tachograph system shall rely on so-called PKIoverheid certificates to guarantee the authenticity and integrity of digital messages exchanged with other participants, as specified in the respective Interface Requirements Specifications, [11] and [12]. These certificates shall be issued in the 'Domein Organisatie Services' under the Staat der Nederlanden Root CA - G3 root certificate. For more information, please refer to https://www.pkioverheid.nl/. The Certification Practices Statement of PKIoverheid can be found at https://cps.pkioverheid.nl/.

In accordance with chapter 4 of the Smart Tachograph ERCA Certificate Policy [5], the cryptographic strength of the security mechanisms used to protect messages exchanged between Dutch Smart Tachograph system participants shall be at least as strong as the strength of the transported keys and encrypted data.

If any participant in the Dutch Smart Tachograph system must rely on any other external PKI for any other service or function, they shall review and approve the Certificate Policy and/or Certification Practices Statement of the external certification service provider prior to applying for certification services as a subject.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identical to those described in section 3.2.

3.3.2 Identification and authentication for re-key after revocation

Identical to those described in section 3.2.

3.4 Identification and authentication for revocation request

Certificate revocation requests (see section 4.9) received by the MSCA from the Dutch MSA or the CIA shall be validated by direct communication. The MSCA shall ignore certificate revocation requests from any other party.

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

4.1 Certificate Life-cycle operational requirements for certificates

4.1.1 Certificate application

4.1.1.1 Who can submit a certificate application

Key Certification Requests (KCR) can only be submitted to the MSCA by the Card Personaliser.

Continuation of key certification services from the MSCA shall depend on timely receipt by the MSA of the audit reports for all PKI participants (see chapter 9), demonstrating that all of these parties are continuing to fulfil their obligations as laid down in this MSA certificate policy.

4.1.1.2 Enrolment process and responsibilities

As there is only one appointed party (the Card Personaliser) that can submit a key certification request, there is no enrolment process for such parties.

The responsibilities of the Card Personaliser regarding an application for a card certificate are:

- to securely generate an RSA or ECC key pair (as applicable), in accordance with the requirements in section 7.1.1.2 of this policy. For an ECC key pair, the CP shall use standardised domain parameters having the same key strength as those used in Dutch MSCA certificate indicated in the CAR field of the Key Certification Request.
- to create a Key Certification Request (KCR) message as specified in the Interface Requirement Specification [11], and send it to the MSCA. The format and contents of the KCR shall be identical to the tachograph card certificate to be signed by the 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, [2]. For ECC certificates, the signature shall be created as specified in CSM_150 in section 9.3 of Appendix 11.
- to digitally sign the KCR as specified in [11], using a key pair certified by a PKIoverheid certificate (see section 3.2.6).

The Gen-1 application on a tachograph card needs a single card certificate. The Gen-2 application on a tachograph card needs a card certificate for Mutual Authentication. Additionally, the Gen-2 application on a driver card and a workshop card needs a card certificate for Signing. Consequently, for each driver card and workshop card to be issued, the CP shall send two KCRs for Gen-2 certificates to the MSCA (in addition to a KCR for a Gen-1 certificate). The only differences between the two Gen-2 KCRs shall be in the value of

- the Public Point field,
- the CHA field, as specified in section 2.67 of Appendix 1 to Annex 1C, [2] and [3],
- the CExD field, as specified in requirements CSM_88 and CSM_89 in Appendix 11 to Annex 1C.

4.1.2 Certificate application processing

4.1.2.1 Performing identification and authentication functions

The MSCA shall authenticate the KCR message received from the CP by verifying the digital signature over the message or by using an authenticated connection dedicated to sending KCR messages and responses, as specified in the Interface Requirement Specification [11].

If this authentication fails, the MSCA shall reject the KCR and shall send an appropriate error message to the CP, as specified in [11].

4.1.2.2 Approval or rejection of certificate applications

The MSCA shall

- verify that the KCR format complies with the specification in [11].
- verify the signature over the KCR, using the public key contained in the KCR,
- verify that the Certification Authority Reference contained in the KCR indicates a MSCA private key currently valid for signing card certificates.
- verify that the Certificate Holder Reference (CHR) in the KCR is unique within the context of both Production and Interoperability Testing card certificates. However, the same CHR shall be used for all certificates on a given card. This means that the same CHR will be used in the KCRs for
  - the Card certificate in the Gen-1 application on the card,
  - the Card_MA certificate in the Gen-2 application on the card,
  - the Card_Sign certificate in the Gen-2 application on the card (for driver cards and workshop cards only)[7].
- for Gen-2 KCRs only: verify that the domain parameters specified in the request are of equal strength as those in the MSCA certificate indicated in the Certification Authority Reference.
- verify that the public key in the KCR is unique within the context of both Production and Interoperability Testing card certificates.
- verify that the Card Personaliser has not previously used the public key in the KCR as an ephemeral key for key agreement in a Key Distribution Request to the ERCA (see section 5.1), even for Interoperability Test purposes.
- for Gen-2 KCRs only: verify that the Public Point is on the curve indicated by the Domain Parameters in the KCR.
- verify the correctness of the validity period of the requested tachograph card certificate. For Gen-1 certificates, this can be done using the Start of Validity (SOV)[8] field and the EOV and CHA fields in the certificate. For Gen-2 certificates, this can be done using the CEfD, CExD and CHA fields.

If any of these checks fails, the MSCA shall reject the KCR. The MSCA shall send an appropriate error message to the CP, as specified in [11]. In such a case, the Card Personaliser shall not send a KCR for a new card certificate in place of the rejected request. Instead, it is the responsibility of the CIA to investigate and (let) solve the problem, and to send a new Card Application Message to the Card Personaliser for the same tachograph card once the problem is solved.

4.1.2.3 Time to process certificate applications

[7] The CHA field in a certificate is used to indicate whether it is a Card_Sign or a Card_MA certificate.

[8] Note that there is no SOV field in a Gen-1 certificate. However, this data is transmitted in a Card Application Message sent by the CIA to the CP, and in the KCR message sent by the CP to the MSCA.

4.1.2.4 Service levels for MSCA services

The certificate signing services of the MSCA shall be available to the Card Personaliser and the Card Issuing Authority 24 hours per day, 7 days per week. Immediately following generation, the MSCA shall send the complete and accurate certificate to the Card Personaliser, as specified in [11].

The exact service levels regarding e.g. service availability, response times, maximum failure rates, maximum down time after a failure and business continuity shall be defined by appropriate Key Performance Indicators in the contract between the CIA and the MSCA.

4.1.2.5 Service levels for CP services

The CP card personalisation services shall be available to the Card Issuing Authority 24 hours per day, 7 days per week.

The exact service levels regarding e.g. service availability, response times, maximum failure rates, maximum down time after a failure and business continuity shall be defined by appropriate Key Performance Indicators in the contract between the CIA and the CP.

4.1.2.6 Service levels for CIA services

The card application services of the CIA shall be available to Card Holders 24 hours per day, 7 days per week.

The exact service levels regarding e.g. service availability, response times, maximum failure rates, maximum down time after a failure and business continuity shall be defined by appropriate Key Performance Indicators in the contract between the Dutch MSA and the CIA.

4.1.2.7 Service levels for CD services

The exact service levels for the Card Distributor regarding e.g. service availability, response times, maximum failure rates, maximum down time after a failure and business continuity shall be defined by appropriate Key Performance Indicators in the contract between the CIA and the CD.

4.1.3 Certificate issuance

4.1.3.1 MSCA actions during certificate issuance

If all checks specified in section 4.2.2 succeed, the MSCA shall proceed to sign the requested tachograph card certificate. The format of the certificate shall comply with the format specified in Appendix 11 to Annex 1C [2].

The following information shall be recorded in an MSCA database for each Key Certification Request received:

- the complete KCR originating from the CP,
- the Certificate Holder Reference,
- the Certificate Authority Reference,
- 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,
- a timestamp.

4.1.3.2 Notification to subscriber by the CA of issuance of certificate

The MSCA does not directly notify the subscriber (i.e., the Card Holder). The MSCA shall return the tachograph card certificate to the Card Personaliser as specified in the Interface Requirement Specification [11]. The MSCA shall also return the MSCA certificate used to sign the tachograph card certificate.

4.1.4 Certificate acceptance

4.1.4.1 Conduct constituting certificate acceptance

Upon reception of the certificate, the Card Personaliser shall check that:

- the format of the certificate complies with the format specified in Appendix 11 to Annex 1C [2].
- all certificate field values match the values requested in the KCR.
- the certificate signature can be verified using the MSCA public key indicated in the CAR field of the certificate.

If any of these checks fail, the Card Personaliser shall abort the process, and contact the CIA. The CIA shall then revoke the certificate according to the certificate revocation procedure (see section 4.9).

4.1.4.2 Publication of the certificate by the MSCA

The MSCA is not required to publish any tachograph card certificate it signed.

4.1.4.3 Notification of certificate issuance by the MSCA to other entities

No stipulation.

4.1.5 Key pair and certificate usage

4.1.5.1 Subscriber private key and certificate usage

The subscriber (i.e., the Card Holder) shall use the private key in their tachograph card in accordance with all requirements in Annex 1C [2].

If the Card Personaliser generates a tachograph card private key outside the card itself (see section 7.1.1), the CP shall not use the private key for any purpose except inserting it into the designated tachograph card. After finishing the personalisation process of the card, the Card Personaliser shall destroy any copies of the private key that exist outside the card.

4.1.5.2 Relying party public key and certificate usage

Relying parties shall use the tachograph card certificate in accordance with the requirements in section 1.4 of this policy. Relying parties shall verify the signature over any tachograph card certificate before using or trusting it, unless they have verified it in the past.

4.1.6 Certificate renewal

Certificate renewal, i.e. the extension of the validity period, is not allowed for a tachograph card certificate.

4.1.7 Certificate re-key

Certificate re-key means the signing of a new tachograph card certificate, in replacement of the existing certificate. Certificate re-key is not allowed for tachograph card certificates.

As specified in section 7.3.2, the MSCA shall use a given private key for two years. The MSCA shall generate a new key pair timely, and ensure that the ERCA signs a corresponding MSCA certificate, according to the procedures specified in section 4.1.8 in the ERCA certificate policy [5].

The MSCA is allowed to use multiple MSCA private key concurrently, with overlapping validity periods of the corresponding certificates. In the CPS, the 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 revocation

The MSCA shall revoke a tachograph card certificate upon:

- rejection on receipt of a newly issued certificate by the Card Personaliser (see section 4.4.1).
- reception of a revocation request from the CIA or the MSA.

The CIA should request the revocation of a card certificate in the following circumstances:

- confiscation, loss, theft or malfunctioning of the tachograph card.

The CIA shall request the revocation of a card certificate in the following circumstances:

- compromise, suspected compromise or loss of a workshop card PIN.
- compromise or suspected compromise of a card private key.

The MSA shall request the revocation of a card certificate in the following circumstances:

- revocation of the MSCA certificate used to sign the card certificate.
- failure of the MSCA to meet obligations under this MSA certificate policy.

4.1.9.2 Who can request revocation

The Dutch MSCA shall consider revocation requests originating from the following entities as authoritative:

- the Dutch Member State Authority.
- the Card Issuing Authority.

The MSCA shall reject revocation requests originating from any other entity.

4.1.9.3 Procedure for revocation request

The MSCA shall describe the revocation procedure for tachograph card certificates, originating from either the CIA or the MSA, in the CPS..

4.1.9.4 Revocation request grace period

The grace period for tachograph card certificate revocation shall be specified in the CPS. Within this grace period the CIA or MSA shall make a revocation request to the MSCA.

4.1.9.5 Time within which CA must process the revocation request

Immediately after the receipt of an authorised request to do so, the MSCA shall revoke the certificate by changing its status in the database mentioned in section 4.10.1.

4.1.9.6 Revocation checking requirement for relying parties

No stipulation.

4.1.9.7 CRL issuance frequency (if applicable)

Not applicable. The MSCA is not required to publish a CRL.

4.1.9.8 Maximum latency for CRLs (if applicable)

Not applicable.

4.1.9.9 On-line revocation/status checking availability

Not applicable.

4.1.9.10 On-line revocation checking requirements

No stipulation.

4.1.9.11 Other forms of revocation advertisements available

No stipulation.

4.1.9.12 Special requirements regarding key compromise

No stipulation.

4.1.9.13 Circumstances for suspension

Certificate suspension, i.e. the temporary withdrawal from service of a tachograph card certificate, is not allowed.

4.1.9.14 Who can request suspension

Not applicable.

4.1.9.15 Procedure for suspension request

Not applicable.

4.1.9.16 Limits on suspension period

Not applicable.

4.1.10 Certificate status services

4.1.10.1 Operational characteristics

The MSCA shall maintain a database containing certificate status information for all card certificates issued. The MSCA shall allow the MSA and the other participants in the Dutch Smart Tachograph PKI to request the current status of a given certificate. In the CPS, the MSCA shall specify how these parties can obtain this information, how long an information request will take to be answered and in what form the information will be distributed.

4.1.10.2 Service availability

In the CPS, the MSCA shall specify the availability of this service.

4.1.10.3 Optional features

No stipulation.

4.1.11 End of subscription

Subscription for the MSCA's certificate signing services ends when the CIA decides to appoint a different party to the role of Card Personaliser.

In such a case, card certificates requested by the existing Card Personaliser do not need to be revoked for this sole reason.

4.1.12 Key escrow and recovery

4.1.12.1 Key escrow and recovery policy and practices
Key escrow is expressly forbidden: MSCA private keys shall not be exported to or stored in any system apart from the MSCA systems. Likewise, after card personalisation is finished, tachograph card private keys shall not be stored in any system apart from the tachograph card itself.

4.1.12.2 Session key encapsulation and recovery policy and practices
No stipulation.

4.2 Life-cycle operational requirements for master keys

4.2.1 Master key application

As specified in Annex 1C [2], workshop cards shall be equipped with the Motion Sensor Master Key – Workshop Card part (K_{M-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 an MSCA as specified in the ERCA certificate policy, [5].

In order to be able to store these master keys in the corresponding cards, the Card Personaliser shall have these keys at its disposal. All details of the process of distributing these keys from the ERCA to the CP (via the MSCA) are specified in the Interface Requirements Specification [13]. On a high level, the distribution process is as follows:

1. The Card Personaliser generates a Key Distribution Request (KDR) for a master key conform section 4.2.1 of the ERCA certificate policy [5], and protected according to section 4.2.3, including the generation of an ephemeral key pair for key agreement in their HSM.
2. The Card Personaliser sends the KDR to the MSCA.
3. The MSCA verifies the correctness of the KDR as specified in section 5.2.
4. The MSCA sends the KDR to the ERCA by courier, as specified in the ERCA certificate policy and the ERCA CPS [6]. The MSCA shall comply with all applicable requirements in section 4.2.2 of the ERCA certificate policy.
5. The ERCA creates a Key Distribution Message (KDM) as specified in the ERCA certificate policy and returns this to the MSCA.
6. The MSCA verifies the correctness of the KDM as specified in section 5.3.
7. The MSCA sends the KDM to the Card Personaliser.
8. The Card Personaliser processes the KDM as specified in section 5.3.

4.2.2 Master key application processing

Before forwarding the Key Distribution Request received from the Card Personaliser to the ERCA, the MSCA shall verify that:

- the KDR format complies with the specification in section 4.2.1 of the ERCA certificate policy, [5].
- the type of master key requested in the KDR is the K_{M-WC} or the K_{DSRC}.
- 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 MSCA certificate(s).
- the ephemeral public point in the request has not been certified by the 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 MSCA shall not send the KDR to the ERCA, but shall notify the Card Personaliser of the problem. The Card Personaliser shall then generate a new KDR.

If all checks pass, the 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 [2], 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 MSCA shall send the KDR to the ERCA by means of a courier, in compliance with all requirements in section 4.2.5 of the ERCA certificate policy, [5].

4.2.3 Master key distribution

Distribution of the Key Distribution Message shall take place as described in section 5.1 and in more detail in in the Interface Requirements Specification [13].

Before forwarding the Key Distribution Message received from the ERCA to the Card Personaliser, the MSCA shall carry out the first set of checks specified in section 4.2.6 of the ERCA certificate policy[9].

When receiving the KDM from the MSCA, the Card Personaliser shall carry out the second set of actions and checks specified in section 4.2.6 of the ERCA certificate policy. In case any of these checks fail, the CP shall contact the MSCA, who in turn shall contact the ERCA.

After the CP confirms to the MSCA that processing the Key Distribution Message was successful, the MSCA shall destroy any copy of the KDM that may still be in its possession.

4.2.4 Master key acceptance

No stipulation.

4.2.5 Master key usage

The Card Personaliser shall use all master keys in accordance with all applicable requirements in this policy, especially those in chapter 7.

[9] Since the MSCA does not have the ephemeral private key (which is generated by the Card Personaliser), it can only perform the first five checks in that section.

4.2.6 Master key renewal

No stipulation.

4.2.7 Master key re-key

At regular intervals, the ERCA will create a new version of the master keys; see section 4.2.8 of the ERCA certificate policy. Once the ERCA announces the availability of a new master key version, the Card Personaliser (via the MSCA) shall request this key from the ERCA as specified in sections 5.1 - 5.4. The CP and the MSCA shall take into account the guaranteed turnaround time of the ERCA of one month.

The Card Personaliser shall make sure that at all times it has in its possession all valid versions of the K_{M-WC} and the K_{DSRC}, in order to be able to issue workshop cards and control cards containing these key versions, as specified in Annex 1C [2], Appendix 11, sections 9.2.1.2 and 9.2.2.2.

4.2.8 Master key modification

Not applicable.

4.2.9 Master key revocation and suspension

Not applicable.

4.2.10 Master key status services

Not applicable.

4.2.11 End of subscription

Not stipulation.

4.2.12 Key escrow and recovery

Key escrow of K_{M-WC} and K_{DSRC} is expressly forbidden: these keys shall not be exported to or stored in any system apart from the Card Personaliser systems, workshop cards and control cards.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The key management and certificate generation and revocation services of the MSCA and the CP shall be housed in a secure area, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorised 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 CIA, the MSCA, the CP and the CD shall provide continuous monitoring and alarm facilities to detect and register any unauthorised or irregular attempts to access its resources, and to react upon them in a timely manner.

5.1.2 Physical access

The MSCA, CIA, Card Personaliser and Card Distributor 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 authorised individuals, i.e. persons in a trusted role as described in section 6.2.1.

5.1.3 Power and air conditioning

In the CPS, the CIA, MSCA, CP and CD 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 CIA, MSCA, CP and CD shall take measures to minimise 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 CIA, MSCA, CP and CD shall take measures to minimise the risk of fire in the facilities housing their systems.

5.1.6 Media storage

The MSCA, CIA. CP and CD shall take measures to protect any storage media used to store confidential data[10], such as hard disks, smart cards and HSMs, against unauthorised 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.

[10] Refer to section 10.3 for the definition of confidential data.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

In the CPS, the MSCA and the CP shall consider the use of an off-site backup of all critical information, especially 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 the Certification Practice Statement, the CIA, MSCA, CP and CD 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.

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

5.2.2 Number of persons required per task

The CIA, MSCA, CP and CD shall identify in the CPS 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 CPS 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 CIA, MSCA, CP and CD systems shall ensure effective user administration and access management. Access to critical systems shall be limited to individuals who are properly authorised 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 authorised 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 6.2.1.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All personnel involved with the CIA, MSCA, CP and CD 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 CPS.

5.3.2 Background check procedures

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

5.3.3 Training requirements

CIA, MSCA, CP and CD personnel training shall be managed according to a training plan described in the CPS.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorised actions

CIA, MSCA, CP and CD personnel shall be held accountable for their activities, which shall be logged in event logs as described in section 6.4. Possible consequences of unauthorised actions should be defined in personnel employment contracts.

5.3.7 Independent contractor requirements

Tasks may be outsourced to a specialised 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 6.3 and in the CPS shall be maintained.

The CIA, MSCA, CP and CD 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 document.

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

All significant security events in the CIA, MSCA, CP and CD 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.

In addition, the CIA software shall log the following events:

- Reception of a request to issue to tachograph card from a Card Holder.
- Sending a card application message to the CP.
- Sending a certificate revocation request to the MSCA.

In addition, the MSCA software shall log the following events:

- Reception of key certification requests.
- Reception of a certificate revocation request from the CIA or the MSA.
- 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.

In addition, the Card Personaliser software shall log the following events:

- Reception of a card application message from the CIA.
- Sending of a key certification request to the 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.
- Personalisation 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 addition, the Card Distributor software shall log the following events:

- Reception of a request from the CIA to distribute a tachograph card to a Card Holder.
- Confirmation to the CIA of the success or failure of card distribution.

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.

5.4.2 Frequency of processing log

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

In addition, the CIA, MSCA, CP and CD shall periodically inspect system logs for integrity. These inspections shall take place at least annually.

5.4.3 Retention period for audit log

In the CPS, the CIA, MSCA, CP and CD shall specify how long system event logs will be retained.

5.4.4 Protection of audit log

The CIA, MSCA, CP and CD shall maintain the integrity of system event logs during storage.

In the CPS, each of these parties shall specify who (which role) is authorised to inspect, modify or delete log files, and under what circumstances. Logs shall be protected from unauthorised inspection, modification, deletion or destruction.

5.4.5 Audit log backup procedures

System events logs shall be backed-up and stored in accordance with procedures described in the CPS.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The CIA, MSCA, CP and CD shall give in the CPS 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 CIA, MSCA, CP and CD 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 CIA, MSCA, CP and CD shall put in place measures and procedures to ensure that

- only persons in authorised 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 CIA, MSCA, CP and CD shall document these measures and procedures in the CPS.

5.5.4 Archive backup procedures

The CIA, MSCA, CP and CD 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 CIA, MSCA, CP and CD 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

The MSCA shall use a Gen-1 or Gen-2 MSCA private key for a period of two years. In order to guarantee the continuation of its services, the MSCA shall generate a new MSCA key pair in time. The MSCA shall request the ERCA, via the CIA, 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 Tachograph card key pairs

Tachograph card key pairs shall never be changed.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The CIA, MSCA, CP and CD 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 MSCA, CP and CD operations shall be reported to the CIA within 4 hours after the incident. All incidents with the CIA operations shall be reported to the 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 an MSCA private key and / or a master key, the MSCA or CP (as applicable) shall inform the Dutch MSA, the ERCA and the other participants in the Dutch Smart Tachograph PKI within 8 hours of detection. The MSA shall take appropriate measures within a reasonable time period.

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

5.7.2 Computing resources, software, and/or data are corrupted

In the CPS, the CIA, MSCA, CP and CD shall outline the procedures for recovering a secure environment after computing resources, software and/or data are corrupted. These mechanisms shall not depend on the ERCA response times.

For the MSCA, these procedures shall also describe which card certificates are revoked (if any).

5.7.3 Entity private key compromise procedures

5.7.3.1 BY THE MSCA

The MSCA shall specify recovery procedures to be used if an 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, 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 MSCA key pair is generated, and how a new MSCA certificate will be requested from the ERCA and be provided to the Card Personaliser. The MSCA shall immediately inform the CIA, CP and the MSA. The MSA shall immediately issue a revocation request for the MSCA certificates to the ERCA. The CIA shall inform the relying parties.
- If a compromise can be ruled out, the key shall be activated again.

In both cases, the MSCA and the MSA shall collaborate to find out the cause of the incident and shall determine any changes in the specified operational or technical security controls that are necessary to avoid a repeat. If changes must be made, they shall be documented in a new version of the CPS, as described in section 1.3.6.1.

5.7.3.2 BY THE CARD PERSONALISER

The Card Personaliser shall specify recovery procedures to be used if a master key is (suspected to be) compromised. These procedures shall describe how the affected 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, including all (backup) copies of it. The CPS shall also specify how a secure environment is re-established in this case, and how a new master key will be requested from the ERCA. The CP shall immediately inform the CIA, MSCA and the MSA. The CIA shall inform the relying parties.
- If a compromise can be ruled out, the key shall be activated again.

In both cases, the CP and the MSA shall collaborate to find out the cause of the incident and shall determine any changes in the specified operational or technical security controls that are necessary to avoid a repeat. If changes must be made, they shall be documented in a new version of the CPS, as described in section 1.3.6.1.

If a card private key is (suspected to be) compromised, the Card Personaliser shall immediately inform the CIA, MSCA and the MSA. The CIA shall inform the relevant relying parties. The MSCA shall revoke the card certificate. The CP and the MSA shall collaborate to find out the cause of the incident and shall determine any changes in the specified operational or technical security controls that are necessary to avoid a repeat. If changes must be made, they shall be documented in a new version of the CPS, as described in section 1.3.6.1.

5.7.4 Business continuity capabilities after a disaster

The following incidents are considered to be disasters:

a) compromise or theft of a private key and / or a master key,
b) non-availability of a private key and / or a master key,
c) IT hardware failure.

The CIA, MSCA, CP and CD shall each 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 MSCA shall ensure that in the event of a disaster, operations are restored within 48 hours.

The CIA, CP and CD shall ensure that in the event of a disaster, operations are restored within 2 weeks. For the CP it has to be considered that the production of the SMART tachograph cards will be done outside The Netherlands. This fact has to be approved by the policy department (DGMO) of the Ministry of Infrastructure and Watermanagement. The procedure for this approval has to be part of the Business Continuity Plan.

The CIA, MSCA, CP and CD 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.

5.8 PKI participant termination

In the event of termination of CIA activity by the currently appointed organisation (see section 1.3.6.1), the Dutch MSA shall appoint a new organisation responsible for the implementation of the applicable requirements in this policy. The current organisation shall transfer its CIA-related assets to the new organisation or to the MSA, while ensuring that confidentiality and integrity are maintained.

In the event of termination of MSCA activity by the currently appointed organisation (see section 1.3.2.3), the CIA shall appoint a new organisation responsible for the provision of key certification services to the Card Personaliser and for the implementation of the applicable requirements in this policy. The current organisation shall transfer its MSCA-related assets, including records required to provide evidence of certification for the purposes of legal proceedings, to the new organisation or to the CIA, while ensuring that confidentiality and integrity are maintained.

In the event of termination of CP activity by the currently appointed organisation (see section 1.3.6.2), the CIA shall appoint a new organisation responsible for the personalisation of Dutch tachograph cards and for the implementation of the applicable requirements in this policy. The current organisation shall transfer its CP-related assets to the new organisation or to the CIA, while ensuring that confidentiality and integrity are maintained.

In the event of termination of CD activity by the currently appointed organisation (see section 1.3.6.3), the CIA shall appoint a new organisation responsible for the distribution of Dutch tachograph cards and for the implementation of the applicable requirements in this policy. The current organisation shall transfer its CD-related assets to the new organisation or to the CIA, while ensuring that confidentiality and integrity are maintained.

In the CPS, the CIA, MSCA, CP and CD shall identify the assets that shall be transferred to another organisation in case of termination.

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

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

- The MSCA shall inform the MSA, CIA, the CP and the ERCA,
- The MSCA shall terminate all authorisation of subcontractors to act on behalf of the MSCA in the performance of any functions related to the process of issuing certificates,
- The MSCA shall perform necessary undertakings to transfer obligations for maintaining event log archives for their respective period of time as indicated in the CPS,
- The MSCA shall perform necessary undertakings to transfer certification status information of issued certificates to the CIA,
- The MSCA shall destroy its private keys,
- The MSCA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the MSCA becomes bankrupt or for other reasons is unable to cover the costs by itself,
- The 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.

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 MSCA shall generate MSCA key pairs for Production in accordance with Appendix 11 to Annex 1C [2]. Generation of key pairs shall be undertaken in a HSM that complies with the requirements in section 7.2. The HSM shall be located in a physically secured environment. 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 MSCA shall use publicly specified and appropriate cryptographic algorithms for key pair generation. The MSCA shall document a secure operation procedure for generating key pairs.

6.1.1.2 BY THE CARD PERSONALISER

The Card Personaliser shall generate tachograph card key pairs for Production in accordance with Appendix 11 to Annex 1C [2]. The Card Personaliser shall also generate ephemeral key pairs for key agreement, as specified in the Smart Tachograph ERCA certificate policy [5]. 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 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 CP shall import a master key for Production as specified in chapter 5. Master key import shall be undertaken in a physically secured environment by personnel in trusted roles under (at least) dual person control.

The 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 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 CARD PERSONALISER

The Card Personaliser 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 Card Personaliser 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 7.2. 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 7.2. 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 personalisation process. After finishing the personalisation process of the card, the Card Personaliser shall destroy any copies of the private key that exist outside the card.

For workshop cards and control cards, the Card Personaliser also needs to transfer K_{M-WC} and/or K_{DSRC} 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 MSCA shall deliver the MSCA public keys to be certified to the ERCA using the procedure described in section 4.1 of the ERCA certificate policy [5].

6.1.3.2 BY THE CARD PERSONALISER

The Card Personaliser shall deliver the card public keys to be certified to the MSCA using a key certification request as specified in the Interface Requirement Specification [11].

6.1.4 Public key delivery to relying parties

6.1.4.1 ERCA PUBLIC KEY DELIVERY

The MSCA and the CP shall download the ERCA root public key (for Gen-1) and the currently valid ERCA root certificate (for Gen-2) from the ERCA repository mentioned in the ERCA certificate policy [5]. When the ERCA publishes a new Gen-2 ERCA root certificate, the MSCA and the CP shall download the new certificate along with the link certificate, and shall verify the link certificate with the previous ERCA root key.

The MSCA shall use the ERCA root public keys to validate the signature over any Gen-1 or Gen-2 MSCA certificate it receives from the ERCA.

The Card Personaliser 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 Card Personaliser 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 [2]. Finally, if available, the Card Personaliser 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

The MSCA shall provide the Card Personaliser 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 MSCA to the CP, as specified in the Interface Requirement Specification [11]. The Card Personaliser 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 Card Personaliser 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 [2].

6.1.5 Key sizes

The MSCA and the CP shall choose the key sizes of the key pairs they generate in accordance with the requirements in Appendix 11 of Annex 1C [2].

6.1.6 Public key parameters generation and quality checking

In the CPS, the MSCA and the CP shall indicate whether they will use the Brainpool or NIST family of standardised domain parameters for their Gen-2 key pairs, in accordance with requirement CSM_48 in Annex 1C [2].

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 (as per X.509 v3 key usage field)

The MSCA shall use the MSCA private keys only for digitally signing issued tachograph card certificates, as detailed in chapter 4 of this policy.

The Card Personaliser 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 [2].

6.2 Private key and master 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 MSCA and the CP shall generate and use any private keys exclusively in a Hardware Security Module (HSM) or tachograph card. Similarly, the 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 [15][11] using a suitable Protection Profile; or
- meet the requirements in ISO/IEC 19790 [16] level 3; or
- meet the requirements in FIPS PUB 140-2 [17] level 3; or
- offer an equivalent level of security according to equivalent nationally or internationally recognised evaluation criteria for IT security.

[11] Better known as Common Criteria

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 MSCA shall make sure that 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 the CPS, the MSCA shall specify the number and trusted role of persons needed to carry out the following operations on MSCA private keys in an HSM:

- generation,
- activation for use (see section 7.2.8),
- 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 7.4.

6.2.2.2 BY THE CARD PERSONALISER

If tachograph card private keys are generated on-board the card (see section 7.1.2.2), 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 Card Personaliser 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.

The CP shall make sure that master 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 master keys used for Interoperability Testing.

In the CPS, the 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.

In addition, the CPS shall specify the number and trusted role of 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 7.4.

6.2.3 Private key and master key escrow

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

Key escrow of card private keys is expressly forbidden: after personalisation 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 Card Personaliser systems and in tachograph workshop cards and control cards.

6.2.4 Private key and master key backup

In the CPS, the MSCA and the CP shall describe backup and restore procedures for the 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 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

MSCA private key import and export into or from an HSM shall only take place for back-up and recovery purposes. 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 (see section 7.1.2.2)

Master key import shall only take place during the initial import of the Key Distribution Message received from the ERCA (see section 5.1), 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 of master keys stored inside a HSM for use, the MSCA and the 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 an MSCA private key (as specified in Appendix 11 of Annex 1C [2]), the 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 Card Personaliser shall destroy all copies of the key in its possession, such that it cannot be retrieved.

When an HSM containing a 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 7.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

MSCA public key certificates and hence the public keys shall be archived indefinitely, as discussed in section 6.5.

Tachograph card public keys shall not be archived.

6.3.2 Certificate operational periods and key pair usage periods

All MSCA certificates and tachograph card certificates shall have the validity period specified for them in Appendix 11 to Annex 1C [2].

As specified in Appendix 11, the MSCA shall use a 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

6.4.1 Activation data generation and installation

The MSCA and the CP shall describe in the CPS all credentials, such as passwords, PINs, authentication smart cards or other tokens, that are necessary to bring the HSM(s) containing the 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.

The MSCA and the 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 MSCA and the CP shall document the secure operating procedures to be followed to set each of the credentials to their initial value and to change them.

All knowledge-based credentials 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.

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

The MSCA, CIA, CP and CD 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 the CPS, the

MSCA, CIA, CP and CD 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 MSCA, CIA, CP and CD shall describe their policy regarding updates of hardware, operating systems and software. Change control procedures shall exist for modifications and releases for any operational software. In particular, 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 MSCA, CIA, CP and CD shall document their network architecture, including the use of firewalls and IDS/IPS, if any.

The MSCA and the CP shall devise 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 Time-stamping

The time and date of an event shall be included in every audit trail entry. The CPS shall describe how time is synchronised and verified by the MSCA, CIA, CP and CD.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)
All MSCA and tachograph card certificates requested and used by the MSCA and the CP shall have the profile 1, specified in Annex 1C, Appendix 11 and Appendix 1 [2].

7.1.2 Certificate extensions
No stipulation.

7.1.3 Algorithm object identifiers
No stipulation.

7.1.4 Name forms
No stipulation.

7.1.5 Name constraints
No stipulation.

7.1.6 Certificate policy object identifier
No stipulation.

7.1.7 Usage of Policy Constraints extension
No stipulation.

7.1.8 Policy qualifiers syntax and semantics
No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension
No stipulation.

7.2 CRL profile

7.2.1 Version number(s)
No stipulation. The MSCA is not required to publish a CRL.

7.2.2 CRL and CRL entry extensions
No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)
No stipulation. The MSCA is not required to maintain an OCSP.

7.3.2 OCSP extensions
No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The MSA is responsible for ensuring that regular audits of the MSCA, CIA, CP and CD take place.

In particular:

- The MSCA, CIA, CP and CD operating under this The Netherlands' MSA certificate policy shall be audited for conformance with the policy regularly. The first full and formal audit shall be performed within 12 months of the moment the first Dutch Generation-2 Production tachograph card is issued. Subsequently, an audit shall take place at least once every 24 months. If an audit finds evidence of nonconformity, the next audit shall be performed within 12 months.
- The audit shall cover the MSCA's, CIA's, CP's and CD´s practices for the Digital and Smart Tachograph, and verify their compliance with this policy as well as with the CPS and other internal documentation.
- The MSA is responsible for planning and conducting the CIA audit. The MSA may consult or sub-contract an external certification or accreditation organisation for the audit.
- The CIA is responsible for planning and conducting the MSCA, CP and CD audits. The CIA may consult or sub-contract an external certification or accreditation organisation for the audit.
- Before the start of the operations of the CIA, MSCA, CP and CD covered by the MSA certificate policy, the MSA or CIA (as appropriate) shall carry out a pre-operational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements in this 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 6.1 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 7 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 6.2 of this policy, and that the assignees comply with the requirements in section 6.3.

8.2 Identity/qualifications of assessor

Any person selected or proposed to perform a compliance audit of the CIA, MSCA, CP or CD shall first be approved by the Dutch Member State Authority. The name(s) of the auditors which will perform each audit shall be registered.

Auditors shall comply with the following requirements:

- Ethical behaviour: trustworthiness, uniformity, confidentiality regarding their relationship to the organisation 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 organisation being the subject of the audit.

8.4 Topics covered by assessment

Each audit shall cover compliance to this MSA certificate policy, the CPS and the associated procedures and techniques documented by the organisation.

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 operations (chapter 3);
- operational functions/services (chapter 4 and 5);
- physical, procedural and personnel security controls (chapter 6);
- technical security controls (chapter 7).

During the audit, the auditor shall assess the audit logs (see section 6.4) to determine whether weaknesses are present in the security of the systems of the organisation to be audited. Determined (possible) weaknesses shall be mitigated. The assessment and possible weaknesses shall be recorded.

8.5 Actions taken as a result of deficiency

The auditor shall deliver an audit report for each audit to the MSA or the CIA, as appropriate. If irregularities are found in an audit, a corrective action plan (CAP) will be drawn up by the audit organisation, The CAP shall define corrective actions, including an implementation schedule. The audit organisation shall carry out these corrective actions according to this schedule. As specified in section 9.1, another audit shall be performed within 12 months to verify that the irregularities have been solved.

Upon the receipt of an audit report, the MSA or CIA shall take appropriate action, depending on severity of the findings.

8.6 Communication of results

The CIA shall report on the results of any audit of the MSCA, CP and CD and provide an audit report, in English, to the MSA. This report shall include at least the number of deviations found and the nature of each deviation. If requested by the ERCA, the MSA shall send the full results of the compliance audit to the ERCA.

The MSA shall report on the results of any MSCA audit and provide an audit report, in English, to the ERCA. This report shall include at least the number of deviations found and the nature of each deviation.

Conclusive results[12] of the audits shall be available to other participants in the Dutch Smart Tachograph PKI system upon request.

[12] A 'conclusive result' is defined to be information on any irregularity that may affect a relying party's trust in a certificate, including an adequate judgment of its level of seriousness, but excluding detailed information that can be used to attack the systems of the audited party.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees
No stipulation.

9.1.2 Certificate access fees
No stipulation.

9.1.3 Revocation or status information access fees
No stipulation.

9.1.4 Fees for other services
No stipulation.

9.1.5 Refund policy
No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage
No stipulation.

9.2.2 Other assets
The CIA, MSCA, CP and CD shall have adequate arrangements to cover liabilities arising from their operations and/or activities.

9.2.3 Insurance or warranty coverage for end-entities
No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information
Confidential data shall comprehend at least:

- Private keys,
- Symmetric master keys,
- Audit logs (see section 6.4),
- Passwords, PINs, activation data (see section 7.4), etc.
- Detailed secure operating procedures and other documents regarding system management and security controls.

9.3.2 Information not within the scope of confidential information
The following information is public:

- information included in public key certificates issued by the MSCA,
- certificate status information in the MSCA repository (see section 4.10),
- this MSA certificate policy.

9.3.3 Responsibility to protect confidential information
Confidential information shall not be released by any PKI participant, unless a legal obligation exists to do so.

9.4 Privacy of personal information

9.4.1 Privacy plan

The CIA, MSCA, the CP and the CD 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 2016/679. Appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of personal data and to prevent accidental loss or destruction of, or damage to, personal data.

9.4.2 Information treated as private

Personally identifiable information, contact information, and authorisations of CIA, MSCA, CP and CD staff are private.

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

9.4.3 Information not deemed private

The following personal information is not deemed private:

- information included in public key certificates issued by the MSCA.
- card numbers.

9.4.4 Responsibility to protect private information

See section 10.4.1.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This MSA certificate policy is valid from the moment the first Dutch Generation-2 Production tachograph card is issued.

9.10.2 Termination

This MSA certificate policy shall be valid until further notice, e.g. when a new version of this document is approved by the ERCA.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

This MSA certificate policy is issued under responsibility of the Dutch Member State Authority. The MSA may revise this document if it deems this necessary. It is allowed to make editorial or typographical corrections to this policy without notification to the Dutch Smart Tachograph PKI participants and to the ERCA, and without an increase in version number. It is allowed to change the contact information in section 1.5 with notification to the PKI participants, but without change to the document version number.

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

1. All PKI participants may submit proposals for change to the MSA certificate policy to the MSA at any time.
2. The MSA shall distribute any proposal to change the MSA certificate policy to all PKI participants.
3. PKI participants may comment on the proposed changes within 15 days of change proposal notice.
4. The MSA shall consider the comments and shall decide which, if any, of the notified changes to implement.
5. The MSA shall notify the PKI participants about its decision.
6. The MSA shall consult the ERCA with respect to the necessity of renewal of the approval as result of the changes. If the MSA and the ERCA determine that the changes have a material impact on a significant number of users of the policy, the MSA shall submit the revised MSA Policy to the ERCA for

approval. The ERCA shall approve the revised version according to the procedure documented in the ERCA CPS [6].

7. The MSA shall publish a new version of the MSA certificate policy including all implemented changes, accompanied by an increase in the version number of the document.
8. The MSA and shall set an appropriate period for the changes to be implemented. Any item in this policy may be changed with 90 days' notice. Changes to items that, in the judgment of the MSA, will not materially impact a substantial majority of the users or relying parties using this policy may be changed with 30 days' notice.
9. All PKI participants shall determine the changes that must be made to its documentation, systems and processes as a result of the changed MSA certificate policy, and shall implement these changes within the implementation period set.

9.12.2 Notification mechanism and period

See the previous section.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute resolution provisions

The CIA, MSCA, CP and CD 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 PKI participants 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 MSA.

9.14 Governing law

The issuance and usage of tachograph cards in The Netherlands is regulated by the 'Regeling Tachograafkaarten', which can be consulted at http://wetten.overheid.nl/BWBR0018544/2018-05-04 (Dutch only).

9.15 Compliance with applicable law

This Certificate Policy is in compliance with Regulation (EU) No 165/2014 of the European Parliament and of the Council [1] and with Commission Implementing Regulation (EU) 2016/799 [2]. In case discrepancies exist between this document and the Regulation or Implementing Regulation, the latter shall prevail.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

If the CIA, MSCA, CP or CD is part of a larger organisation, it shall

- be independent of this organisation for its decisions relating to the establishing, provisioning, maintaining or suspending of services in conformance with this MSA certificate policy. In particular, its senior executive, senior staff and staff in trusted roles shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.
- have a documented organisational structure which safeguards impartiality of operations under this MSA certificate policy.

References

Ref. and Title		Author	Version	Date
[1]	Regulation (EU) No 165/2014, Official Journal of the European Union L60	European Parliament and the Council	-	4 February 2014
[2]	Commission Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 139 (including [3])	European Commission	-	18 March 2016
[3]	Commission Implementing Regulation (EU) 2018/502 amending Implementing Regulation (EU) 2016/799, Official Journal of the European Union L 85	European Commission	-	28 February 2018
[4]	Digital Tachograph System European Root Policy	EC Joint Research Centre	2.1	28 July 2009
[5]	Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy	EC Joint Research Centre	1.0	June 2018
[6]	Smart Tachograph - ERCA Certification Practice Statement	EC Joint Research Centre	1.0	October 2018
[7]	RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	Network Working Group	-	November 2003
[8]	RFC 2119, Key words for use in RFCs to Indicate Requirement Levels	Network Working Group	-	March 1997
[9]	Smart Tachograph Equipment Interoperability Test Specification	EC Joint Research Centre	0.99	May 2018
[10]	The Netherlands MSA Policy for the Digital Tachograph project according EU Council Regulation 2135/98	Human Environment and Transport Inspectorate	1.2	June 7, 2012
[11]	Interface Requirement Specification Card Personaliser & MSCA	Kiwa Register	1.0	TBD
[12]	Interface Requirement Specification Card Issuer & Card Personaliser	Kiwa Register	1.0	TBD
[13]	Key management of Motion Sensor Master Key – Workshop card part (KM-WC) and DSRC Master Key (KDSRC)	Kiwa Register	1.0	TBD

Ref. and Title		Author	Version	Date
[14]	ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements	ISO/IEC	Second edition	2013-10-01
[15]	ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3	ISO/IEC	Third edition	2008 – 2014
[16]	ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules	ISO/IEC	second edition	2012-08-15
[17]	National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules	NIST	-	May 25, 2001