Belgian MSA Policy for the Tachograph System

Belgian MSA Policy

for

the Tachograph system

with reference to

B-CIA, B-MSA, B-MSCA, and B-CP

Table of Contents

Belgian MSA Policy

1 INTRODUCTION

This document is the Belgian Member State Certification Authority Policy (hereinafter, B-MSCA) for the Tachograph system. Parties involved in the life cycle of certificates, tokens and applications of the Belgian Tachograph, must follow the requirements set out in this certificate policy.

This B-MSCA policy meets the requirements for the management of keys, certificates and associated equipment in relation with the Tachograph system.

- These requirements emanate from the documents stated below The Council Regulation of the Tachograph System 2135/98 of 24 September 1998 (OJ L274, 09.10.98)
- The Commission Regulation 1360/2002 of 13 June 2002 (OJ, L07, 05.08.02)
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates
- Guidelines and Template National CA policy –version 1.0.
- European Digital Tachograph Common Security Guidelines
- Digital Tachograph System, European Root Policy, version 2.0

Additional input references and a full list of acronyms are provided in the end of this document.

1.1 System overview and responsible organizations

1.1.1 Tachograph system overview

At European level, within the Tachograph system, a single European key pair (EUR.SK and EUR.PK) is generated. The European private key is used to certify Member States public keys including those of Belgium. A European Root Certification Authority (hereinafter, ERCA) operating under the authority and responsibility of the European Commission has responsibility for the management of the European key pair that is used to certify member state keys. ERCA also manages a European Root policy that sets out requirements for this B-MSCA policy.
.

At Member State level, a Member State Authority (MSA) generates a key pair (MS.SK and MS.PK). A member state key pair is also generated in Belgium. The European Certification Authority certifies public keys generated by the Belgian MSA (hereinafter B-MSA). The Belgian private key is used to certify public keys used with authorized Tachograph equipment (e.g. vehicle unit, Tachograph cards and motion sensors). The B-MSA also manages this B-

MSCA certificate policy that lays out the requirements for certificate management life cycle for the tachograph system in Belgium.

At equipment level, one single key pair (EQT.SK and EQT.PK) is generated and inserted in each piece of authorized equipment. Motion sensor keys are placed in the workshop card, vehicle unit and motion sensor for the purpose of mutual recognition of these devices. Vehicle units placed on board vehicles carry key pairs for authentication when cards are used. Additionally key pairs are used to digitally sign data downloaded from vehicle units or Tachograph cards to external media.
A Member State certification authority (hereinafter, MSCA) certifies equipment public keys within the Tachograph system. Equipment manufacturers, equipment personalizing agencies and Member State authorities manage the key pair generation and insertion. The equipment key pair is used for authentication, digital signature and encryption of data within the Tachograph system.
The Belgian Card Issuing Authority (hereinafter, B-CIA) acts as Registration Authority in the Tachograph system.

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

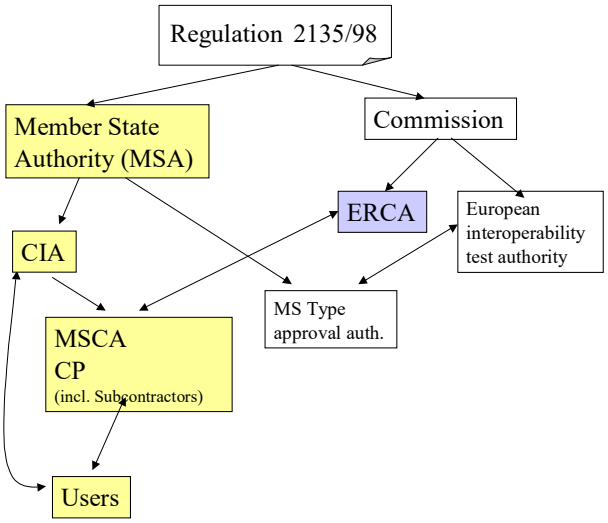

Figure 1 Tachograph system organisation (coloured boxes are covered in this document)

1.1.2 Responsible organisations

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

Federale Overheidsdienst	**Service Public Fédéral**
Mobiliteit en Vervoer	**Mobilité et Transport**
Directoraat-generaal	**Direction générale**
Wegvervoer en Verkeersveiligheid	**Transport routier et sécurité routière**
Dienst Wegvervoer	**Direction Transport par Route**
Vooruitgangstraat 56	**Rue du Progrès 56**
B-1210 Brussel	**B-1210 Bruxelles**

The Appointed Card Issuing Authority for Belgium (hereinafter, B-CIA) is:

Instituut Wegtransport en Logistiek België, VZW	**Institut Transport Routier et Logistique Belqiue, ASBL**
Archimedesstraat 5	**Rue Archimède 5**
B-1000 Brussel	**B-1000 Bruxelles**

B-CIA has appointed a third party external contractor to carry out technical operations with regard to the life cycle management of the Belgian Tachograph certificates. This appointed Belgian Member State Certification Authority (hereinafter, B-MSCA) is :

Verizon *(formerly known as* Cybertrust Belgium NV*)*
Culliganlaan 2E
1831 Diegem

The appointed Belgian Card Personalizing organisation (hereinafter B- CP) is:

Veridos Matsoukis S.A.
69, Dimocratias Ave.
13122 Ilion Athens
Greece

1.2 Approval

This Belgian MSA Policy has been approved by the European Commission, Directorate General, Joint Research Centre, on <January 13 2005.

1.3 Availability and contact details

The B-MSA policy is publicly available at: www.digitach.be

Questions concerning this B-MSCA certificate policy should be addressed to the address of the appointed B-CIA: as indicated above under section 1.1.

2 SCOPE AND APPLICABILITY

This policy applies to the domain of the B-MSCA that carries out certificate management operations within the Tachograph system in Belgium. The B-MSCA certificates can be used within the Tachograph system only to the exclusion of any other. The certificates issued in the Tachograph system can be used for specific electronic Tachograph purposes within the Tachograph system. The keys and certificates issued by the B-MSCA and the cards issued by the B-CIA are exlusively intended to be used within the Tachograph system. The scope of the Belgian MSA Policy within the Tachograph system is presented in the figure below. Four entities are depicted: the ERCA certification service provider (hereinafter, CSP); a MSCA CSP (or B-MSCA); and the two types of component personaliser (hereinafter, CP): tachograph card (B-CP) or vehicle unit manufacturing; and motion sensor manufacturing. With the exeption of the ERCA, assertions in this B-MSCA policy are binding to all these entities.

The ERCA and the B-MSCA create and maintain appropriate secret encryption keys and use them to validate digital tachograph security data, only after verifying that the data to encrypt are complete, correct, and duly authorized. The card, vehicle unit or motion sensor CPs insert validated security data into digital tachograph equipment by appropriately secured means.

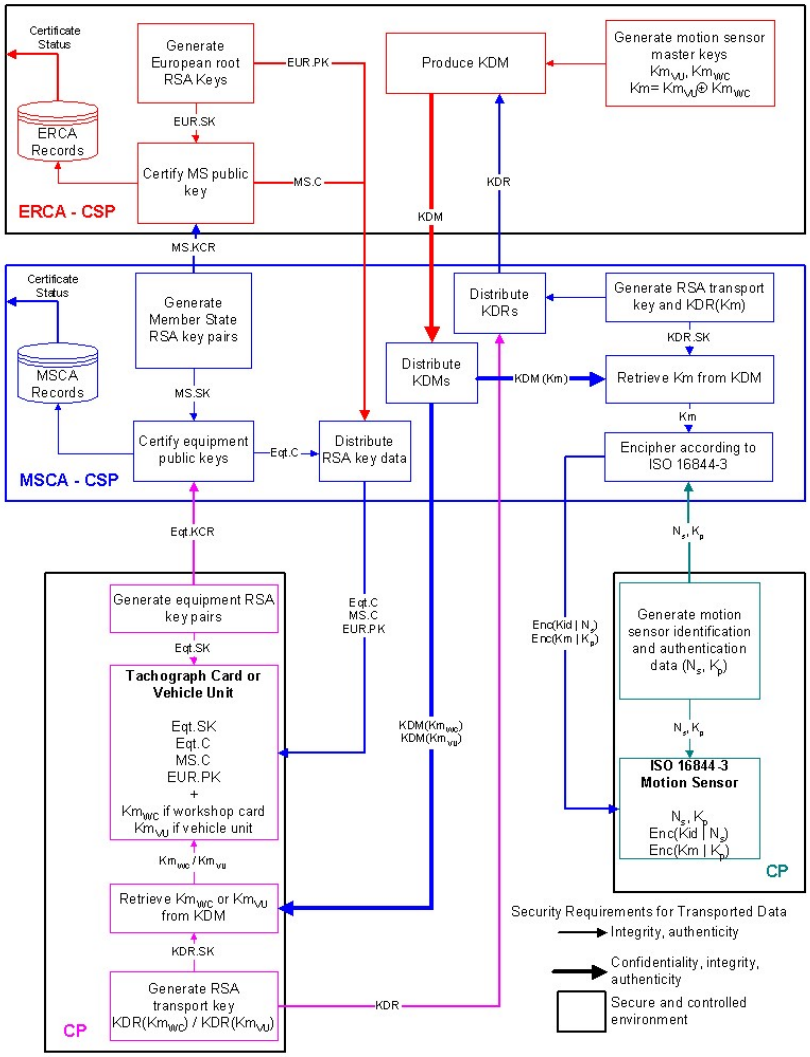

Figure 2 Tachograph system keys, certificates and equipment management. (Scope of policy is marked with bold lines.)[1]

Within the Tachograph system vehicle units and Tachograph cards use a public-key cryptographic system to provide for:

- Authentication of transmissions between vehicle units and cards.
- Transport of session keys between vehicle units and Tachograph cards.
- Digital signature of data downloaded from vehicle units or Tachograph cards to external media.
- The mutual recognition between the workshop card, vehicle unit and motion sensor.

Additionally, vehicle units and Tachograph cards use a symmetric cryptographic system to provide a mechanism for data integrity during user data exchange between vehicle units and Tachograph cards, and, where

[1] MSi is Belgium.

applicable, confidentiality of data exchange between vehicle units and Tachograph cards.

Within the Tachograph system the policy components follow the layout and interactions that are presented in the figure below:

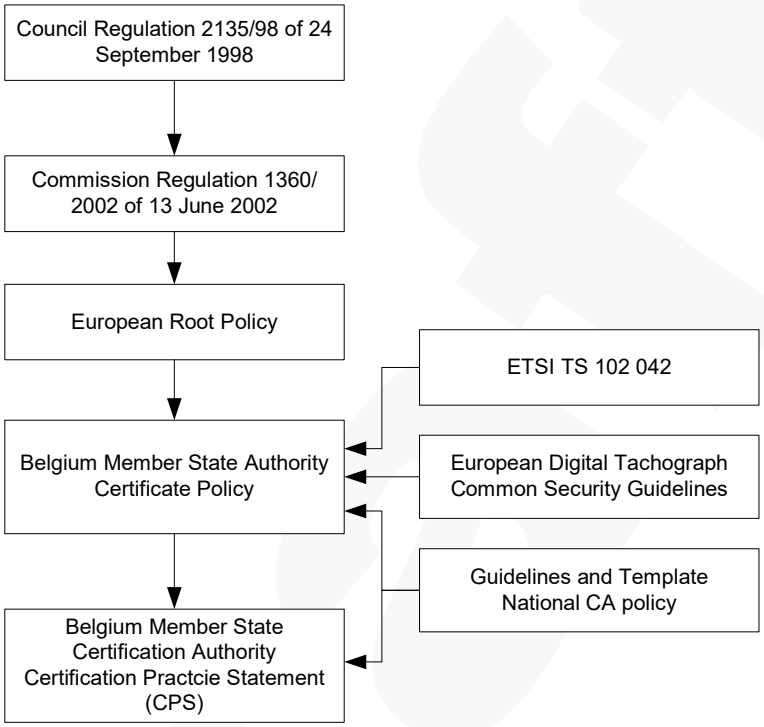

Figure 3 Tachograph system policy components

At a European level the European Root Policy sets out the conditions to be followed by member state authorities with competence over the Tachograph system within their respective states. Within Belgium this B-MSA CP provides guidance with regard to the conditions prevailing in the lifecycle management of the Tachograph system components. The B-MSCA CPS stipulates the conditions for the lifecycle management of certificates and components of the Tachograph system in Belgium.

Normative input is provided through the Council and Commission's Regulations. Additionally normative input is provided through the ETSI TS 102 042 standard, the European Digital Tachograph Security guidelines and the Guidelines and Template for National CA Policy.

3 GENERAL PROVISIONS

This section contains provisions relating to the respective obligations of B-MSA, B-CIA, B-MSCA, B-CP and users, and other issues pertaining to law

and dispute resolution. Discreet references to the B-MSA are made in order to meet with the requirements of the operational environment.

3.1 Obligations

This section contains provisions relating to the respective obligations of the:

- B-MSA
- B-CIA
- B-MSCA
- B-CP
- End Users (Cardholders, VU manufacturers and Motion Sensor manufacturers)

3.1.1 B-MSA and B-CIA obligations

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

The B-MSA shall:

a) Maintain the Belgian MSA Policy.
b) Appoint a B-MSCA and a B-CP.
c) Audit the appointed B-MSCA and B-CP.
d) Approve the Certification Practice Statement of the B-MSCA and the B-CP.
e) Inform the appointed parties on this policy.
f) Inform the VU manufacturers and the Motion Sensor manufacturers about this policy.
g) Submit this policy to the European Commission to seek approval.

The CIA shall:

a) Ensure that correct and pertinent user information is input to the B-MSCA and the B-CP
b) Inform the end users of the requirements in this policy certificate policy connected to the use of the system, i.e. the Cardholders, the VU manufacturers and the Motion Sensor manufacturers
c) Make certificate status information available on Tachonet or through any other appropriate mechanism approved by ERCA.

3.1.2 B-MSCA obligations

The appointed B-MSCA shall:

a) Follow this Belgian MSA Policy
b) Publish a B-MSCA Practice Statement that includes reference to this Belgian MSA Policy and which is to be approved by the B-MSA.
c) Implement the requirements specified in the B-MSCA Certification Practice Statement.

d) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the Belgian MSA Policy, in particular to bear the risk of liability damages.

The B-MSCA has the responsibility for conformance with the procedures prescribed in this certificate policy, also when subcontractors undertake certain functions pertaining to the role of the B-MSCA in part or whole. The B-MSCA will make certificate status information available for publication or through any other appropriate mechanism approved by ERCA..

The B-MSCA has no further obligations.

3.1.3 B-CP obligations

The appointed card personalization organization (herein under, B-CP) shall:

a) Follow this Belgian CA certificate policy

b) Publish a B-CP Practice Statement (B-CP PS) that includes reference to this Belgian MSA Policy and which is to be approved by the B-MSA.

c) Maintains sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National CA certificate policy, in particular to bear the risk of liability damages.

The B-CP shall ensure that all requirements on the BCP addressed in this Belgian certificate policy are implemented as appropriate.

The B-CP has the responsibility for conformance to the procedures prescribed in this certificate policy, even when subcontractors undertake B-CP functionalities.

3.1.4 Cardholder obligations

The B-CIA obliges, through agreement (see 5.1.2), the user (or the user's organization) to fulfil the following requirements:

a) To submit accurate and complete information to the B-CIA in line with the requirements on registration or any other requirements set out in this certificate policy.

b) To use the keys and certificates only within the Tachograph system.

c) To use the Tachograph cards only within the Tachograph system.

d) To refrain from and - take precautions against unauthorized use of the equipment, including the Tachograph private key and the Tachograph card.

e) To use only his personal keys, certificate and card (Regulation14.4.a).

f) To only have one valid driver card at any time (Regulation14.4.a);

g) A user may only under very special, and duly justified, circumstances have both a workshop card and a hauling company card (Annex 1B VI:1); or both a workshop card and a driver card; or several workshop

cards. The possession of multiple Tachograph cards has to be duly justified by the circumstances and it might be subject to specific authorisation by the designated member state authority in Belgium.

h) To refrain from using a damaged or expired card (Regulation14.4.a)

i) To promptly notify the B-CIA up to the end of the validity period indicated in the certificate if:

- The equipment private key or card has been lost, stolen or potentially compromised (Regulation15.1); or
- The certificate content is, or becomes, inaccurate.

3.1.5 VU manufacturers' obligations (role as personalization organization)

The B-MSA shall oblige, through agreement (see 5.1.2), the VU manufacturers to ensure that the following obligations are fulfilled:

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

b) the keys and certificates are only used in the Tachograph system.

c) the equipment private key is only used within the VU.

d) reasonable care is exercised to avoid unauthorized use of the equipment private key.

e) notify the B-MSA without any unreasonable delay, if any of the following occur until the end of the validity period of a certificate:

- The private key of the equipment has been lost, stolen, potentially compromised.
- The certificate content is, or knowingly becomes, inaccurate.

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

The B-MSA shall oblige, through agreement (see 5.1.2), the Motion Sensor manufacturers to ensure that the following conditions are fulfilled:

a) accurate and complete information is submitted to the B-MSA in accordance with the requirements of this policy, particularly with regards to registration.

b) the keys are only used in the Tachograph system.

c) notify the B-MSA without any unreasonable delay if the secret key has been lost or destroyed.

3.1.7 Relying parties

Within the Tachograph system parties that rely on certificates (relying parties) validate certificates by using directories or blacklist services. Blacklist service contains information on revoked or expired certificates and equipment or devices that are used within the Tachograph system. Blacklists follow the requirements for a Certificate Revocation List (CRL).Relying parties accept the terms of use of certificates included in the B-MSCA Certification Practice Statement.

3.2 Liability

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

Liability towards end users is dealt with by of the MSA and CIA.

The B-MSCA bears the responsibility for the proper execution of its tasks, even if it uses subcontractors in part or wholly. If subcontractors are used the B-MSCA informs the B-MSA thereof and provides it with all resources necessary for the B-MSA to meet its obligations.

The B-CP bears the responsibility for proper execution of its tasks, even if it subcontracts other parties for the execution of all or some of these tasks.

If the B-CP uses subcontractors it informs the B-MSA thereof and provides it with access to necessary resources in a way that the B-MSA meets its obligations.

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

With regard to Tachograph certificates the B-MSCA warrants that:

a. The information contained in the certificate at the time of issuance is accurate and the same as the information delivered to the B-MSCA by the B-MSA.

b. The certificate contains all information required for a Tachograph certificate at the time of issuance. The B-CIA warrants correct input to the B-MSCA.

c. The B-CP holds the private key corresponding to the public key identified in the certificate request. The B-CP takes all precautions necessary to ensure correct input to the B-MSCA.

The B-MSCA issues a certificate only if it has received both an Equipment Key Certification Request (EQT.KCR) from the B-CP and a corresponding Equipment Key Certification Authorisation (EQT.KCA) from the B-MSA.

The B-MSCA takes adequate measures to meet its potential responsibilities, resulting from its activities, in particular to risk, including any financial risk, as

a result of liability for damages. The B-MSCA has adequate financial means and stability at its disposal to meet the requirements in accordance with this certificate policy.
If the B-MSCA reorganises its service delivery in a way that makes additional resources necessary it seeks approval of any such changes by the B-MSA. Should the B-MSA approve the proposed changes, the B-MSCA makes additional resources available to all implicated parties.

The B-CP takes adequate measures to cover responsibilities, resulting from its activities, in particular to cover the (financial) risk resulting from liability for damages. The B-CP has adequate financial means and stability to fulfil the requirements in accordance with this certificate policy.

If the B-CP reorganises its service delivery in a way that makes additional resources necessary it seeks approval of any such changes by the B-MSA. Should the B-MSA approve the proposed changes, the B-CP makes additional resources available to all implicated parties.

Additional limitations of warranties from the Certification Practice Statement might apply.

3.2.1 Limitations of Liability

Within the limits permitted by law the total liability of the CA is limited in accordance with the provision of section 3.1.2 of this certificate policy.

3.2.2 Severability

If any provision of this certificate policy, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder is interpreted in such manner as to reflect the original intention of the parties.

3.2.3 Governing Law

This B-MSA certificate policy is governed by the laws of Belgium.

3.3 Miscellaneous Provisions

The certificate policy incorporates by reference the following information:

- Terms and conditions in this certificate policy.
- Any other applicable certificate policy including the ERCA certificate policy.
- The mandatory elements of applicable standards and mandated elements of the Tachograph system.
- Any non-mandatory but customised elements of applicable standards.
- Content of certificates not addressed elsewhere.
- Any other information that is indicated to be so in a field of a certificate.

3.4 Confidentiality and personal data

Confidentiality is restricted according to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the

movement of such data. The Tachograph services also meet the requirements of the Belgian law of 8 December, 1992, on privacy protection in relation to the processing of personal data as modified by the law of 11 December 1998, implementing the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 p. 0031 – 0050). The Tachograph services also meet the requirements of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. This legislation specifies that a person or organization, which collects personal identifiable information, is required to:

- Obtain the consent of the person whose personal data is collected.
- Collect only such personal data that are relevant, adequate and accurate for the purpose of the processing.
- Collect personal data only for specified, explicit and legitimate purposes for a period of time not longer than needed to carry out the scope of the processing.
- Permit end users to request and amend information held about them.

With regard to personal data, further information can be obtained at the address provided elsewhere in this certificate policy. Additional assertions apply to services delivered by the B-MSCA.

3.4.1 Types of information to keep confidential

The B-MSCA and the B-CP treat as confidential the following types of information:

- Any personal or corporate information held by the B-MSCA and the B-CP that is not featured on issued cards or certificates is considered confidential, and shall not be released without the prior consent of the user, nor (where applicable) without prior consent of the user's employer or representative, unless required otherwise by Law. Private keys and secret used by the B-MSCA or the B-CP under this certificate policy.
- Private and secret keys used within VU manufacturers under this certificate policy.
- Private and secret keys used by Motion Sensor manufacturers under this certificate policy.
- Any audit logs and records

In addition to the above the B-MSCA and B-CP consider confidential all:

- Transaction records.

- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of the B-MSCA infrastructure, certificate management and request services and data.

3.4.1.1 Disclosure of confidential information

The B-MSCA and the B-CP do not release nor is it required to release any confidential information without an authenticated and justified request specifying, as applicable:

- The party to whom the B-MSCA and the B-CP owes a duty to keep information confidential
- The party requesting such information;
- A court order.

Confidential information is not released without the prior consent of the user, or (where applicable) the prior consent of the user's employer or representative, unless required otherwise by Law.

Parties requesting and receiving confidential information are granted permission on the explicit assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

3.4.1.2 Confidential communications

All communications of personal or confidential information are encrypted including:

- The communications link between the B-MSCA, B-CP and B-CIA.
- Sessions to deliver certificate validation information.

3.4.2 Types of information not considered confidential

Certificate content and status information on a certificate are not confidential and can be accessed by authorised parties through appropriate directories. Identification information or other personal or corporate information appearing on cards and in certificates is not considered confidential, except as otherwise provided by Law.

3.4.2.1 Accessing non confidential information

Non-confidential information can be disclosed to any user and relying party under the conditions below:

- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult non-confidential information the B-MSCA holds.

4 PRACTICE STATEMENT (PS)

The B-MSCA and the B-CP have statements of the practices and procedures, called Certification Practice Statement[2], that are used to address all the requirements identified in the Belgian MSA Policy. The Certification Practice Statement is subject to approval by the B-MSA. In particular:

a) The Certification Practice Statement shall identify the obligations of all external organizations supporting B-MSCA and B-CP services including the applicable policies and practices.

b) The Certification Practice Statement shall be made available to the B-MSA, to users of the Tachograph system, and to third parties (e.g. control bodies). The Certification Practice Statement of the B-MSCA and the B-CP does not necessarily make all details on practices publicly available to all users. Additional information regarding the policies and practices of the B-MSCA and the B-CP can be sought directly through the communication address provided elsewhere in this document.

c) The management of the B-MSCA and the B-CP ensures that the Certification Practice Statement is properly implemented.

d) The Certification Practice Statement of the B-MSCA and the B-CP shall define a review process.

e) The B-MSCA and the B-CP shall give due notice on changes they make to the Certification Practice Statement and following approval make the revised certificate policy immediately available. Minor revisions may be released without B-MSA approval.

f) An approved Certification Practice Statement meets the requirements of ERCA and the B-MSA. Additional policy limitations might apply as stipulated by Law or through agreements with MSAs from other member states.

The Certification Practice Statement becomes binding for the applicant of the service, pursuant to an application for service according to the forms to be found under: http://www.digitach.be

4.1 Review process

A maintenance process aims at handling updates of the Certification Practice Statement. Any updates become binding for all certificates that have been issued or are due to be issued within 30 days after the date of the publication of the updated version of the Certification Practice Statement.

[2] The statements of practices and procedures of B-MSA, the B-MSCA and B-CP are consolidated in one single Practice Statement document managed by the B-MSCA.

4.1.1 Versions

Changes are indicated through versions numbers, being a number code composed by an integer and a decimal number. Minor changes are indicated by a change of the decimal number. Minor changes include without limitation, editorial changes, or any change that does not materially affect the content of this Certificate Policy or the interpreattion thereof. The Policy Management Authority has competence to classify changes as minor or otherwise. Changes are also indicated by a publication date.

4.1.2 Policy updates

B-MSCA and B-CP management and/or contractors contribute to the updates of the Certification Practice Statement.

4.1.3 Policy Management Authority

New versions and updates of the Certification Practice Statement are approved by a Policy Management Board. The Policy Management Board consists of the following parties:

- One member representing each organisation being the B-MSA, the B-MSCA and the B-CP. Members must be involved in the management of the respective organisations or in the project management for the Tachograph system.
- At least one agent directly involved in the drafting and development of the Certification Practice Statement.

The representative of the B-MSA chairs the Policy Management Board.

All members of the Policy Management Board have one vote. There are no other voting rights reserved for any other party. In case of lock vote the vote of the Chairperson of the Policy Management Board i.e. the representative of the B-MSA counts double.

5 EQUIPMENT MANAGEMENT

The equipment in the Tachograph system includes the following items:

- Tachograph cards
- Vehicle units
- Motion Sensors

The equipment is handled and managed by several parties acting under the following discreet roles:

- B-CIA: having competence over the entire life cycle of the certificates used, including registration for new cards and certificates, requests for certificate or card renewal, certificate suspension, certificate revocation, card deactivation, etc.
- B-MSCA; being the certification authority with competence over the designation of certificates, key pairs, maintaining the Certificate Revocation List (CRL), etc.
- B-CP: with competence over smart card personalisation including visual and electronic personalization, distribution, deactivation etc.
- VU manufacturers and Motion Sensor manufacturers

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

- Quality control (type approval)

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

- Applications for cards, VU certificates and Motion sensor keys
- Application approval registration
- Equipment registration and data storage (DB)

The following functions are carried out by the B-MSCA and the B-CP:

- Quality control (sample tests)
- Key insertion
- Personalization of cards
- Distribution

The following functions are carried out by the VU manufacturers :

- Personalization of VU units
- Motion Sensor key insertion
- Distribution

The following functions are carried out by the Motion Sensor manufacturers :

- Motion Sensor key insertion
- Distribution

5.1 Tachograph cards

5.1.1 Quality control

The MSCA/CP shall ensure that only type approved cards according to the Regulation are personalized in the Tachograph system. See also 5.1.7.5

5.1.2 Application for card – handled by the B-CIA

The B-CIA shall inform the user of the terms and conditions regarding the use of the card. This information is available in a readily understandable language being Dutch, French and German.

By applying for a card, and accepting delivery of the card, the end user shall accept the terms and conditions set out in this certificate policy.

A replacement card shall have the same card expiration date as the replaced one. If, however, the remaining validity period of the replaced card is less than 2 months the card shall be renewed instead of replaced.

5.1.2.1 User application

Applicants for a Tachograph card shall fill out an application form. The content of the application is determined by the B-MSA. To have a card issued the following information is required unless it can be collected from other sources:

Driver card specific:

- Gender;
- Full name (including surname and given names) of the user;
- Date and place (city and country) of birth;
- Place of residence;
- National identification number;
- Postal address;
- Photograph;
- Preferred language;
- Signature;
- Driving license number and category;
- Member State issuing the driving licence;
- Name of the issuing authority;
- Billing address and VAT number (if any).

In case of replacement or renewal of the card:

- Card number.

Workshop card specific:

Workshop cards are issued to natural persons only in their capacity as agents of a legal person authorised to take part in the Tachograph system. Workshop cardholders must provide the following evidence:

- Workshop data:
    - Full name and legal status of the associated legal person or other organizational entity;
    - Abbreviated name;
    - Postal address;
    - Phone number;
    - Fax number;
    - E-mail address;
    - Company identification number [3].
- Card holder data:
    - Gender;
    - Full name (including surname and given names) of the user;
    - Date and place (city and country) of birth, reference to a nationally recognized identity document, or other attributes of the user which may be used to, as far as possible, distinguish the person from others with the same name;
    - Place of residence;
    - National identification number (if any);
    - Agreement number of the card holder;
    - Preferred language.
- Billing address and VAT number (if any).

In case of replacement or renewal of the card:

- Card number.

Control body card specific:

Control body certificates are issued only to natural persons in their capacity as agents of a legal person authorised to take part in the Tachograph system. Control body certificate holders must provide the following information:

- Control body data:
    - Full name and legal status of the associated legal person or Control Body Agency;
    - Postal address;
    - Phone number;

[3] The BCE/KBO (Banque-Carrefour des Entreprises / Kruispuntbank voor ondernemingen) issues a unique identification number for each Belgian company.

- Fax number;
- E-mail address.

In case of replacement or renewal of the card:

- Card number.

Hauling company card specific:

Hauling company certificates are issued only to natural persons in their capacity as agents of a legal person authorised to take part in the Tachograph system. Hauling company certificates holders must provide the following evidence:

- Company data:
  - Full name and legal status of the associated legal person or other organizational entity;
  - Abbreviated name;
  - Postal address;
  - Phone number;
  - Fax number;
  - E-mail address;
  - Company identification number;
  - Amount of cards asked.
- Card holder data:
  - Full name (including surname and given names) of the user;
  - Function;
  - Card delivery postal address;
  - Preferred language;
- Billing data:
  - Full name and legal status of the associated legal person or other organizational entity;
  - VAT number (if any);
  - Postal address.

In case of replacement or renewal of the card:

- Card number.

5.1.2.2 Agreement

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

- the user agrees to the terms and conditions regarding use and handling of the Tachograph card
- the user agrees to, and certifies, that from the time of card acceptance and throughout the operational period of the card, until CIA is notified otherwise by the user:
    - no unauthorized person has ever had access to the user's card
    - all information given by the user to the CIA relevant for the information in the card is true;
    - the card is being conscientiously used in consistence with usage restrictions for the card

5.1.2.3 B-CIA terms of approval - Driver card specific

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

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

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

5.1.3 Card renewal – handled by B-CIA

Workshop cards are valid for no more than one year (Regulation 12.1).

Driver cards are valid for no more than five years (Regulation 14.4.a).

Company cards are valid for no more than five years. Control Cards are valid for no more than five years. A validity period commences on the date of issuance of a card.

An application for renewal follows section 5.1.2

5.1.3.1 Driver cards

The user shall apply for a renewal card at least 15 working days prior to card expiration. (Regulation article 15.1)

If the user complies with the above rule, the B-CIA will issue a new driver card before the current card expires. (Regulation article 14.4.a)

5.1.3.2 Workshop cards

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

The B-CIA will issue a renewal card within 5 working days of receiving a complete application. (Regulation article 12.1)

5.1.3.3 Company cards

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

If the user complies with the above rule, the B-CIA will issue a new company card before the current card expires.

5.1.3.4 Control cards

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

The B-CIA will issue a renewal card within 5 working days of receiving a complete application.

5.1.4 Card update or exchange – handled by the B-CIA

A user who changes country of residence may request to have his/her driver card exchanged.

If the current card is valid, the user shall only show proof of residence in order to have the application granted.

The CIA shall upon delivery of the new card take possession of the previous card and send it to the MSA of origin. (Regulation article 14.4.c)

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

5.1.5 Replacement of lost, stolen, damaged and malfunctioned cards – handled by the B-CIA

If a card has been lost or stolen, the user shall report this to the local Police and receive a copy of the report. Loss of card may be reported by the user, or

by the Police upon receiving a found card. The Police shall without delay notify the issuing CIA of the report.

Stolen and lost cards are reported on a directory put on a blacklist accessible by all Member States authorities.

Damaged and malfunctioning cards are delivered to the issuing B-CIA. They are subsequently visually and electronically cancelled and reported on a directory.

If the card is lost, stolen, damaged or malfunctioning, the user applies for a replacement card within 7 days. (Regulation article 15.1)

The B-CIA issues a replacement card with new key pairs and certificate within 5 working days from receiving a request. (Regulation article 14.4.a)

The replacement card has the same validity period as the card that has been lost or stolen, unless the card has less than two months remaining validity, in which case a replacement card is issued instead. (Regulation Annex 1B: VII).

5.1.6 Application approval registration – handled by the B-CIA

The B-CIA registers approved requests for certificates and card applications in a data-store that is made accessible to the B-MSCA and the B-CP. This information will be used as input to the certificate generation and card personalization.

5.1.7 Card personalization – handled by the B-CP

5.1.7.1 Visual personalization

Cards are personalized both visually and electronically.
Cards are visually personalized according to Regulation Annex 1B, section IV.

5.1.7.2 User data entry

Data is inserted in the card according to the structure given in Regulation Annex 1B, appendix 2, rules TCS_403, TCS_408, TCS_413 and TCS_418, depending on card type.

5.1.7.3 Key entry

The private key will be created in a way that no person, in any way whatsoever, can get control of the generated private key. See also equipment key management, 7.2.

5.1.7.4 Certificate entry

The user certificate is loaded on the card prior to delivering the card to the user.

5.1.7.5 Quality Control

Documented control procedures are implemented to ensure that visual and electronic information in issued user's cards and certificates match with the validated owner and meet all appropriate requirements.

5.1.7.6 Cancellation (destruction) of non-distributed cards

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

All destroyed cards shall be registered in a cancellation blacklist (CRL).

5.1.8 Card registration and data storage (DB) – handled by the B-CP and the B-CIA

The B-CP I cards with card numbers and card users. This linkage data is transferred from the B-CP to the B-CIA in a secure way.

5.1.9 Card distribution to the user – handled by the B-CP

a) The personalisation cards are kept in a secure and safe environment. ISO 9000/2000 documented procedures are implemented for the exception handling, including outages in the production process, failure of delivery, and loss of or damage to cards.
b) Personalized cards are immediately transferred to the place where they are delivered or distributed to the user, i.e. a controlled area.
c) Personalized cards shall always be kept separate from non-personalized cards.
d) The Tachograph cards shall be distributed in a manner that offers a reasonable guarantee of delivery to the end user.
e) The pin code of a workshop card is distributed in a manner that minimizes the risk of unauthorized persons accessing the code without it being noticed by the end user.
f) At the point of delivery of a workshop card to a user, proof of that user's identity (e.g. name) is checked against a natural person.

5.1.10 Authentication codes (PIN) – generated by the B-CP

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

PIN codes consist of 6 digits (Regulation Annex 1B, App 10: Vehicle Units:4.1.2).

5.1.10.1 PIN generation

PIN codes are generated in a secure system, securely transferred to workshop cards, and direct-printed to PIN-envelopes. PIN codes are never stored on a computer system in a manner that allows connection between PIN and user. The PIN generation system meets the requirements FIPS 140-2 (or 140-1) level 3 or higher [FIPS]].

5.1.10.2 PIN distribution

At the point of delivery of the pin codes to a user, proof of that user's identity (e.g. name) is checked against a natural person.

PIN codes are distributed through registered mail and in connection with the corresponding cards.

5.1.11 Card deactivation – handled by B-MSA/B-CIA and B-CP

The B-CIA may permanently deactivate cards and key pairs by using dedicated equipment and keeping appropriate records of its actions. The B-CIA may permanently deactivate a card and any keys residing thereon. A decision of deactivation is taken and carried out by the B-MSA or the B-CIA, but the actual operation is carried out by the B-CP.

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

Deactivation of cards is registered in the card database and the card number is recorded on a blacklist (CRL).

5.2 Vehicle Units and Motion Sensors

5.2.1 Quality control - B-CIA function

The B-CIA ensures that certificates (and encrypted motion sensor data) are issued only to type approved VU (and Motion Sensors).

5.2.2 VU and Motion Sensor application/registration process– handled by the B-CIA

For VU manufacturers the request procedure for certificates is the same as for Tachograph cards. Motion Sensor manufacturers request Motion Sensor keys.

5.2.2.1 Vehicle Units

At the registration phase, the B-CIA ensures that the evidence of a VU identity is properly established.

VU manufacturers may apply for certificates that will be used in vehicle units that have not been previously identified, however, mapping between VU-identity and certificate is promptly added to the registration (Regulation Annex 1B, Appendix 11: 3.3.1).

The B-CIA informs the manufacturer of the terms and conditions regarding the use of a certificate in a readily understandable language, being Dutch, French and German

By making an application for a certificate and accepting delivery of the certificate the manufacturer enters an agreement with B-MSA, accepting the pertaining terms and conditions. The manufacturer provides a postal address, or other contact details as appropriate.

5.2.2.2 Motion Sensors

Manufacturers request the B-CIA for their respective Motion Sensor keys. This request is treated as a certificate request. Motion sensor data such as serial number and manufacturer are stored in a database.

5.2.3 Application approval registration – handled by the B-CIA

The B-CIA registers approved applications in a database. The data from this database is made available to the B-CP as input for the certificate generation process.

5.2.4 VU certificate registration and storage (DB) – handled by the B-CIA and the B-MSCA

The B-CP is responsible for registering which certificate is issued to which VU or VU certificate request. The B-CIA is responsible for maintaining the database mapping VUs and certificates.

5.2.5 VU personalization – handled by the VU manufacturers

VUs are personalized by inserting the VU certificate and keys. It is expected that in most cases this task will be handled by VU manufacturers, but the regulation allows for the task being handled by special equipment personalizers or even by the B-MSCA (Regulation Annex 1B, appendix 11:3.1.1).

5.2.5.1 Key entry

The private RSA is inserted in the VU without ever leaving the key generation environment. This environment must guarantee that no person, in any way whatsoever, can get control of the generated private key without detection. The symmetric key Km_{VU} is inserted in the VU in a safe manner. See also equipment key management 6.5.

5.2.5.2 Certificate entry

The user certificate is loaded in the VU in a way that maintains its integrity.

5.2.6 VU and Motion Sensor keys and certificate distribution to equipment manufacturers– handled by B-MSCA

B-MSCA is responsible for the distribution of keys and certificates for the VUs and Motion Sensors to the respective manufacturers in a secure way.

5.2.7 VU distribution – handled by VU manufacturers

VU distribution is the responsibility of the VU manufacturers.

5.2.8 VU renewal

A VU may be replaced due to malfunction, damage, theft etc.

5.2.9 Replacement of lost, stolen, damaged or malfunctioning VUs

Replacement of a VU follows the practices for requesting a new VU.

If a VU has been lost or stolen, the driver or vehicle user shall report this to the local Police and receive a copy of the report. Loss of VU may be reported by the driver or vehicle user, or by the Police upon receiving a found card.

Stolen or lost VUs should be registered in a blacklist to be distributed to all Member States. This is a task of the CIA.

5.2.10 End of life of VUs

End of life of VUs have their keys and certificates destroyed.

Destruction of a VU is registered by the B-CIA in the country of issuing.

6 ROOT KEYS MANAGEMENT: EUROPEAN ROOT KEY, BELGIAN KEYS, MOTION SENSOR KEYS

This section contains provisions for the management of

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

The ERCA certificate public key is used to sign the certificate issued to the B-MSCA.

The B-MSCA keys are the Member State signing keys for Belgium and may also be called Member State Belgium root keys.

Motion Sensor keys are symmetric keys placed on the workshop card, VU and Motion Sensor for authentication. The B-MSCA receives the Motion Sensor keys from the ERCA and distributes them to the manufacturers.

Transport keys are the symmetric keys used for securely exchanging information between the ERCA and the B-MSCA.

Any other cryptographic keys than the above, that the B-MSCA might need are not part of the Tachograph system and are not dealt with in this policy.

The B-MSA shall follow the procedure, formats and/or media prescribed by ERCA in:

- Submitting MSCA public keys for certification by the ERCA
- Requesting motion sensor master keys from the ERCA
- Transporting the key and certificate

The B-MSCA ensures that the Key Identifier (KID) and modulus (n) of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of the B-MSCA.

The B-MSA recognizes the ERCA public key in the prescribed distribution format.
The B-MSCA follows strict audited guidelines with regard to the practices and operations associated with key management. For all keys it issues (i.e. B-MSA keys, being B-MSCA keys for vehicle units and B-MSCA keys for the Tachograph cards, as well as the Motion sensor Transport keys) the following policies apply:

- B-MSCA Key Management policy
- B-MSCA Key Management procedures
- B-MSCA Security Policy

The above-mentioned policies have been audited for integrity and compliance according to strict criteria set out by the Belgian federal government and address in particular the following requirements:

Transportation of private keys during key certification request is forbidden.

6.1 ERCA public key

The B-MSCA ensures the integrity and availability of the ERCA public key (EUR.PK) at all times.

The B-CP ensures that EUR.PK is inserted in all Tachograph cards.

Vehicle Unit Manufacturers have to ensure that EUR.PK is inserted in all vehicle units of their domain.

6.2 Member State key pair of the B-MSCA

The Member State keys are the B-MSCA signing key pair(s), which is used to sign all equipment certificates.
The key pair consists of a public key (MS.PK) and a private, or secret, key (MS.SK).
The B-MSCA generates its own key pair and submits it to ERCA for certification. The MSCA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times. If the EUR.PK is stored in the B-CP, the same rule applies.

The B-MSCA ensures that the keys are not used for any other purposes than signing Tachograph equipment with the exception of the production of the ERCA key certification request as described in ERCA CP, Annex A.

The B-MSA signs equipment certificates within the same device used to store the Member State Private Keys.

6.2.1 Key pair generation of the B-MSCA

The B-MSA Key Pair generation takes place in a physically secured environment by personnel in trusted roles under, at least dual control.

The Key pair of the B-MSCA is generated in a device which either:

- Meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]].
- Meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]].
- Is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC]], to E3 or higher in ITSEC, or equivalent security criteria. This is a security target or protection profile that meets the requirements of this certificate policy based on risk

analysis and taking into account physical and other non-technical security measures.

A key generation device is a stand alone one and meets the requirements stated in the B-MSCA Certification Practice Statement.

The key generation system should be stand-alone

The actual device used and requirements met are publicised through the B-MSCA Certification Practice Statement.

The B-MSCA key-pair generation requires the active participation of three separate actors. At least one of them has a role as CAA/PA (a certification authority/ personalization administrator) and the remaining have trusted roles (see section 9.3.1 for role descriptions).

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

Because ERCA may not be able to issue replacement Member State certificates rapidly, to ensure business continuity, the B-MSCA may have more than one Member State key pairs with associated signing certificates. The B-MSCA has at least two (2) and maximum five (5) Member State key pairs with associated signing certificates.

6.2.2 Member State keys' period of validity

The maximum usage period of private keys is set to two (2) years starting from the issuance of a certificate by ERCA certifying the corresponding public key...

The corresponding public key will have no end of validity..

6.2.3 B-MSCA Member State private key storage

The operational private keys are contained in and operated from inside a tamper resistant device that:

- Meets the requirements of FIPS 140-2 (or 140-1) level 3 or higher [FIPS]].
- Is a trustworthy system, assured to EAL 4 or higher level in accordance with ISO 15408 [CC]], to E3 or higher in ITSEC, or equivalent security criteria. There are security targets or protection profiles that meet the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

Dual control is required to access the B-MSCA private signing keys.

6.2.4 B-MSCA private key backup

The B-MSCA private signing keys may be backed up, using a key recovery procedure requiring at least dual control. The procedure used is specified in the Certification Practice Statement of B-MSCA.

6.2.5 Member State private key escrow

The private signing keys for Belgium are not subjected to key escrow.

6.2.6 Member State keys compromise

If the private keys for Belgium are considered or suspected to be compromised documented guidelines outline the measures to be taken by users and security staff at the B-MSCA.

In such case the B-MSCA informs the B-MSA, ERCA and all other MSCAs.

6.2.7 Member State keys end of life

The B-MSCA has documented procedures to ensure that it always has a valid, certified signing key pair for Belgium.

Upon termination of use, the MSCA signing keys are unloaded from the online production chain and are stored offline in a secure environment under dual control and split knowledge.

The online production system software is designed to prevent use of expired keys by checking validity and usability periods of MSCA keys prior to end entity certificate issuance.

The B-MSCA applies procedures to ensure that at end of life keys are handled in a physically secured environment by personnel in trusted roles under, at least dual control. Additional conditions apply as prescribed in the B-MSCA:

- B-MSCA Key Management policy
- B-MSCA Key Management procedures
- B-MSCA Security Policy

6.3 Motion Sensor keys

The B-MSCA requests ERCA for motion sensor key(s). (Regulation Annex 1B, app 11:3.1.3).

Upon manufacturer request, the B-MSCA encrypts Motion Sensor data (pairing key K_P and extended serial number N_S) with Km (Regulation Annex 1B, app 11:3.1.3). Km is only used to encrypt motion sensor data for the purpose of motion sensor manufacturers.

The motion sensor master key (Km) will never leave the secure and controlled environment of the MSA.

The ERCA will deliver an encrypted version of the Vehicle Unit Symmetric Key KM_{vu} through a KDM (Key Distribution Message) created from the Vehicle Unit Manufacturer KDR (Key Distribution Request) as per European Root Policy Version Annex D. The B-MSCA forwards the received KDM to manufacturers of Vehicle Units for insertion into the VU (Regulation Annex 1B, app 22:3.1.3).

The ERCA will deliver an encrypted version of the Workshop Card Symmetric Key KM_{wc} through a KDM created from the B-CP KDR as per European Root Policy Version Annex D. The B-MSCA forwards the received KDM to the B-CP for insertion within theWorkshop cards.

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

During storage, use and distribution the B-MSCA and/or the B-CP protect the motion sensor keys with high assurance physical and logical security controls. The keys are stored in a specific tamper resistant device which:

- Meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS] (FIPS 140-1 Level4 for the B-CP HSM).
- Is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC]], to E3 or higher in ITSEC, or equivalent security criteria. This will be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

6.4 Transport keys

The B-MSA Transport Key Pair generation takes place in a physically secured environment by personnel in trusted roles under, at least dual control.
Member State Key Pairs for motion sensor master key distribution (transport keys) shall be generated and stored within a device which is either:

- certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher;
- or is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2; or is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 to level E3 or higher in ITSEC [12] or equivalent security criteria; or demonstrated to provide an equivalent level of security.

The Key Distribution Requests (KDR) need accordingly to be generated by the Component Personalizer (CP) (Vehicle Unit manufacturers or Tachograph Cards manufacturers). The MSCA will validate the CP KDR by checking conformity as per European Root Policy Annex D and forward it to the BCA for further processing by ERCA. The ERCA shall ensure that MSCA public key certification requests and motion sensor master key distribution requests are complete, accurate, and duly authorized.

The resulting Key Distribution Message (KDM) will be returned to the MSCA that will hand it over to the CP without validation or processing.

As such it is the component personalizer responsibility to have the necessary tools in its possession to generate KDRs according to the specifications and to process the KDMs up to their production environment.

7 EQUIPMENT KEYS (ASYMMETRIC)

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

- Tachograph cards
- Vehicle Units

Symmetric Motion Sensor keys are not handled here.

7.1 General aspects B-CP/ B-MSCA and VU manufacturers

Equipment (Card and VU) initialisation, key loading and personalisation are carried out in a physically secure and controlled area. Entry to this area is strictly controlled and requires the presence of minimum two persons to operate the system. A log file is compiled with reference to the entries and the actions in the system.

No sensitive information contained in the key generation systems may leave the system unless as provided in this certificate policy.

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

VU/Motion Sensor: No sensitive information in the VU personalization system may leave the system unless as provided in this certificate policy.

B-CP and VU manufacturers must ensure the uniqueness of the equipment serial number within their domain (Manufacturer Code) when generating the 'Certificate Content' for certificate request to the B-MSCA. The B-MSCA will check Certificate Holder Reference (CHR) identifier for uniqueness within its domain and reject any request for a duplicate CHR.

Organizations (Subcontractors) that carry out key generation and card personalization on behalf of more than one Member State separate the processes for each one of them. A log is kept of each individual process and the B-MSA has access to it on request.

VU manufacturers that perform VU personalization separate this process from VU production. Logs are kept of the personalization and the relevant B-MSA has access to it on request.

B-MSCA/B-CP /VU manufacturers: Logs of the personalisation system contain a reference to the order, and list the corresponding equipment numbers and certificates. The B-MSA has access to it.

7.2 Equipment key generation

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

The entity that performs the key generation makes sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret. Key generation is carried out within a device which either:

- Meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]].
- Meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]].
- Is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC]], to E3 or higher in ITSEC, or equivalent security criteria. This is assured be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

Keys are generated using the RSA algorithm having a key length of modulus *n* 1024 bits. (Annex 1B, Appendix 11:2.1/3.2)

The generation procedure and storage of the private key prevents it from being exposed outside of the system that created it. Furthermore, it is erased from the system immediately after having been inserted in the VU.

The key generation entity undertakes adequate measures to ensure that the public key is unique within its domain before certificate binding takes place.

7.2.1.1 Batch key generation

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

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

7.2.2 Equipment key validity

7.2.2.1 Keys on cards

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

7.2.2.2 Vehicle units

The private key of the Vehicle Unit will not be valid beyond the lifetime of the Vehicle Unit itself.

7.2.3 Equipment private key protection and storage - Cards

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

Copies of the private key may only be kept on the Tachograph card.

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

7.2.4 Equipment private key protection and storage – VUs

The VU manufacturer ensures that the VU private key, and the corresponding means of its usage, are protected by, and restricted to, a VU.

Copies of the private key may only be kept in the VU unless required during key generation and device personalization.

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

7.2.5 Equipment private key escrow and archival

Equipment private keys neither is escrowed nor archived.

7.2.6 Equipment public key archival

All certified public keys are archived by the certifying B-MSCA.

7.2.7 Equipment keys end of life

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

Upon termination of use of a Vehicle Unit, the public key is archived, and the private key is destroyed in a way that the private key cannot be retrieved.

8 EQUIPMENT CERTIFICATE MANAGEMENT

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

8.1 Data input

8.1.1 Tachograph cards

Cardholding users have their certificates issued on the basis of information submitted with the application for a Tachograph card (section 5.1.2) and captured from a B-CIA register. The cardholders' public key is generated on board of the card at the key generation process.

The B-CP ensures that input data contains information that renders the Certificate Holder Reference unique. The B-MSCA ensures the uniqueness of the Certificate Holder Reference within its own domain.

8.1.2 Vehicle units

Manufacturers (or their representatives) of vehicle units must apply for certificates according to section entitled VU and Motion Sensor application/registration.
The B-CP ensures that the registration data contains information that renders the Certificate Holder Reference (CHR) unique. The B-MSCA verifies the uniqueness of CHR within its domain.

If the equipment key pair is not generated by the B-MSCA, the certificate request process ensures that the manufacturer has possession of the private key associated with the public key presented for certification.

8.2 Tachograph card certificates

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

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

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

Hauling company certificates are issued only to successful applicants for a Hauling Company card.

8.3 Vehicle unit certificates

Vehicle unit certificates are issued to the VU manufacturer by the B-MSCA in the country of Type approval, and only to type approved VUs.

Vehicle unit certificates are issued only to manufacturers, and evidence must be provided of:

- Identifier of the device by which it may be referenced (e.g. type approval and serial number), or a Certificate Request Identifier, if the device is not identified.
- Full name of the manufacturer.
- A nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the manufacturer from others with the same name.
- The registering representative's association with the manufacturer.

8.4 Equipment certificate time of validity

Certificates always have a finite validity period, which is equal to or shorter than the corresponding hardware equipment (section 5):

- Driver certificates have a maximum validity of not more than 5 years (Regulation 14.4.a).
- Workshop certificates have a maximum validity of 1 year (Regulation 12.1).
- Control body certificates have a maximum validity of 5 years.
- Hauling company certificates have a maximum validity of 5 years.
- Vehicle Unit certificates have an undefined end of validity.

8.5 Equipment certificate issuing

The B-MSCA ensures the authenticity and integrity of the certificates it issues.

8.6 Equipment certificate renewal and update

See Equipment management (section 5). Certificates and cards have the same validity period; therefore, they are managed together. VU certificates have no expiration date or they have a very long validity period. The lifetime of the equipment is shorter than that of the certificate.

8.7 Dissemination of equipment certificates and information

The B-MSCA exports all card related certificate data to a B-CP register and all VU related certificate data to the B-CIA register so that certificates, equipment and users are connected**.** The B-CIA makes the VU certificate data available for the VU manufacturers.

The B-CIA ensures users, relying parties and other stakeholders that:

- Certificates are made available through an accessible directory.
- Terms and conditions, as well as relevant parts of the B-MSCA certificate policy are made available.

8.8 Equipment certificate use

The Tachograph certificates are only used within the Tachograph system.

8.9 Equipment certificate revocation

Certificates are not revoked. Invalid Tachograph equipment is reported to a blacklist.

8.10 Certificate Content

Within the Tachograph system, public key certificates are built with the following data in the following order:

Data	Format	Bytes	Obs
CPI	INTEGER	1	Certificate profile identifier (¡01¡ for this version)
CAR	OCTET STRING	8	Certification authority reference
CHA	OCTET STRING	7	Certificate holder authorisation
EOV	*TimeReal*	4	Certificate end of validity. Optional, ¡FF¡ padded if not used
CHR	OCTET STRING	8	Certificate holder reference
n	OCTET STRING	128	Public key (modulus)
e	OCTET STRING	8	Public key (public exponent)
		164	

9 B-MSCA AND B-CP INFORMATION SECURITY MANAGEMENT

This section describes the Information Security measures mandated by this policy.
Additional information regarding information security measures can be obtained by the B-MSCA at the address provided elsewhere in this Certificate Policy. Additional information regarding information security guidelines may also be obtained by the B-MSA at the address provided elsewhere in this Certificate Policy. This section may, at least in part, be substituted by Information Security policies for the relevant entities.

9.1 Information security management of the B-MSCA and the B-CP

The B-MSCA and the B-CP ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

The B-MSCA and the B-CP retain the responsibility for all aspects of key certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties are clearly defined by the B-MSCA and the B-CP and appropriate arrangements are made to ensure that third parties are bound to implement any controls required by the B-MSCA and the B-CP. The B-MSCA and the B-CP retain responsibility for the disclosure of relevant practices of all parties.

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

The B-MSCA and the B-CP meet the requirements of the standard ISO 17799 with regard to security management. Formal accreditation is not mandated.

9.2 Asset classification and management of B-MSCA/B-CP

The B-MSCA and the B-CP ensure that their assets and information receive an appropriate level of protection:

- The B-MSCA and the B-CP carry out a risk assessment to evaluate business risks and determine the necessary security requirements levels and procedures.
- The B-MSCA and the B-CP maintain an inventory of all information assets and assign a classification for the protection requirements to those assets consistent with a risk assessment.

9.3 Personnel security controls of B-MSCA/B-CP

9.3.1 Trusted Roles

To carry out their tasks the B-MSCA and the B-CP use personnel in discreet roles that include:

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

The CAA/PA role includes:

a) Key generation;
b) Certificate generation; (Generating signed certificate requests to be processed and executed by the B-MSCA/B-CP equipment according to defined rules)
c) Personalization and secure distribution of equipment;
d) Administrative functions associated with maintaining the B-MSCA/B-CP database and assisting in compromise investigations.

The SA role includes:

a) Performing initial configuration of the system including secure boot start-up and shut down of the system;
b) Initial set up of all new accounts;
c) Setting the initial network configuration;
d) Creating emergency system restart media to recover from catastrophic system loss;
e) Performing system backups, software upgrades and recovery, including the secure storage and distribution of the backups and upgrades to an off-site location. Backups will be performed at least once per week, and the system will be powered on/off after a backup is performed, so that hardware integrity checks are performed.
f) Changing of the host name and/or network address.

The ISSO role includes:

a) Assigning security privileges and access controls of CAA/PAs.
b) Assigning passwords to all new accounts.
c) Performing archiving of required system records

d) Review of the audit log to detect CAA/PA compliance with system security policy. Review of the audit log will be done at least once per week.

e) Personally conducting or supervising an annual inventory of the B-MSCA/B-CP's records.

f) Participating in Member State key generation

Note that the ISSO, who is not directly involved in issuing certificates, performs a supervisory function in examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

9.3.2 Separation of roles

Within the B-MSCA and the B-CP several individuals fill each of the above-mentioned positions and at least one individual is appointed per task.

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.
Where dual control is required at least two trusted members of the B-MSCA staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.
The B-MSCA contains the following distinct work groups:

- The B-MSCA operating personnel that manages operations on certificates.
- Administrative personnel to operate the platform supporting the B-MSCA.
- Security personnel to enforce security measures.

9.3.3 Identification and Authentication for Each Role

Identification and authentication of CAA/PA, SA and ISSO are appropriate and consistent with practices, procedures and conditions stated in this policy.

9.3.4 Background, qualifications, experience, and clearance requirements

The role of CAA/PA (Certification Authority/ Personalization Administrator), requires vetting to ensure its trustworthiness.

The B-MSCA and the B-CP personnel in trusted roles including, at least, all CAA/PA and ISSO (Information System Security Officer):

- Are not assigned duties that may lead to a conflict with their duties and responsibilities as CAA/PA and ISSO.
- Have not been previously relieved of a past assignment for negligence or non-performance of duties.
- Have received proper training to carry out their duties.

- Has the right to work in Belgium (nationality of an EU member state and/or valid employment permit in Belgium)
- Can produce a certificate of good conduct.
- Have no previous criminal conviction for a serious crime.

9.3.5 Training requirements

Personnel have adequate training for the role and the function.

9.4 System security controls of the CA and personalization systems

The B-MSCA and the B-CP shall ensure that the systems are secure and correctly operated, with minimal risk of failure:

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

The Belgian Certification Authority System and Personalization system provide sufficient system security controls for enforcing the separation of roles described in this certificate policy.

The security controls provide access control and traceability to an individual level on all functions affecting the use of the B-MSCA's private issuing keys.

9.4.1 Specific computer security technical requirements

Initialising the system that operates the private certification keys of the B-MSCA requires at least two operators, which are securely authenticated.

9.4.2 Computer security rating

The CA and personalization systems do not require formal rating as long as they fulfil all requirements in this section.

9.4.3 System development controls

The B-MSCA and the B-CP use trustworthy systems and products that are protected against modification.

An analysis of security requirements are carried out at the design and requirements specification stage of any systems development project undertaken by the B-MSCA and the B-CP or on behalf of the B-MSCA and the B-CP to ensure that security is built into IT systems.

Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

9.4.4 Security management controls

The system roles (section 9.3.1) are implemented and enforced.

9.4.5 Network security controls

Controls (e.g., firewalls) are implemented to protect the B-MSCA and the B-CP's internal networks from external networks accessible by third parties. Sensitive data are protected when exchanged over non-secure networks.

9.5 Security audit procedures

Security audit procedures are carried out for all computer and system components that affect the operation of keys, certificates and equipment issuing processes under this policy.

9.5.1 Types of event recorded

Security audit functions related to the B-MSCA and the B-CP computer/system log, for audit purposes:

a) The creation of accounts (privileged or not).
b) Transaction requests together with record of the requesting account, type of request, indication of whether the transaction was completed or not and eventual cause of uncompleted transaction.
c) Installation of new software or software updates.
d) Time and date and other descriptive information about all backups.
e) Shutdowns and restarts of the system.
f) Time and date of all hardware upgrades.
g) Time and date of audit log dumps.
h) Time and date of transaction archive dumps.

9.5.2 Frequency of processing audit log

The logs are processed regularly and analysed against malicious behaviour. Log procedures are described in the Certification Practice Statement.

9.5.3 Retention period for audit log

Audit logs are retained for at least 7 years.

9.5.4 Protection of audit log

The integrity of audit logs is appropriately protected. All entries are individually time stamped. Audit logs are verified and consolidated at least monthly. At least two people in SA or ISSO roles (see section 9.3.1) are present for verification and consolidation.

9.5.5 Audit log backup procedures

Two copies of the consolidated log are made and stored in separate physically secured locations. Audit logs are stored in a way that makes it possible to examine the log during its retention period. Audit logs are protected from unauthorized access.

9.5.6 Audit collection system (internal vs. external)

Only an internal audit collection system is required.

9.6 Record archiving

9.6.1 Types of events recorded by the B-CIA

Records include all relevant evidence in the B-CIA's possession including, but not limited to:

a) Certificate requests and all related messages exchanged with the B-MSCA and the B-CP, users, and the directory.

b) Signed registration agreements from user's applications for certificates and cards, including the identity of the person responsible for accepting the application.

c) Signed acceptance of the delivery of cards.

d) Contractual agreements regarding certificates and associated cards.

e) Certificate renewals and all messages exchanged with the user.

f) Revocation requests and all recorded messages exchanged with the originator of the request and/or the user.

g) Currently and previously implemented policy documents

9.6.2 Types of event recorded by the B-MSCA and the B-CP

Records comprise of all relevant evidence in the possession of the B-MSCA and the B-CP including, but not limited to:

a) Contents of issued certificates.

b) Audit journals including records of annual auditing of the B-MSCA and the B-CP's compliance with this certificate policy.

c) Currently and previously implemented certificate policy documents and the certificate policy.

Records of all digitally signed electronic requests made by the B-MSCA or the B-CP (CAA/PA) include the identity of the administrator responsible for each request and all information required for non-repudiation checking of the request for as long as the record is retained.

9.6.3 Retention period for archive

Archives are retained and protected against modification or destruction for a period as specified in the Certification Practice Statement of the B-MSCA and the B-CP.

9.6.4 Procedures to obtain and verify archive information

The B-MSCA and the B-CP act in compliance with requirements regarding confidentiality as stated in section 3.4.

Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.

To the extent permitted by Law a fee may be charged against record retrieval costs. The B-MSCA and the B-CP ensure the availability of the archive and that archived information is stored in a readable format during its retention period, even if the B-MSCA and the B-CP's operations are interrupted, suspended or terminated.

If the B-MSCA or B-CP services are interrupted, suspended or terminated, the B-MSCA or the B-CP notify all customer organizations to ensure the continued availability of the archive. All requests for access to archived information is sent to the B-MSCA and the B-CP or to the entity identified by the B-MSCA and the B-CP prior to terminating its service.

9.7 B-MSCA and B-CP continuity planning

The B-MSCA and the B-CP have a business continuity plan (BCP) that includes but is not limited to addressing:

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

The ERCA will be notified of any disasters without any delay.
Disaster response mechanisms do not depend on ERCA response time.

9.7.1 Member State keys compromise

Belgian keys compromise is dealt with in section 6.

9.7.2 Other disaster recovery

The B-MSCA, the B-CP and subcontractors have routines established to prevent and minimize the effects of system disasters as provided in the BCP.

9.8 Physical security control of the CA and personalization systems

Physical security controls are implemented to control access to the B-MSCA or B-CP hardware and software. This includes the workstations and other parts of the CA and personalization hardware and any external cryptographic hardware module or card. A log is kept over all physical entries to premises. The B-MSCA premises feature numbered zones and locked rooms, cages, safes, and cabinets.

The Belgian keys for signing certificates are kept physically and logically protected as described in this certificate policy.
Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.
Power and air conditioning operate with a high degree of redundancy.
Premises are protected from any water exposures.
The CA operator implements prevention and protection as well as measures against fire exposures.
Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.
To prevent unwanted disclosure of sensitive data waste is disposed of in a secure manner. The sites of the CA operator host the infrastructure to provide the CA services. The CA operator sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access control list, which is subject to audit.
The premises of the B-MSCA and the B-CP can be used to store backup and distribute media in a way sufficient to prevent loss, tampering with, or unauthorized use of the stored information. Backups are kept for data recovery and for the archival of important information. Backup media are stored at a separate discreet site to permit restoration in the event of a natural disaster to the primary facility. A security check of the B-MSCA and B-CP premises is done at least once every 24 hours.

9.8.1 Physical access

Access to the premises hosting the Belgian State keys and the means for their usage, requires simultaneously presence of at least 2 persons which have been individually obtained the right to enter the designated area.

Access to other B-MSCA or B-CP premises is limited to personnel in trusted roles (see 9.3.1).

The B-MSCA CPS stipulates the controls implemented to ensure secure physical access.

10 B-MSCA OR B-CP TERMINATION

10.1 Final termination

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

a) Inform all users and parties with whom the B-MSCA and the B-CP have agreements or other form of established relations.

b) Make publicly available information of its termination at least 3 months prior to termination.

c) The B-MSCA and the B-CP terminate all authorization of subcontractors to act on behalf of the B-MSCA and B-CP in the process of issuing certificates.

d) The B-MSCA and the B-CP maintain and provide continuous access to record archives by handing them over to ERCA.

10.2 Transfer of B-MSCA or B-CP responsibility

Transfer of B-MSCA or B-CP responsibility occurs when the B-MSA appoints a new B-MSCA or B-CP. The B-MSA ensures the transfer of responsibilities, assets and all root keys to the new B-MSCA. In addition to the above:

- The B-MSA ensures the orderly transfer of responsibilities and assets.
- The outgoing B-MSCA transfers all root keys to the B-MSA. The B-MSA subsequently transfers all root keys to the new B-MSCA .
- The outgoing B-MSCA destroys any copies of keys that are not transferred.

11 AUDIT

The B-MSA is responsible to carry out audits on the B-MSCA and the B-CP. The B-MSCA and the B-CP are audited at least annually against the Belgian certificate policy.

The B-MSA may use the services of an external auditor or carry it out itself.

The B-MSA takes appropriate action with regard to possible irregularities discovered in the audit.

Results of the audits on a security status level will be sent in English to the ERCA.

The content of the audit reports provided to ERCA shall include descriptions of any corrective actions and a corresponding implementation schedule.

Actual audit reports will not be disclosed except, as it might be required by Law or ERCA regarding audit results that are submitted in a report, in English. Other parties may submit requests to access audit results and if duly justified, they might be allowed access to them.The audited parties may select how to best implement the audit findings and recommendations.

12 B-MSCA AND B-CP CERTIFICATE POLICY CHANGE PROCEDURES

12.1 Items that may change without notification

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

a) Editorial corrections
b) Changes to the contact details

12.2 Changes with notification

12.2.1 Notice

Any item in this certificate policy may be changed with 90-calendar days notice. Changes to items, which do not materially affect a significant number of users or relying parties, may be done with 30 days notice.

12.2.2 Comment period

Impacted users may file comments with the policy administration organization within 15 days from notice.

12.2.3 Whom to inform

All eligible changes are notified to the B-MSA.

12.2.4 Period for final change notice

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

12.3 Changes requiring a new Belgian MSA Policy approval

If a change in this certificate policy is deemed by the B-MSA to impact the Belgium CA policy, action is taken to make appropriate updates.

13 REFERENCES

[BPM]] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. (under construction), owned by the Commission

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

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

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

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

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

[CSG]] Common Security Guideline, Card Issuing Project. (under construction), owed by the Commission

14 GLOSSARY/DEFINITIONS AND ABBREVIATIONS

14.1 Glossary/Definitions

CA Policy: A named set of rules that indicates the applicability of keys, certificates and equipment to a particular community and/or class of application with common security requirements.
Card/Tachograph cards: Integrated Circuit equipped card, in this policy this is equivalent to the use of the terms ”**IC-Card**” and ”**Smart Card**”.
Cardholder: A person or an organization that is a holder and user of a Tachograph card. Included are drivers, company representatives, workshop workers and control body staff.
Certificate: In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.
Certification Authority System (CAS): A computer system in which certificates are issued by signing certificate (user) data with the CA private signing key.
Certification Practice Statement practice statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual CA policy. The CPS takes a broader view to address key usage, certificates and equipment.
Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.
Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.
Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.
Practice Statement (PS). A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.
Private key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called Secret key.
Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.
Tachograph cards/Cards: Four different types of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.
User: Users are equipment users and are either **Card Holders** for card or **manufacturers** for Vehicle units/Motion Sensors. All users will be uniquely identifiable entities.

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

14.2 List of abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card personalizing organization
CPS	Certificate policy
B-CIA	Belgian CIA
B-CP	Belgian CP
B-MSA	Belgian State Authority
B-MSCA	Belgian CA
ERCA	European Root CA
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KG	Key Generation
MS	Member State
MSA	Member State Authority
MSCA	Member State CA
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	A specific Public key algorithm
SA	System Administrator
PS	Practice Statement
VU	Vehicle Unit
VUP	VU Personalizing organization