# Guideline and Template

# National CA policy

## Keys, certificates and equipment management

(Registration, key generation, certificate issuing, personalization, distribution, use and end of life)

**for**

## the Tachograph system

**for**

## the CIA, MSA, MSCA, and CP

**Version**

| | | | |
|---|---|---|---|
| Draft Version 0.4 | February 2002 | Presented to the Card Issuing project SWG3 in Paris | May-Lis Farnes, SNRA |
| Draft Version 0.8 | | Distributed to the Card Issuing project SWG3 | May-Lis Farnes, SNRA |
| Draft Version 0.85 | June 2002 | Distributed to the Card Issuing project SWG3 | May-Lis Farnes, SNRA |
| Draft Version 0.90 | 27 June 2002 | To be used and commented by all Member States | May-Lis Farnes, SNRA |
| Version 1.0 | 31 October 2002 | Final version submitted to Member States | May-Lis Farnes, SNRA |


May-Lis Farnes, SNRA, Sweden, +46-70-622 73 57, may-lis.farnes@vv.se

# Table of Contents

# Guideline
# National CA policy

# 0 Guidelines for using the National CA policy Template

## 0.1 Background and introduction

### 0.1.1 About this document

This document is a **Guideline** and a **Template** for the Member States[1] to introduce a CA policy[2] for the Tachograph system. A CA policy is a document to support requirements to secure the management of keys, certificates and equipment. The National CA policy for the Member States introducing the Tachograph system is called the National CA policy.

The Tachograph system is described by Council Regulation 2135/98, which is referred to hereinafter as the Regulation. Responsible for the Regulation is the European Commission, which is referred to hereinafter as the Commission.

This document is based on requirements in the Regulation, standard for Policy requirements [ETSI 102 042], and the Risk analyses partly done for the Tachograph system.

### 0.1.2 How to use this document

It is the view of the Member States participating in the EU work organized by the Commission, Card Issuing Project (SWG3), and the Commission that a National CA policy **is needed for each Member State** to fulfil the Regulation, although it is not expressly required in the Regulation.

Each Member State is responsible for developing its own National CA policy; the Member State Authority, MSA, is the owner of and responsible for the National CA policy.

How the responsibility and work with the Tachograph system is organized will be different in different Member States so the description in this document is a **generic model** to cover these differences and has to be approriately detailed in each country.

**Chapter 0** is a **Guideline** on how to develop a National CA policy and how to use this template. **Chapters 1 through 14** form a **Template** for a National CA policy to be used by the Member States.

[1] Member State is used in the Regulation, but the use of the Tachograph system is not limited to the Member States of the EU but also other parties with agreements with EU to use the system, for example the EES countries.
[2] CA policy is a common terminology for a policy which states requirements to secure the management of keys, certificates and usually, cards, for a certain CA (Certificate Authority).

For more information about security and the terminology used in this document, please use the **Common Security Guideline** explained in chapter 0.4.

| Each National CA policy has to be **approved by the Commission**. |
|---|

### 0.1.3 Origin of this document

This document has been provided by the EU Member State representatives in the framework of the Card Issuing Working Group granted by the Commission.

### 0.1.4 Holder of the document

| The **Commission** is the holder of this document. |
|---|

## 0.2 Scope

It is the responsibility of each Member State to set up the means of guaranteeing the security of this new system. Each Member State is therefore required to define its own Tachograph organisation and to establish its own National security policy and National CA policy containing the security requirements for each entity involved within its organisation. Compliance with this document is considered by the Member States and the Commission to be an acceptable proof of being in accord with the regulation when asking the European Root Certification Authority for certification of Member State keys. This compliance underpins the need for consistency across Member States if confidence in all Tachograph systems is to be inspired.

The scope of a National CA policy is the management of keys, certificates and equipment (cards, VUs and Motion Sensors) within the Tachograph system, on the Member State level.

This includes several processes and functions throughout the entire lifecycle of the keys, certificates and equipment.

The two main processes are:

- issuing of Tachograph cards incl. keys and certificates, incl. renewal etc.
- issuing of keys and certificate for the VU, and keys for the Motion Sensor

These processes includes the following functions throughout the processes:

- registration (RA function) connected to application process
- key management
- key generation
- certficate issuing

- personalization
- distribution of cards, keys and certificates

In addition the following phases are covered:
- use of equipment (partly)
- end of life of equipment (partly)
- end of life for the MSCA

The organisations affected by this policy are (as defined in this document and the Common Security Guideline, CSG):
- MSA – Member State Authority
- CIA – Card Issuing Authority
- *(NCA) – National CA*
- MSCA – Member State Certification authority
- CP – Card Personalization organisation
- Equipment manufacturers, i.e. VU manufacturers and Motion Sensor manufacturers
- ERCA – European Root CA

*(The NCA may be used as a common name for the two functions:*
- *Member State CA (MSCA)*
- *Card Personalization organisation (CP) )*

Outside the scope of this document are:
- Type approval of the equipment
- Non-Tachograph applications/certificates on the Tachograph cards
- Detailed requirements of the use of the equipment
- Requirement for the end of life of the equipment
- User support

## 0.3 Definitions and interpretation

The definitions used throughout this document are described in this chapter and in chapter 14 (Glossary/Defintions and abbreviations) to help and guide the Member States to the use of this document.

### 0.3.1 Tachograph system organization overview

A schematic view of the Tachograph system organization is shown in the diagram below.

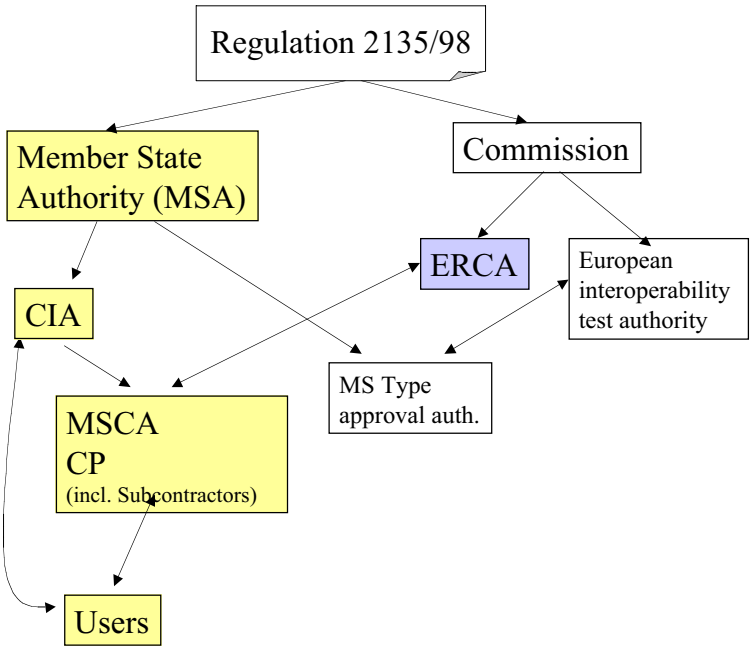


**Figure 1. Tachograph system organisation (coloured boxes are covered in this document)**

The Tachograph system is an **hierarchic csystem** where a root is established at the EU level (**ERCA**) and is connected to the different Member States to make a consistent and secure system. The role of the ERCA is to securely certify the root keys of the Member States to establish a trusted certification chain.

In this text the different roles are described. Note that these roles need not be separate organizations, they may be combined in one or more organizations.

The following roles are covered in this document:

- Member State Authority (**MSA**)
- Card Issuing Authority (**CIA**)
- Member State CA (**MSCA**)
- Card Personalization organisation (**CP**)
- **Users** of equipment (Tachograph cards, VUs and Motion Sensors)

The communication with the European Root CA (**ERCA**) is partly covered, to be consistent with the ERCA policy.

**The MSA** has overall responsibility for issuing processes in the Tachograph system on Member State level.

**The CIA** is either a part of the MSA organisation, another organisation in the Member State or a subcontractor **appointed by the MSA**. The CIA carries out the issuing processes.

**The MSCA** is either a part of the MSA organisation, another organisation in the Member State or a subcontractor **appointed by the MSA**. The MSCA carries out certain parts of the issuing processes.

**The CP** is either a part of the MSA organisation, another organisation in the Member State or a subcontractor **appointed by the MSA**. The CP carries out certain parts of the issuing processes.

In this document, **the NCA**, if applicable, is a combined authority carrying out the roles of **MSCA** and **CP**. If a member state chooses to use this model, the NCA is **appointed by the MSA.**

The responsiblities of the various roles are elaborated below.

#### *0.3.1.1 Member State Authority*

Each Member State is responsible for implementing the Tachograph system within its domain. Each Member State has to designate a Member State Authority, MSA, in order to implement the issuing processes.

**The MSA has the overall responsibility for the issuing processes in the Tachograph system in its country**.
The MSA has to coordinate the different tasks within the Tachograph system and, in the scope of this document, these tasks are part of one of two main processes, one for the cards, and the other for the VUs and Motion Sensors:

- issuing of Tachograph cards, incl. keys and certificates
- issuing of keys for the Motion Sensors and certificates and keys for VUs

**The MSA is responsible for setting up the Tachograph organization in its domain:**

- **The MSA is responsible for appointing a CIA**
- **The MSA is responsible for appointing a MSCA.**
- **The MSA is responsible for appointing a CP.**

#### *0.3.1.2 Card Issuing Authority*

**The CIA is appointed by the MSA**, and is the authority carrying out the user management, including functions of card application and approval, user support, and in some instances card distribution.

#### *0.3.1.3 The Card Personalization organisation*

**The CP is appointed by the MSA**, and is responsible for key generation (optional), card personalization and (optionally) distribution of certificates and cards in the Tachograph system.

The appointed CP is responsible for:

- generation of equipment key pairs, i.e. to cards and VUs (actual key generation need not be carried out by the CP, but the responsibility for secure operations lies with the CP)
- personalization of cards, i.e. inserting user data, RSA keys and certificate into the card, and printing visual data on the card. Includes ensuring that visual and electronic data match.
- distribution of cards (this function may be shared with the CIA or MSCA)

#### *0.3.1.4 Member State Certification Authority*

**The MSCA is appointed by the MSA**, and is defined as the authority responsible for issuing public key certificates for equipment (cards and VUs), and for managing the Member State root keys. MSCA may also generate card asymmetric keys.

The different functions of the MSCA may be carried out by the MSCA itself or subcontracted parties, Service Agencies, in which case the MSCA may be a virtual, rather than physical, organization.

The main part of the MSCA is the CA function, responsible for:

- Key management
- Key generation (optional)
- Certificate issuing

In more detail, the appointed MSCA is responsible for:

- secure generation and management of member state key pair(s)
- issuing of certificates for equipment public keys (i.e. to cards and vehicle units)
- keeping records of all public keys together with equipment identification (i.e. keep records of issued certificates)
- management and distribution of the symmetric Motion Sensor keys Km, $Km_{VU}$ and $Km_{WC}$ to manufacturers of Motion Sensors, VUs and workshop cards. including encryption of Motion Sensor data with Km. The keys are delivered from the ERCA upon request.
- **distribution** of MSCA certificate and ERCA public key to cards and VUs (this function may be shared with the CIA or CP)

#### *0.3.1.5 Users (certificate holders)*

Users are defined as the users of the equipment of the Tachograph system.

The equipment (or equipment parts) of the Tachograph system is defined as:

- Tachograph cards
- Vehicle Units (VU)
- Motion Sensors

Four different types of users of Tachograph cards exist and therefore four different types of cards exist:

- Driver Cards
- Company Cards
- Workshop Cards
- Control Cards

The user who has a card is called a card holding user and is:

- Drivers (D)
- Hauling Companies[3] (HC)
- Workshops (WS)
- Control body (CB)

The users of the VUs and Motion Sensors are defined as the equipment manufacturers, and the respective manufacturers are:

- VU manufacturers
- Motion Sensor manufacturers

### 0.3.2 Relying party of the MSCA (MSA)

Relying party of the MSCA (MSA) is the Control Body in each Member State.

In their enforcement work the Control Body users (card holders) have to rely on the certificates issued in all different Member States, and the corresponding Member State certificates.

### 0.3.3 Main processes and functions

The main processes supported by the National CA policy are:

- issuing of Tachograph cards, incl. keys and certificates (incl. renewal of cards etc.)
- issuing of VU and Motion Sensor keys and certificates
- management of the MSCA and ERCA root keys and certificates
- usage of equipment, keys and certificates (partly)
- end of life of MSCA

These five processes are described in more detail in the following subchapters.

#### *0.3.3.1 Issuing of Tachograph cards*

The card issuing process is described in figure 3, below.

[3] Transport companies

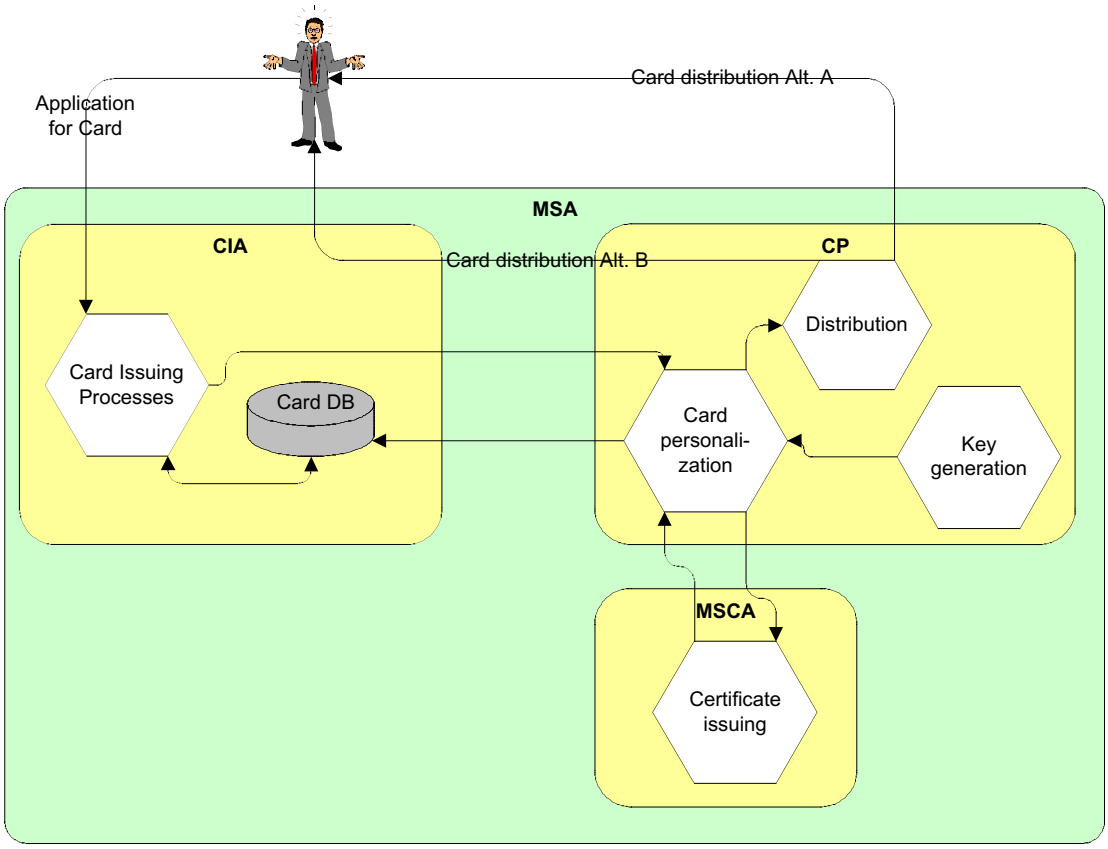


**Figure 2. Process: Tachograph card issuing**

**The MSA has the overall responsiblity** for the entire process of issuing Tachograph cards, including key and certificate generation.

**The CIA has responsibility** for:

- application process (incl. approval etc.)
- approved application registration (input to MSCA and CP)
- maintaining a database of issued cards
- (optional) distribution of cards (this function may be carried out by the MSCA or CP)

In the application process, applications are received and approved or rejected. Once an application is approved and registered, the information is moved to the MSCA.

The CIA may be responsible for distribution of Tachograph cards to users, as indicated by Alternative B in figure 3, above.

**The NCA (i.e. either MSCA or CP) has responsibility** for the following:

- key generation (although actual key generation may be carried out by a subcontractor or by the equipment manufacturer) In practice, key generation is closer to personalization than to certificate issuing.

**The CP has responsibility** for the following:

- card personalization (visual and electronic)
- (optional) distribution of cards (this function may be carried out by the MSA or CIA)

**The MSCA has responsibility** for the following:
- certificate issuing
- keeping records of all public keys together with equipment identification (i.e. keep records of issued certificates)
- management of the Motion Sensor keys $Km_{VU}$, $Km_{WC}$ and Km (for the Workshop Cards)

*0.3.3.2 Issuing of keys and certificates for the VU and Motion Sensor*

The **MSA has the overall responsibility** for the entire process of issuing keys and certificates for the VUs, and keys for the Motion Sensors. This process includes both the asymmetric key distribution and certificate issuing, as well as the symmetric key distribution.

The process is in most parts similar to that of card issuing.

The **CIA is responsible** for the following:
- application process (incl. approval etc.)
- approved application registration (input to MSCA)
- maintaining a database of equipment
- (optional) distribution of keys and certificate (this function should rather be carried out by the MSCA)

**The NCA (i.e. either MSCA or CP) has responsibility** for the following:
- key generation (although actual key generation may be carried out by a third party or by the equipment manufacturer)
- certificate issuing to VUs
- keeping records of all public keys together with equipment identification (i.e. keep records of issued certificates)
- management of the Motion Sensor keys $Km_{VU}$, $Km_{WC}$ and Km
- (optional) distribution of keys and certificates to the equipment manufacturers (this function may be carried out by the CIA)

The **VU manufacturers are responsible** for VU personalization, i.e. insertion of keys and certificates into the VU

The **Motion Sensor manufacturers are responsible** for insertion of encrypted Motion Sensor data into the Motion Sensor

The division of MSA or CIA tasks, MSCA and the equipment manufacturers tasks in the issuing of keys and certificates for the VUs and Motion Sensors is shown in figure 4, below.

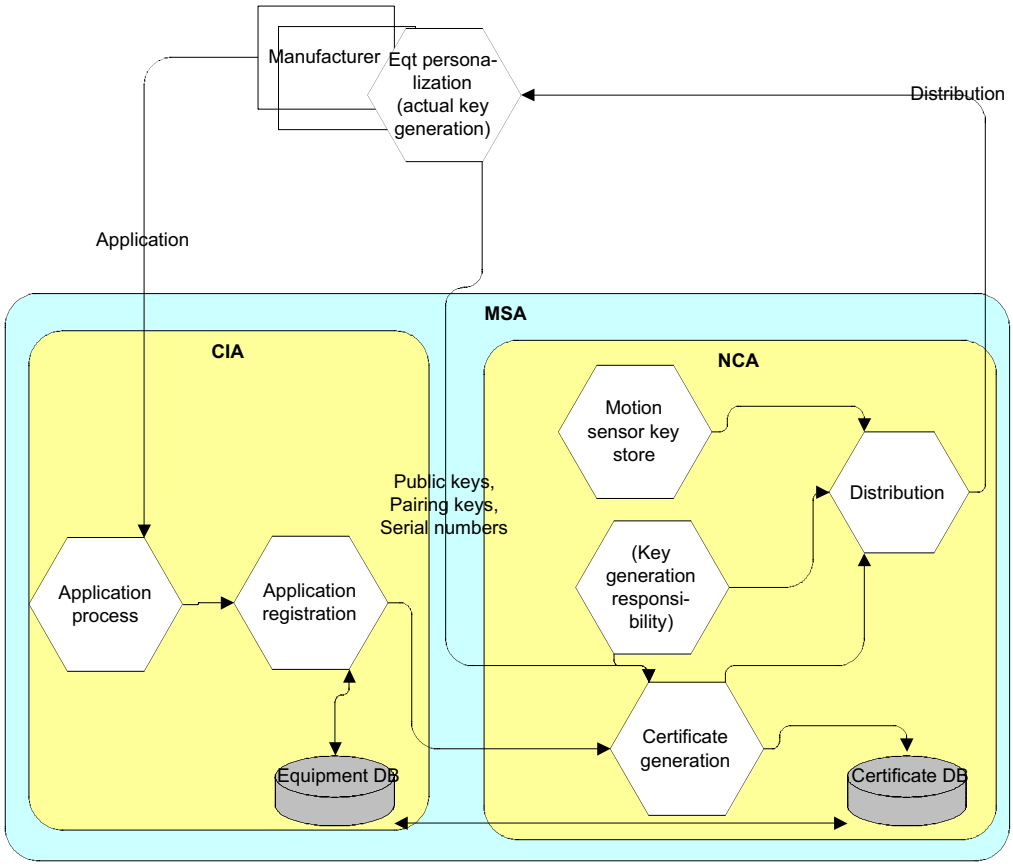


**Figure 4. Process: Keys and certificates issuing for VU and Motion Sensor**

### *0.3.3.3 Root keys and certificates management*

The MSCA is responsible for management of the European and Member State root keys, the Motion Sensor keys and for having its Member State public key certified by the ERCA.

The MSCA is responsible for:

- generation and management of Member State key pair(s)
- submission of Member State public key to ERCA for certification
- Member State certificate management
- ERCA public key management
- Motion Sensor keys management
- Secure distribution of keys and certificates between MSCA and CP

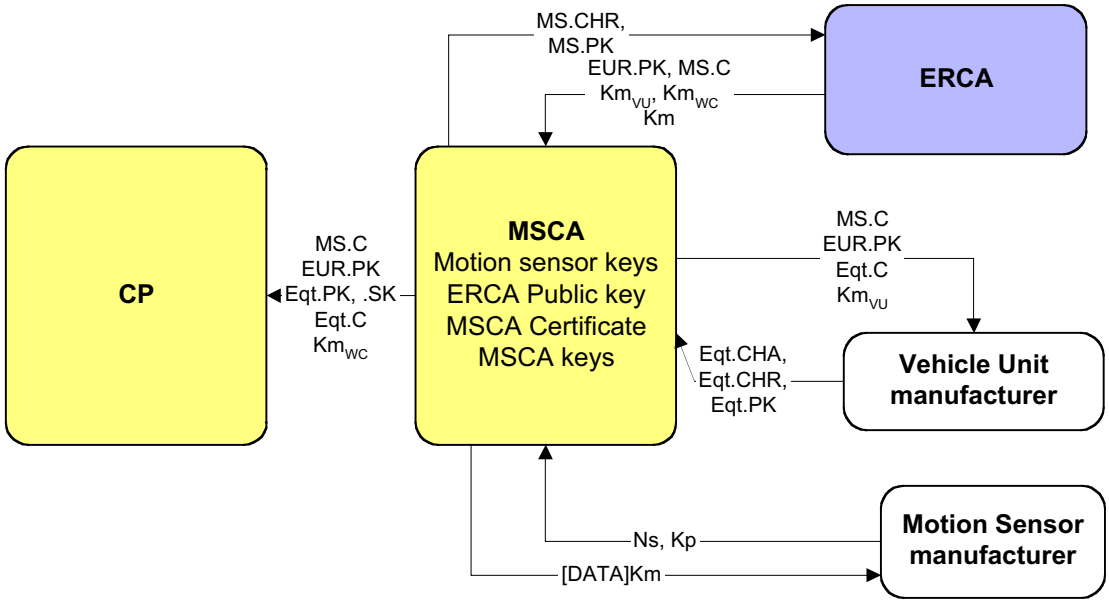


**Figure 5. Process: Root keys and certicate management**

### *0.3.3.4 Usage process - equipment*

To ensure the function and security of the system, the equipment has to be used in a proper way.

MSA/CIA is responsible for giving the users information/instructions/rules for usage of equipment.

### *0.3.3.5 End of life*

Some aspects of equipment end-of-life is handled in the policy. Other aspects should be considered by the respective Member State Authorities.
The end of life (termination) of the MSCA is handled in this policy. This is needed in case of changing of MSCA or end of use of the Tachograph system.

## 0.4 Policy and security document structure for the Tachograph system

The documents to support the implementation of the Tachograph system are:

- Common Security Guidelines [CSG]
- Card Issuing Best Practice Manual [BPM]
- National CA policy Guideline and Template (this document)

In addition the following documents are developed by the ERCA:

- European Root CA policy (ERCA policy)
- ERCA PS (ERCA Practice Statement)

Each MSA is responsible for developing the following documents:

- National CA policy (based on this guideline and template)

- National Information Security policy based on CSG (optional)
- National Card Issuing Process description based on BPM (optional)

The appointed MSCA and CP are responsible for development of the following documents to be approved by the MSA:

- Practice Statement (PS) (optional)
- Information Security policy (National) (optional)

The structure of the different documents is laid out in the diagram below.

**Overview of documents for the Tachograph system**

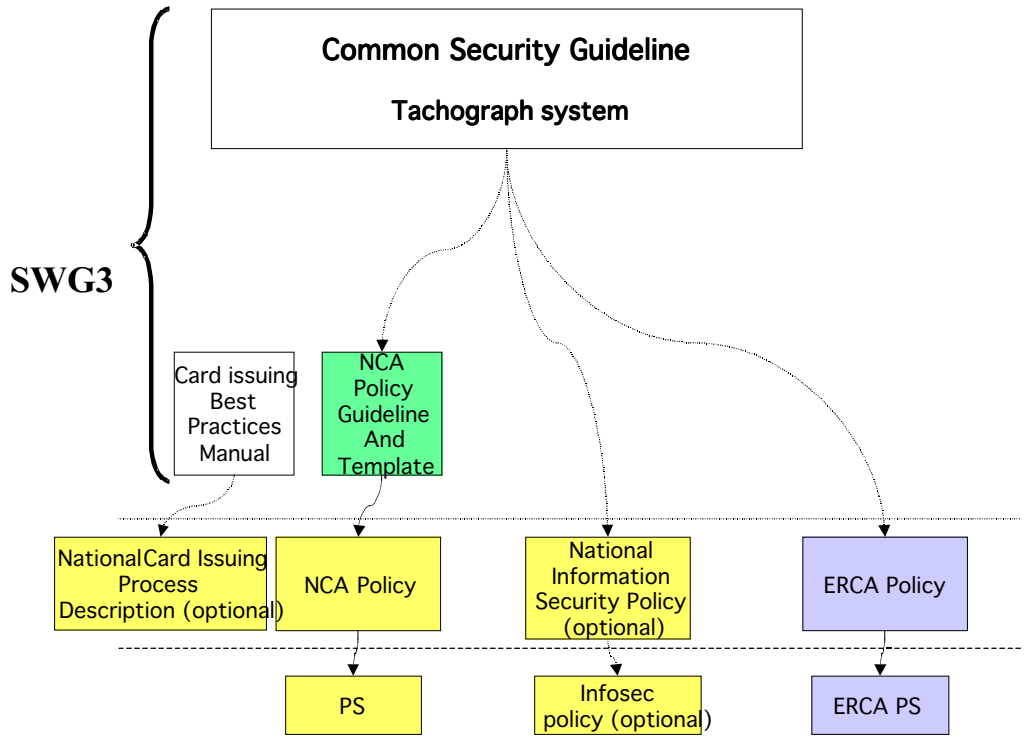


**Figure 6. Document structure of key, certificate and card management in the Tachograph System.**

A more detailed descriptions of the documents follows below.

### 0.4.1 Common Security Guideline

The Common Security Guideline (CSG) exists as a global framework for all relevant organizations in the system. It offers an overview of the security requirements in the Regulation.

It is an advisory document, pointing to the actual policy document at Member State and European level.

| The Commission is the holder of the CSG. |
|---|

### 0.4.2 The Card Issuing Best Practice Manual

The Card Issuing Best Practice Manual (BPM) is input for all Member States and the MSA when developing the Card Issuing Process and mainly the application process, as well as other MSA processes.

It is an advisory document but helps the Member State to implement the Card Issuing Processes and a National Card Issuing Process policy (optional).

| |
|---|
| The Commission is the holder of the Card Issuing Best Practice Manual. |

### 0.4.3 The National CA policy Guideline and Template

The National CA policy Guideline and Template (this document) is a Guideline and Template for each Member State to develop a National CA policy.

| |
|---|
| This National CA policy Guideline and Template should be used by all Member States, to ensure compatibility between Member State policies and the security of the whole system. |

| |
|---|
| The Commission is the holder of the National CA policy Guideline and Template. |

### 0.4.4 The National CA policy

A National CA policy should be developed [recommended] by each Member State to specify needed set of rules for managing keys, certificates and equipment in the Tachograph System.

It is imposed on the MSCA by the MSA. See section 0.3 for more details.

| |
|---|
| In order to ensure conformity and interoperability between all Member States, the Commission has to approve each National CA policy, as well as any significant revision thereof. |

| |
|---|
| The National CA policy of each Member State is owned by the relevant MSA. |

### 0.4.5 The Practice Statement (PS)

The PS is the MSCA's and CP's procedural documents, which details how the National CA policy is enforced in day-to-day management. It has a strong security focus. In a standard PKI structure and organization, this document is called a CPS (Certification Practice Statement). If Service Agencies carry out certain functions each agency shall have a Practice Statement to implement the National CA policy. See further details in section 0.6.

| |
|---|
| The PS is owned by the MSCA, CP, or each Service Agency. |

| |
|---|
| The Practice Statements have to be approved by the MSA. |

### 0.4.6 The ERCA policy

The ERCA policy is the set of rules under which the European Root CA is managed.

| |
|---|
| The ERCA policy is owned by the ERCA itself. |

| |
|---|
| The ERCA policy has to be approved by the Commission. |

### 0.4.7 The ERCA Practice Statement (ERCA PS)

The ERCA PS is the ERCA's procedural document, which details how the ERCA policy is enforced in day-to-day management.

The document is developed by the ERCA.

| |
|---|
| The ERCA PS is owned by the ERCA. |

## 0.5 Overview of the National CA policy

A National CA policy is needed, in order to ensure that the keys, certificates and equipment (cards, VUs and Motion Sensors) are managed in a safe and trustworthy manner by the following organisations:

- ERCA
- MSA
- CIA
- MSCA
- CP
- Users

The National CA policy is a set of rules that describes the way keys, certificates and equipment are issued.

The National CA policy partly describes rules on how the equipments are going to be used.

In addition the end of life process is handled for the MSCA itself.

| |
|---|
| The National CA policy states requirements **mainly** on **the MSCA, the CP, and their subcontractors**. |

For the different involved parties it is important to have the possibility to evaluate the level of trust linked with the keys, certificates and equipment of the Tachograph system. Trust is not something that easily can be put into

figures. The National CA policy is a way of proving trust for the MSCA organization's security, stability and integrity.

The National CA policy should basically answer the following questions:

- What is the intention with the keys, certificates and equipment?
- What rules and controls are in place to ensure security, stability and trust?

## 0.6 Overview of the Practice Statement (PS)

In order to document the implementation of the National CA policy, especially concerning security matters, Practice Statements, PS, are needed. Both the Card Personalization organization (CP) and MSCA need to have a PS. Combined, they are more or less equivalent to a CPS (Certification Practice Statement), which is a standard document in a PKI.

Where subcontractors or Service Agencies carry out some or all functions, each such SA shall have a PS, which describes the security practices that are used in the process(es).

The PS enforces the rules established by a specific National CA policy and is a rather detailed description of the terms and conditions as well as business and operational practices of a MSCA and CP in issuing and otherwise managing keys, certificates and equipment. A PS defines how the organizations meet the technical, organizational and procedural requirements identified in the National CA policy.

The PS should give an answer to the question:

- How are the functions, processes and security controls formed that enforces the National CA policy?

If Service Agencies are employed and have Statements, these shall be compiled by the CP or MSCA and made available for the users through the **MSA or CIA**.

## 0.7 Overview of the Information Security policy

All organisations in the Tachograph system have to manage Information Security on a general level and specific for the requirements of the Regulation.

For the purpose of handling Information Security it is considered best practice today to develop an Information Security policy for each organisation and to base it on the standard ISO 17799 -Standard for Information Security management [ISO 17799]. This standard describes what the organisation should consider when developing its Information Security policy.

A detailed description of ISO 17799 is beyond the scope of this document, therefore we refer to the standard itself.

The organizations on Member State level strongly having a need for an Information Security policy are:

- MSA and CIA [recommended]
- MSCA [strongly recommended]
- CP [strongly recommended]

In addition the following organizations strongly needing an Information Security policy are:

- the equipment manufacturers [strongly recommended]
- the workshops [recommended]
- the control bodies [optional]

The Information Security policy documents shall take strong input from the Common Security Guideline (CSG) and this document (National CA policy Guideline and template). For more information se the Common Security Guideline (CSG).

| |
|---|
| It is **recommended** that the MSA or CIA and the workshops implement Information Security policies. |

| |
|---|
| It is **strongly recommended** that the MSCA, CP and equipment manufacturers implement an Information Security policy. |

## 0.8 How to use the MSCA Guidelines and template

**Chapter 0** is an introduction and guideline for developing a National CA policy using this document as a template. **Chapters 1 through 14** form a template for a National CA policy.

This guideline and template is suggested for use by all Member States. By using the template appropriately a Member State will fulfil the relevant Regulation requirements and needed security requirements.

| |
|---|
| **National CA policy Guideline and Template** -> **National CA policy** for each Member State |

**Chapters 1 through 14** should be seen as a template for the National CA policy. All Member States are allowed, and encouraged, to copy the chapters and to use the template as a start of making a National CA policy.

The exact references to the Regulation in this document should not be included in the actual National CA policy, they are informational only.

| |
|---|
| It is **strongly recommended** that the template is followed as far as possible, as it makes it easier to read each other's MSCA policies (for mutual agreement and acceptance). |

If a Member State doesn't use this template, it shall undertake adequate measures to ensure that all requirements in this National CA policy Guideline and Template are fulfilled.

### 0.8.1 Interpretation of the template

Text parts forming requirements on MSCA procedures and responsibilities are called rules and are marked with the reference prefix "**[r*n*]**" where *n* is a sequential number throughout the document.

The template has three levels of rules denoted by the following formatting:

- Mandatory requirement (required either by Regulation or by recognized standards. If required by the Regulation, a reference is given.)
- [Recommended] Strongly recommended by the Card Issuing Working Group to reach the required security level.
- [Practice] Good practice recommended by the Card Issuing Project (SWG3) to reach a recommended security level.

When the template uses brackets **<>** the content should be specified by the specific MSCA (Member State specific).

A Member State may also add optional requirements to the policy, provided this does not intervene with the Regulation.

## 0.9 Revision procedure of this document

Member States can submit proposals for modifications to the **Commission**. The **Commission** will inform the other Member States of the proposed modifications. If necessary, the **Commission** shall arrange a meeting of Member States representatives to consider revisions of the document.

The current revision of this document shall be available from the **Commission** upon request.

The **Commission** shall notify all Member States of published revisions.

# Template
# National CA policy

# 1 Introduction

This document is the National CA policy, for <country> for the Tachograph system.

This National CA policy is in accordance with

- the Council Regulation of the Tachograph System, 2135/98
- the Commission Regulation 1360/2002
- [strongly recommended] the " Guideline and Template National CA policy "
- [strongly recommended] the "Common Security Guidelines"

## 1.1 Responsible organization

Responsible for this National CA policy is the Member State Authority, MSA < organization>.

The appointed **CIA** is <organization>.

The appointed **MSCA** is <organization>.

The appointed **CP** is <organization>.

The MSCA or CP may subcontract parts of its processes to subcontractors, Service Agencies. The use of Service Agencies in no way diminishes the MSCA's or CP's overall responsibilities.

[Recommended] List of Service Agencies:
<SA 1>
<SA 2>
….

## 1.2 Approval

This National CA policy is approved by the Commission by <name> at <date>.

## 1.3 Availability and contact details

[Recommended] The National CA policy is publicly available at <internet address>

Questions concerning this National CA policy should be addressed to:
< organization >.

[Recommended] <Contact details for this National CA policy>

# 2 Scope and applicability

[r1] The National CA policy is valid for the Tachograph system only.

[r2] The keys and certificates issued by the MSCA are only for use within the Tachograph system.

[r3] [Recommended] The cards issued by the system are only for use within the Tachograph system.

The scope of the National CA policy within the Tachograph system is shown in the figure below.

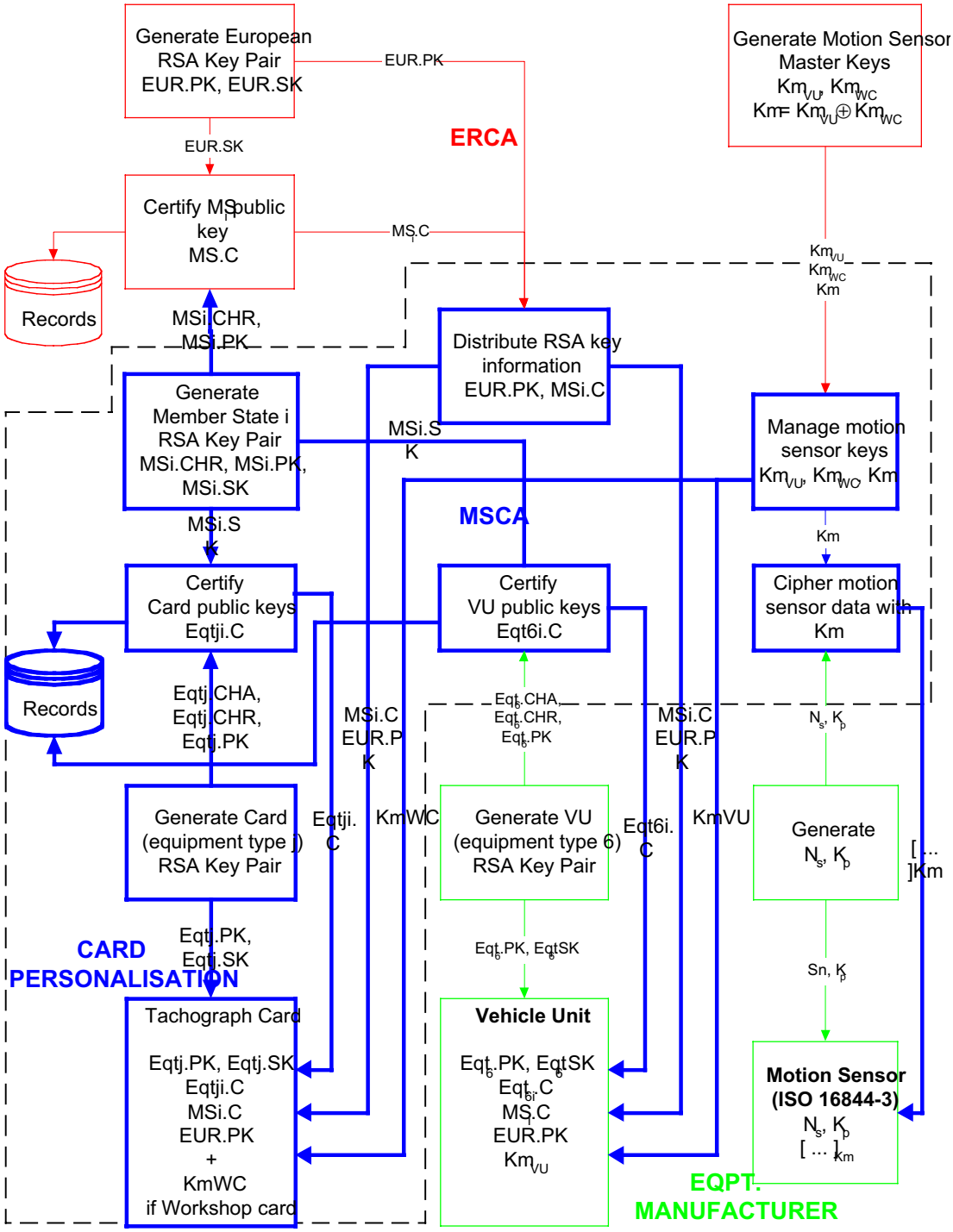


**Figure. Tachograph system keys, certificates and equipment management. (Scope of policy is marked with bold lines.)**

# 3 General provisions

This section contains provisions relating to the respective obligations of MSA, CIA, MSCA, CP, Service Agencies and users, and other issues pertaining to law and dispute resolution.

## 3.1 Obligations

This section contains provisions relating to the respective obligations of:

- MSA and CIA
- MSCA and Service Agency (if any)
- CP and Service Agency (if any)
- Users (Cardholders, VU manufacturers and Motion Sensor manufacturers)

### 3.1.1 MSA and CIA obligations

With regard to this NCA policy, the MSA and CIA has the following obligations.

[r4] The MSA shall:

a) Maintain the National CA policy
b) Appoint an MSCA and a CP
c) Audit the appointed MSCA and CP including Service Agencies
d) Approve the MSCA/CP PS
e) inform the appointed parties about this policy
f) inform the VU manufacturers and the Motion Sensor manufacturers about this policy
g) let this policy be approved by the **Commission**

[r5] The CIA shall:

a) Ensure that correct and relevant user information from the application process is input to the MSCA and CP
b) inform the **users** of the requirements in this policy connected to the use of the system, i.e the Cardholders, the VU manufacturers and the Motion Sensor manufacturers

### 3.1.2 MSCA obligations

[r6] The appointed MSCA shall:

a) Follow this National CA policy
b) Publish a MSCA Practice Statement (MSCA PS) that includes reference to this National CA policy, to be approved by the MSA
c) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National CA policy, *in particular to bear the risk of liability damages*

[r7] The MSCA shall ensure that all requirements on MSCA, as detailed in this policy, are implemented.

[r8] The MSCA has the responsibility for conformance with the procedures prescribed in this policy, even when the MSCA functionality is undertaken by subcontractors, Service Agencies. The MSCA is responsible for ensuring that any Service Agency provides all its services consistent with its Practice Statement (PS) and the National CA policy.

### 3.1.3 CP obligations

[r9] The appointed CP (card personalization organization) has to:

a) Follow this National CA policy

b) Publish a CP Practice Statement (CP PS) that includes reference to this National CA policy, to be approved by the MSA

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

[r10]The CP shall ensure that all requirements on it, as detailed in this policy, are implemented.

[r11]The CP has the responsibility for conformance with the procedures prescribed in this policy, even when the CP functionality is undertaken by subcontractors, Service Agencies.

### 3.1.4 Service Agency obligations

[r12]Service Agencies (if applicable) have obligations towards the MSCA or CP and the users according to contractual agreements.

### 3.1.5 Cardholder obligations

[r13][Recommended]The CIA shall oblige, through agreement (see 5.1.2), the user (or user's organization) to fulfil the following obligations:

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

b) the keys and certificate are only used in the Tachograph system;

c) [Recommended] the card is only used in the Tachograph system;

d) reasonable care is exercised to avoid unauthorized use of the equipment private key and card;

e) the user may only use his own keys, certificate and card (Regulation14.4.a);

f) a user may have only one valid driver card (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);[Recommended] or both a workshop card and a driver card; or several workshop cards

h) the user shall not use a damaged or expired card (Regulation14.4.a);

i) the user shall notify the CIA without any reasonable delay if any of the following occur up to the end of the validity period indicated in the certificate:

- the equipment private key or card has been lost, stolen or potentially compromised (Regulation15.1); or

- the certificate content is, or becomes, inaccurate.

### 3.1.6 VU manufacturers' obligations (role as personalization organization)

[r14]The 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 MSA in accordance with the requirements of this policy, particularly with regards to registration;

b) the keys and certificate 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 MSA without any reasonable delay if any of the following occur up to the end of the validity period indicated in the certificate:

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

### 3.1.7 Motion Sensor manufacturers' obligations (role as personalization organization)

[r15]The MSA shall oblige, through agreement (see 5.1.2), the Motion Sensor manufacturers to ensure that the following obligations are fulfilled:

a) accurate and complete information is submitted to the 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 MSA without any reasonable delay if the secret key has been lost or destroyed

## 3.2 Liability

Note: the Regulation does not discuss the issue of liability.

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

Any liability issues towards end users are the responsibility of the MSA/CIA.

[r16][Recommended] 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.

### 3.2.1 MSA and CIA liability towards users and relying parties

[r17][Recommended] The MSA and CIA are liable for damages resulting from failures to fulfill their obligations only if they have acted negligently. If the MSA or CIA has acted according to this National CA policy, and any other governing document, it shall not be considered to have been negligent.

### 3.2.2 MSCA and CP liability towards the MSA and CIA

[r18][Recommended] The CP or MSCA is liable for damages resulting from failures to fulfill these obligations only if it has acted negligently. If the organization has acted according to this National CA policy and the corresponding PS, it shall not be considered to have been negligent.

## 3.3 Interpretation and enforcement

### 3.3.1 Governing law

*The matter of governing law is not resolved.*

## 3.4 Confidentiality

Confidentiality is restricted according to Directive 95/46/EC (or corresponding national law) on the protection of individuals with regard to the processing of personal data and on the movement of such data.

### 3.4.1 Types of information to be kept confidential

[r19]Any personal or corporate information held by the MSCA, the CP or Service Agencies that is not appearing 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.

[r20]All private and secret keys used and handled within the MSCA/CP operation under this National CA policy are to be kept confidential.

[r21] All private and secret keys used and handled within the VU manufacturers operation under this National CA policy are to be kept confidential.

[r22] The secret keys used and handled within the Motion Sensor manufacturers operation under this National CA policy are to be kept confidential.

[r23]Audit logs and records shall not be made available as a whole, except as required by law.

### 3.4.2 Types of information not considered confidential

[r24]Certificates are not considered confidential.

[r25] Identification information or other personal or corporate information appearing on cards and in certificates is not considered confidential, unless statutes or special agreements so dictate.

# 4 Practice Statement (PS)

[r26] The MSCA and CP shall have statements of the practices and procedures used to address all the requirements identified in the National CA policy, Practice Statements (PS). The MSA shall approve the PS.

In particular:

a) The PS shall identify the obligations of all external organizations supporting the MSCA and CP services including the applicable policies and practices.

b) The Practice statement shall be made available to the MSA, to users of the Tachograph system, and to relying parties (e.g. control bodies).

   However, the MSCA/CP is not generally required to make all the details of its practices public and available for the users.

c) The management of the MSCA/CP has responsibility for ensuring that the PS is properly implemented

d) The MSCA/CP shall define a review process for the PS.

e) The MSCA/CP shall give due notice of changes it intends to make in its PS and shall, following approval, make the revised PS immediately available. Minor revisions may be released without MSA approval.

# 5 Equipment management

The equipment in the Tachograph system is defined as:

- Tachograph cards
- Vehicle units
- Motion Sensors

The equipment is handled and managed by several roles:

- CIA (registration, renewal, etc.)
- MSCA (certificates, keys)
- CP (visual and electronic personalization, distribution, deactivation)
- VU manufacturers and Motion Sensor manufacturers

The following functions are carried out by the MSA:

- Quality control (type approval)

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

- Motion Sensor key insertion
- Distribution

## 5.1 Tachograph cards

### 5.1.1 Quality control – MSCA/CP function

[r27] 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 CIA

[r28] The CIA shall inform the user of the terms and conditions regarding use of the card. This information shall be available in a readily understandable language.
[Practice] It is recommended that the information is available in at least both the national language(s) of the member state and in English.

[r29] The user shall, by applying for a card, and accepting delivery of the card, accept the terms and conditions.

#### *5.1.2.1 User application*

[r30] Applicants for a Tachograph card shall deliver an application in a form to be determined by the MSA or CIA. As a minimum, the application shall include the data needed to ensure the correct identification of the user. Other data could for example be gathered from the driving license register.

Note: According to the Regulation, workshop, company and control certificates and cards may be issued either to individuals representing companies or organizations (legal persons) or to the legal person itself. It is recommended that the former apply, since it provides higher security. If it is decided that these cards and certificates may be non-individual, the policy below should be amended accordingly.

The following information is required for issuing a card. Unless gathered from other sources, it should be included in the application:

- Full name
- Date and place of birth
- Place of residence
- [Recommended] National registration number (if available)
- [Recommended] Postal address
- Photo (unless a valid filed photo is used) (Optional except for driver cards)
- Preferred language

*Driver card specific:*

- Driving license number

*Workshop card specific:*

[r31][**Recommended**]Workshop cards shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

- full name (including surname and given names) of the user;
- date and place 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;
- full name and legal status of the associated legal person or other organizational entity;

*Control body card specific:*

[r32][**Recommended**]Control body certificates shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

- full name (including surname and given names) of the user;
- date and place 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;
- full name and legal status of the associated legal person or other organizational entity;

*Hauling company card specific:*

[r33][**Recommended**]Hauling company certificates shall be issued to individual representatives of companies owning or holding vehicles fitted with digital Tachograph and who can provide evidence of:

- full name (including surname and given names) of the user;

- date and place 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;
- full name and legal status of the associated legal person or other organizational entity;
- any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;
- the user's association with the legal person or other organizational entity.

*5.1.2.2 Agreement*

[r34] 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 CIA terms of approval - Driver card specific*

[r35] A Driver card shall only be issued to individuals having permanent residence in the country of application.

[r36] The CIA shall ensure that the applicant does not have a valid Driver card issued in another Member State.

[r37] 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 the CIA

[r38] Workshop cards shall be valid for no more than **one** year from issuance (Regulation 12.1).

[r39] Driver cards shall be valid no more than **five** years from issuance (Regulation 14.4.a).

[r40] Company cards shall be valid no more than **five** years from issuance.

[r41] Control cards shall be valid no more than **two** years from issuance.

[r42] The CIA shall establish routines to remind the user of pending expiration.

[r43] An application for renewal shall follow section 5.1.2

*5.1.3.1 Driver cards*

[r44] The user shall apply for a renewal card at least **15** days prior to card expiration. (Regulation article 15.1)

[r45] If the user complies with the above rule, the CIA shall issue a new driver card before the current card expires. (Regulation article 14.4.a)

*5.1.3.2 Workshop cards*

[r46] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r47] The CIA shall issue a renewal card within **5** working days of receiving a complete application. (Regulation article 12.1)

*5.1.3.3 Company cards*

[r48] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r49] If the user complies with the above rule, the CIA shall issue a new company card before the current card expires.

*5.1.3.4 Control cards*

[r50] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r51] The CIA shall issue a renewal card within **5** working days of receiving a complete application.

### 5.1.4 Card update or exchange – handled by the CIA

[r52] 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.

[r53] 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)

[r54] 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 CIA

[r55] 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.

[r56]Stolen and lost card shall be put on a blacklist available to authorities in all Member States.

[r57]Damaged and malfunctioning cards shall be delivered to the issuing CIA, visually and electronically cancelled, and put on a blacklist.

[r58]If the card is lost, stolen, damaged or malfunctioning, the user shall apply for a replacement card within **7** days. (Regulation article 15.1)

[r59]Provided the user follows the above requirements, the CIA shall issue a replacement card with new keys and certificate within 5 working days from receiving a complete application. (Regulation article 14.4.a)

[r60]The replacement card shall inherit the time of validity from the original card. (Regulation Annex 1B: VII). If the replaced card has less than six months remaining validity, the CIA may issue a renewal card instead of a replacement card.

### 5.1.6 Application approval registration – handled by the CIA

[r61]The CIA shall register approved applications in a database. This data is made available for the MSCA/CP, which uses the information as input to the certificate generation and card personalization.

### 5.1.7 Card personalization – handled by the CP

Cards are personalized both visually and electronically. In some cases this process will be carried out by Service Agents, this does not diminish the overall responsibility of the MSA.

#### *5.1.7.1 Visual personalization*

[r62]Cards shall be visually personalized according to Regulation Annex 1B, section IV.

#### *5.1.7.2 User data entry*

[r63] Data shall be inserted in the card acording to the structure 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*

[r64][Recommended]The private key shall be inserted in the card without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection. See also equipment key management, 7.2.

#### *5.1.7.4 Certificate entry*

[r65]The user certificate shall be inserted in the card before distribution to the user.

*5.1.7.5 Quality Control*

[r66] Documented routines shall exist to ensure that the visual information on users' cards and the electronic information in issued cards and certificates matches each other and also matches the validated owner. The routines shall be described in the personalization PS.

*5.1.7.6 Cancellation (destruction) of non-distributed cards*

[r67] All cards that are damaged or destroyed (or for other reasons are not finalized and distributed) during personalization shall be physically and electronically destroyed (cancelled).

[r68] All destroyed cards shall be registered in a cancellation database.

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

[r69] The CP is responsible for keeping track of which card and card number is given to which user. Data shall be transferred from the CP to the CIA register.

### 5.1.9 Card distribution to the user – handled by the CP or CIA

[r70]

a) The personalization shall be scheduled so as to minimize the time that the personalized card require safe-keeping before delivery to the user. Storage over night requires secure safe-keeping. Documented routines shall exist for exception handling, including disturbances in the production process, failure of delivery, and loss of or damage to cards.
b) Personalized cards shall be immediately transferred to the place where they are to be delivered or distributed to the user, i.e. a controlled area.
c) Personalized cards shall always be kept separated from non-personalized cards.
d) The Tachograph card shall be distributed in a manner so as to minimize the risk of loss.
e) At the point of delivery of the card to the user, evidence of the user's identity (e.g. name) shall be checked against a physical person.
f) [Recommended] The user shall present valid means of identification
g) [Recommended] The reception of the card shall be acknowledged by the user's signature.

### 5.1.10 Authentication codes (PIN) – generated by the CP

This section applies only to Workshop cards.

[r71] Workshop cards shall have a PIN code, used for authenticating the card to the Vehicle unit (Regulation Annex 1B, App 10: Tachograph cards: 4.2.2)

[r72] PIN codes shall consist of at least **4** digits (Regulation Annex 1B, App 10: Vehicle Units:4.1.2).

*5.1.10.1 PIN generation*

[r73]PIN codes shall be generated in a secure system, securely transferred to workshop cards, and direct-printed to PIN-envelopes. PIN codes shall never be stored on a computer system in a manner that allows connection between PIN and user. The PIN generation system shall meet the requirements of ITSEC E3, CC EAL4 or equivalent security criteria.

*5.1.10.2 PIN distribution*

[r74]PIN codes may be distributed by regular mail.

[r75]PIN codes shall not be distributed in connection with the corresponding cards.

### 5.1.11 Card deactivation – handled by MSA/CIA and CP

[r76][Recommended] It shall be possible to permanently deactivate a card and any keys residing thereon. A decision of deactivation shall be taken by the MSA or CIA, the actual operation should be carried out by the CP or a Service Agency.

[r77]Deactivation of cards shall take place in equipment suitable for the operation and it shall be verified that card functions and keys are destroyed. The card shall also be visually cancelled.

[r78]Deactivation of cards shall be registered in the card database and the card number shall be put on the blacklist.

## 5.2 Vehicle Units and Motion Sensors

### 5.2.1 Quality control - CIA function

[r79]The CIA shall ensure 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 CIA

VU manufacturers apply for certificates, not equipment, but functionally the application process is equivalent to that used for Tachograph cards, and therefore it is dealt with here. Motion Sensor manufacturers requests Motion Sensor keys, and this request may be handled as a registration.

*5.2.2.1 Vehicle Units*

[r80]The CIA shall ensure that evidence of a VU's identification and accuracy of the manufacturer's names and associated data are properly examined as part of the registration service.

[r81]VU manufacturers may apply for certificates for as yet unidentified vehicle units. If this is the case, mapping between VU-identity and certificate shall be added to the registration as soon as possible (Regulation Annex 1B, Appendix 11: 3.3.1).

[r82]The CIA shall inform the manufacturer of the terms and conditions regarding use of the certificate. This information shall be available in a readily understandable language.
[Practice] It is recommended that the information is available in at least both the national language(s) of the member state and in English.

[r83][Recommended] The manufacturer shall, by making an application for a certificate and accepting delivery of the certificate, make an agreement with the MSA (or CIA), accepting the terms and conditions

[r84] The manufacturer shall provide a postal address, or other attributes, which describe how it may be contacted.

#### *5.2.2.2 Motion Sensors*

Manufacturers request Motion Sensor keys from the CIA. Included in the request is Motion Sensor and manufacturer data. Functionally this may be seen as an application. Motion Sensor data such as serial number and manufacturer shall be stored in a database.

### 5.2.3 Application approval registration – handled by the CIA

[r85]The CIA shall register approved applications in a database. This data is made available for the CP, which uses the information as input to the certificate generation.

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

[r86]The CP is responsible for registering which certificate is issued to which VU or VU certificate request. The 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 personalisers or even by the MSCA (Regulation Annex 1B, appendix 11:3.1.1).

[r87]If personalization is a task of the manufacturer, the MSA in the country of type approval shall inspect and approve of the personalization facility.

#### *5.2.5.1 Key entry*

[r88]The private RSA key shall be inserted in the VU without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection. The symmetric key $Km_{VU}$ shall be inserted in the VU in a safe manner. See also equipment key management 7.2.

*5.2.5.2 Certificate entry*

[r89]The user certificate shall be inserted in the VU in such a way as to maintain its integrity.

### 5.2.6 VU and Motion Sensor keys and certificate distribution to equipment manufacturers– handled by the CP

[r90]CP is responsible for the distribution of keys and certificates for the VUs and Motion Sensors to the respective manufacturers in a proper way!

### 5.2.7 VU distribution – handled by VU manufacturers

[r91]VU distribution is the responsibility of the VU manufacturers and has to be handled in a proper way!

### 5.2.8 VU renewal

[r92]The VU itself need not be renewed unless due to malfunction, damage etc.

### 5.2.9 Replacement of lost, stolen, damaged or malfunctional VUs

[r93]Replacement of a VU follows the practices for a new VU.

[r94]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.

[r95][Recommended] 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 should be handled so that:

[r96][Recommended] The keys and certificates are destroyed.

[r97]Destruction of a VU is registered by the CIA in the country of issuing.

# 6 Root keys and transport keys management: European Root key, Member State keys, Motion Sensor keys, transport keys

This section contains provisions for the management of

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

The **ERCA public key** is used for verifying the Member State certificates. The ERCA secret key is not dealt with here, since it never leaves the ERCA.

The **Member State keys** are the Member State signing keys and may also be called Member State root keys.

The **Motion Sensor keys** are the symmetric keys to be placed in the workshop card, VU and Motion Sensor for mutual recognition. The MSCA receives the Motion Sensor keys from the ERCA, stores them and distribute them to manufacturers.

The **transport keys** are the symmetric keys used for securely exchanging information between the ERCA and the MSCA.

If the MSCA has need for other cryptographic keys than the above, these shall not be considered part of the Tachograph system, and is not dealt with in this policy.

## 6.1 ERCA public key

[r98] 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 CP, the same rule applies.

[r99] The CP shall ensure that EUR.PK is inserted in all tachograph cards and vehicle units.

## 6.2 Member State keys

The Member State keys are the 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 MSCA public key is certified by the ERCA, but is always generated by the MSCA itself.

[r100] The Member State keys must not be used for any other purposes than signing Tachograph equipment.

### 6.2.1 Member State keys generation

[r101] Member State key pair generation shall be carried out within a device which either:

- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be 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.

[r102] The key generation device should be stand-alone

[r103] The actual device used and requirements met shall be stated in the MSCA PS.

[r104] MSCA key-pair generation shall require the active participation of three separate individuals. At least one of these shall have a role of CAA/PA (certification authority/ personalization administrator), the others may have other trusted roles (see section 9.3.19.3.1 for role descriptions).

[r105] Keys shall be generated using the RSA algorithm with a key length of modulus *n*=1024 bits (Regulation Annex 1B, app 11:2.1/3.2).

[r106] [Strongly Recommended] The MSCA shall have more than one Member State key pair with associated signing certificates to ensure continuity, since the ERCA cannot issue replacement Member State certificates rapidly.
*or*
[Recommended] The MSCA shall have at least two (2) and maximum five (5) Member State key pairs with associated signing certificates to ensure continuity, since the ERCA cannot issue replacement Member State certificates rapidly.

### 6.2.2 Member State keys' period of validity

[r107] [Recommended] The Member State private key shall not be valid for more than **2** years from certification of the corresponding public key, and shall not be used after its validity period for any purpose.

[r108] The corresponding public key shall have no end of validity.

### 6.2.3 Member State private key storage

[r109] The private keys shall be contained in and operated from inside a specific tamper resistant device which:

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

[r110] For access to the MSCA private signing keys, dual control is required. This means that no single person shall possess the means required to

access the environment where the private key is stored. It does not mean that signing of equipment certificates must be performed under dual control.

### 6.2.4 Member State private key backup

[r111] The Member State private signing keys may be backed up, using a key recovery procedure requiring at least dual control. The procedure used shall be stated in the MSCA PS. However, if key pairs according to [r106] are used, no backup is needed.

### 6.2.5 Member State private key escrow

[r112] The Member State private signing keys shall not be escrowed.

### 6.2.6 Member State keys compromise

[r113] A written instruction shall exist, included in the MSCA PS, which states the measures to be taken by users and security responsible persons at the MSCA and/or Service Agencies if the Member State private keys has become exposed, or is otherwise considered or suspected to be compromised.

[r114] In such case the MSCA shall as a minimum:

- Inform the MSA, the ERCA and all other MSCAs.

### 6.2.7 Member State keys end of life

[r115] The MSCA shall have routines to ensure that it always has a valid, certified Member State signing key pair.

[r116] Upon termination of use of a Member State signing key pair, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

## 6.3 Motion Sensor keys

[r117] The MSCA shall, as needed, request motion sensor keys Km, $Km_{VU}$ and $Km_{WC}$ from the ERCA (Regulation Annex 1B, app 11:3.1.3).

[r118] The MSCA shall, upon manufacturer request, encrypt Motion Sensor data (pairing key $K_P$ and extended serial number $N_S$) with Km (Regulation Annex 1B, app 11:3.1.3).

[r119] The MSCA shall forward the VU key $Km_{VU}$ to manufacturers of Vehicle Units for insertion into the VU (Regulation Annex 1B, app 11:3.1.3).

[r120] The MSCA shall forward the workshop key to the CP for insertion into Workshop cards.

[r121]The CP shall undertake the 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).

[r122]The MSCA and/or CP shall, during storage, use and distribution, protect the motion sensor keys with high assurance physical and logical security controls. The keys should be contained in and operated from a specific tamper resistant device which:

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

## 6.4 Transport keys

[r123]For secure data communication the ERCA issues special, symmetric, transport keys. The MSCA shall, during storage, use and distribution, protect these keys with high assurance physical and logical security controls. The keys should be contained in and operated from a specific tamper resistant device which:

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

# 7 Equipment keys (asymmetric)

Equipment keys are assymetric keys generated somewhere in the isuing/manufacturing process, and certified by the MSCA for the equipment in the Tachograph system:

- Tachograph cards
- Vehicle Units

The symmetric Motion Sensor keys are not handled here.

## 7.1 General aspects CP/MSCA incl. Service Agencies and VU manufacturers

[r124]Equipment (Card and VU) initialization, key loading and personalization shall be performed in a physically secure and controlled environment. Entry to this area shall be strictly regulated, controllable at the individual level, and requiring a minimum of two persons to be present to operate

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

[r125] No sensitive information contained in the key generation systems may leave the system in a way that violates this policy.

[r126] Tachograph cards: No sensitive information in the card personalization system may leave the system in a way that violates this policy.

[r127] VU/Motion Sensor: No sensitive information in the VU personalization system may leave the system in a way that violates this policy.

[r128] **Organizations (Subcontractors, Service Agencies)** that perform key generation and card personalization on behalf of more than one Member State shall do this in a clearly separate process for each of these. A log shall be kept of each individual process and the relevant MSA shall have access to this on request.

[r129] **[Recommended] VU manufacturers** that perform VU personalization shall do this in a process clearly separated from the VU production. A log shall be kept of the personalization and the relevant MSA shall have access to this on request.

[r130] **MSCA/CP/Service Agencies/VU manufacturers:** The log of the personalization system shall contain a reference to the order, and list the corresponding equipment numbers and certificates. The relevant MSA shall have access to the logs on request.

## 7.2 Equipment key generation

[r131] Keys may be generated either by the equipment manufacturer, by the CP or by the MSCA. (Annex 1B, Appendix 11:3.1.1)

[r132] The entity that performs the key generation shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

[r133] Key generation shall be carried out within a device which either:

- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
- meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be 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.

[r134] Keys shall be generated using the RSA algorithm having a key length of modulus *n* 1024 bits. (Annex 1B, Appendix 11:2.1/3.2)

[r135] The generation procedure and storage of the private key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been inserted in the device.

[r136] It is the responsibility of the key generation entity is to undertake adequate measures to ensure that the public key is unique within its domain before certificate binding takes place. (This is presumably done by making sure that the key generation system is random at its nature and therefore the probability of generating non-unique keys is insignificant.)

*7.2.1.1 Batch key generation*

[r137] Cryptographic key generation may be performed by batch processing in advance of certificate request, or in direct connection with certificate request.

[r138] Batch processing must be performed in stand-alone equipment meeting the security requirements stated above. Key integrity have to be protected until certificate issuing is performed.

### 7.2.2 Equipment key validity

*7.2.2.1 Keys on cards*

[r139] Usage of an equipment private key in connection with certificates issued under this policy shall never exceed the end of validity of the certificate.

*7.2.2.2 Vehicle units*

[r140] [Recommended] The private key of the Vehicle Unit shall not be valid more than **30** years.
*or*
The private key of the Vehicle Unit shall not be valid beyond the lifetime of the Vehicle Unit itself.

### 7.2.3 Equipment private key protection and storage - Cards

[r141] The CP shall ensure 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.

[r142] Copies of the private key are not to be kept anywhere except in the tachograph card, unless required during key generation and device personalization.

[r143] 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

[r144] The VU manufacturer shall ensure that the VU private key, and the corresponding means of its usage, are protected by, and restricted to, a VU.

[r145] Copies of the private key are not to be kept anywhere except in the VU unless required during key generation and device personalization.

[r146] In no case may the VU private key be exposed or stored outside the VU.

### 7.2.5 Equipment private key escrow and archival

[r147] Equipment private keys shall be neither escrowed nor archived.

### 7.2.6 Equipment public key archival

[r148] All certified public keys shall be archived by the certifying MSCA, or by the CIA.

### 7.2.7 Equipment keys end of life

[r149] Upon termination of use of a Tachograph card, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

[r150] Upon termination of use of a Vehicle Unit, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

# 8 Equipment certificate management

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

## 8.1 Data input

### 8.1.1 Tachograph cards

Cardholding users do not apply for certificates, their certificates are issued based on the information given in the application for a tachograph card (section 5.1.2) and captured from the CIA register. The public key to be certified is extracted from the key generation process.

[r151] The CP shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique. The MSCA shall verify the uniqueness of the CHR within its domain.

### 8.1.2 Vehicle units

Manufacturers (or equivalent representatives) of vehicle units must apply for certificates according to section [r79]: VU and Motion Sensor application/registration.

[r152] The CP shall ensure that the registration data contains information which renders the Certificate Holder Reference (CHR) unique. The MSCA shall verify the uniqueness of the CHR within its domain.

[r153] If the equipment key pair is not generated by the MSCA, the certificate request process shall ensure that the manufacturer has possession of the private key associated with the public key presented for certification.

## 8.2 Tachograph card certificates

### 8.2.1 Driver certificates

[r154] Driver certificates are issued only to successful applicants for a Driver card.

### 8.2.2 Workshop certificates

[r155] Workshop certificates are issued only to successful applicants for a Workshop card.

### 8.2.3 Control body certificates

[r156] Control body certificates are issued only to successful applicants for a Control body card.

### 8.2.4 Hauling company certificates

[r157] Hauling company certificates are issued only to successful applicants for a Hauling Company card.

## 8.3 Vehicle unit certificates

[r158] Vehicle unit certificates are issued to the VU manufacturer by the MSCA in the country of Type approval, and only to type approved VUs.

[r159] Vehicle unit certificates shall be issued only to manufacturers, and evidence shall 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

[r160]Certificates shall not be valid longer than the corresponding equipment (section 5):

- Driver certificates shall not be valid more than **5** years (Regulation 14.4.a).
- Workshop certificates shall not be valid for more than **1** year (Regulation 12.1).
- [Recommended] Control body certificates shall not be valid more than **2** years.
- [Recommended] Hauling company certificates shall not be valid more than **5** years.
- [Recommended] Vehicle Unit certificates shall not be valid more than **30** years
  *or*
  Vehicle Unit certificates shall have **no** end of validity.

## 8.5 Equipment certificate issuing

[r161]The MSCA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by Regulation Annex 1B, appendix 11.

## 8.6 Equipment certificate renewal and update

See Equipment management (section 5). Since certificates and cards have the same time of validity, they are dealt with together. VU certificates have either no end of, or a very long time of validity, it is assumed that the lifetime of the equipment is shorter than that of the certificate.

## 8.7 Dissemination of equipment certificates and information

[r162]The MSCA shall export all certificate data to the CIA register so that certificates, equipment and users are connected.

[r163]The CIA shall ensure that certificates are made available as necessary to users and relying parties.

[r164]The CIA shall ensure that all terms and conditions, as well as relevant parts of the MSCA PS, and other relevant information, are made readily available to all users, relying parties and other relevant groups.

## 8.8 Equipment certificate use

[r165]The Tachograph certificates are only for use within the Tachograph system.

## 8.9 Equipment certificate revocation

[r166] Certificates are not revoked.

Note: It is foreseen that rather than revoking certificates, non-valid Tachograph equipment is put on a "black list" which may be checked at roadside controls.

# 9 MSCA and CP Information Security management

This section describes the Information Security measures imposed by this policy.

| Note: This section may, at least in part, be substituted by Information Security policies for the relevant entities. |
|---|

## 9.1 Information security management of the MSCA and CP

[r167]The MSCA/CP shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

[r168]The MSCA/CP shall retain responsibility for all aspects of the provision of key certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the MSCA/CP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the MSCA/CP. The MSCA/CP shall retain responsibility for the disclosure of relevant practices of all parties.

[r169]The information security infrastructure necessary to manage the security within the MSCA/CP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the MSA.

[r170]The MSCA/CP shall adopt a security management system equivalent to ISO 17799 [ISO 17799]. Formal certification is not required.

## 9.2 Asset classification and management of the MSCA/CP

[r171]The MSCA/CP shall ensure that its assets and information receive an appropriate level of protection.

In particular:

a) The MSCA/CP shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures.

b) The MSCA/CP shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

## 9.3 Personnel security controls of the MSCA/CP

### 9.3.1 Trusted Roles

[r172][Recommended] An MSCA/CP, supporting this National CA policy, should recognize at least three distinct roles, as outlined below. Different arrangements of separation of duties may be acceptable, provided the resilience to insider attack is at least as strong as with the recommended model and provided the roles are described in the MSCA/CP PS.

[r173]To ensure that one person acting alone cannot circumvent safeguards, responsibilities in MSCA/CP systems need to be attended by multiple roles and individuals. Each account on the systems shall have limited capabilities, commensurate with the role of the account holder.

[r174]The recommended roles are:

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

[r175]The CAA/PA role includes:

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

[r176]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 shall be performed at least once per week, and the system shall 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.

[r177]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 shall be done at least once per week.

e) Personally conducting or supervising an annual inventory of the MSCA/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

[r178]For a MSCA/CP, different individuals shall fill each of the three roles described above and **at least one individual** shall be appointed per task.

### 9.3.3 Identification and Authentication for Each Role

[r179]Identification and authentication of CAA/PA, SA and ISSO shall be appropriate and consistent with practices, procedures and conditions stated in this policy.

### 9.3.4 Background, qualifications, experience, and clearance requirements

[r180]The CAA/PA (Certification Authority/ Personalization Administrator), which involves creating and managing certificate and key information, is a critical position. The individual assuming the CAA/PA role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

[r181]All MSCA/CP personnel in sensitive positions, including, at least, all CAA/PA and ISSO (Information System Security Officer) positions, shall:

a) not be assigned other duties that may conflict with their duties and responsibilities as CAA/PA and ISSO;

b) not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;

c) have received proper training in the performance of their duties.

[r182]MSCA/CP organizations may also specify special requirements such as requirements for citizenship, rank, qualifications, satisfactory credit check,

and absence of a criminal record. Such requirements should be stated in the applicable PS.

### 9.3.5 Training requirements

[r183] Personnel shall have adequate training for the role and job.

## 9.4 System security controls of the CA and personalization systems

[r184] The MSCA/CP shall ensure that the systems are secure and correctly operated, with minimal risk of failure.

In particular:
a) the integrity of systems and information shall be protected against viruses, malicious and unauthorized software;
b) damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures;

[r185] The Certification Authority System (CAS) and Personalization system shall provide sufficient system security controls for enforcing the separation of roles described in this policy or the relevant PS.

[r186] The security controls shall provide access control and traceability down to an individual level on all transactions and functions affecting the use of MSCA's private issuing keys.

[r187] [Recommended] System security controls imposed on computer systems used by Service Agencies depend on the role assigned to the agency. Agencies that undertake CAA/PA (certification authority/ personalization administrator) roles, load certificates onto cards, or initialize such cards, shall meet the requirements imposed upon MSCA/CPs.

### 9.4.1 Specific computer security technical requirements

[r188] Initialization of the system operating MSCA's private certification keys shall require co-operation of at least two operators, both of which are securely authenticated by the system.

### 9.4.2 Computer security rating

[r189] The CA and personalization systems does not require formal rating as long as they fulfil all requirements in this section.

### 9.4.3 System development controls

[r190] The MSCA/CP shall use trustworthy systems and products that are protected against modification.

[r191] An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project

undertaken by the MSCA/CP or on behalf of the MSCA/CP to ensure that security is built into IT systems.

[r192] Change control procedures shall exist for releases, modifications and emergency software fixes for any operational software.

### 9.4.4 Security management controls

[r193] The system roles (section 9.3.1) shall be implemented and enforced.

### 9.4.5 Network security controls

[r194] Controls (e.g., firewalls) shall be implemented to protect the MSCA/CP's internal network domains from external network domains accessible by third parties.

[r195] Sensitive data shall be protected when exchanged over networks which are not secure.

## 9.5 Security audit procedures

The security audit procedures in this section are valid for all computer and system components which affect the outcome of keys, certificates and equipment issuing processes under this policy.

### 9.5.1 Types of event recorded

[r196] The security audit functions related to the MSCA/CP computer/system shall 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

[r197] The log shall be processed regularly and analyzed against malicious behavior. Log procedures shall be described in the PS.

### 9.5.3 Retention period for audit log

[r198] Audit log shall be retained for at least **7** years.

### 9.5.4 Protection of audit log

[r199] Audit logs shall be appropriately integrity protected. All entries shall be individually time stamped (system time is sufficient).

[r200] Audit logs shall be verified and consolidated at least monthly. At least two people in SA or ISSO roles (see section 9.3.1) shall be present for such verification and consolidation.

### 9.5.5 Audit log backup procedures

[r201] Two copies of the consolidated log shall be made and stored in separate physically secured locations.

[r202] The audit log shall be stored in a way that makes it possible to examine the log during its retention period.

[r203] The audit log shall be protected from unauthorized access.

### 9.5.6 Audit collection system (internal vs. external)

[r204] Only internal audit collection system is required.

## 9.6 Record archiving

### 9.6.1 Types of event recorded by the CIA

[r205] The records shall include all relevant evidence in the CIA's possession including, but not limited to:

a) Certificate requests and all related messages exchanged with the MSCA/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 MSCA/CP

[r206] The records shall include all relevant evidence in the MSCA/CP's possession including, but not limited to:

a) Contents of issued certificates.

b) Audit journals including records of annual auditing of MSCA/CP's compliance with its PS.

c) Currently and previously implemented certificate policy documents and their related PSs.

[r207] Records of all digitally signed electronic requests made by MSCA/CP or Service Agency personnel (CAA/PA) shall include the identity of the administrator responsible for each request together with 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

[r208] Archives shall be retained and protected against modification or destruction for a period as specified in the PS.

### 9.6.4 Procedures to obtain and verify archive information

[r209] The MSCA/CP shall act in compliance with requirements regarding confidentiality as stated in section 3.4.

[r210] Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.

[r211] MSCA/CP shall make available on request, produced documentation of the MSCA/CP's compliance with the applicable PS according to section 11.5.

[r212] Subject to statute, a reasonable handling fee may be charged to cover the cost of record retrieval.

[r213] The MSCA/CP shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the MSCA/CP's operations are interrupted, suspended or terminated.

[r214] In the event that MSCA/CP services are to be interrupted, suspended or terminated, the MSCA/CP shall send notification to all customer organizations to ensure the continued availability of the archive. All requests for access to archived information shall be sent to the MSCA/CP or to the entity identified by the MSCA/CP prior to terminating its service.

## 9.7 MSCA/CP continuity planning

[r215] MSCA/CP shall have a business continuity plan (BCP). This shall include (but is not limited to) events such as:

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

### 9.7.1 Member State keys compromise

Member State keys compromise is dealt with in section 6.

### 9.7.2 Other disaster recovery

[r216] MSCA/CP and subcontractors shall have routines established to prevent and minimize the effects of system disasters. These routines include secure and remote backup data storage, functioning data restoration procedures etc., to be detailed in the BCP.

## 9.8 Physical security control of the CA and personalization systems

[r217] Physical security controls shall be implemented to control access to the MSCA or 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 shall be kept over all physical entries to this area (or areas).

[r218] The Member state keys for signing certificates shall be kept physically and logically protected as described in the PS.

[r219] The MSCA/CP's facility shall also have a place to store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. Backups shall be kept both for data recovery and for the archival of important information. Backup media shall also be stored at a site different from where the MSCA/CP system resides, to permit restoration in the event of a natural disaster to the primary facility.

[r220] A security check of the facility housing the MSCA/CP's central equipment shall be made at least once every **24** hours. If it is a continuously attended facility, this may be a visual check once per shift to ensure that the systems and any associated cryptographic devices/cards are securely stored if not in use, that the physical security systems (e.g., door locks and alarms) are functioning properly, and that there have been no attempts at forceful entry or unauthorized access.

### 9.8.1 Physical access

[r221] Access to the physical area housing the Member state keys and the means for their usage, shall require simultaneously presence of at least **2** persons which have been individually appointed the right to enter the area.

[r222] Access to other MSCA/CP facilities shall be limited to those personnel performing one of the roles described in section 9.3.1**Erreur ! Source du renvoi introuvable.**. Access may be controlled through the use of an access control list to the room housing the systems. Anyone not on the access control list shall be escorted by a person on the list. If an access control list is not feasible for a particular site, it may be acceptable to make sure that the CA and personalization related material is locked in a secure room or storage area when it is not being used.

# 10 MSCA or CP Termination

## 10.1 Final termination - MSA responsibility

Final termination of an MSCA or CP is regarded as the situation where all service associated with a **logical entity** is terminated permanently. It is not the case where the service is transferred from one organization to another or when the MSCA service is passed over from an old Member State key pair to new Member State key pair or ERCA key.

[r223]The MSA shall ensure that the tasks outlined below are carried out.

| Note: MSCA/CP termination implies either that a Member State withdraws from the Tachograph system or termination of the entire Tachograph system, since this cannot function without MSCAs, or equivalent authorities. |
|---|

[r224]Before the MSCA/CP terminates its services the following procedures has to be completed as a minimum:

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

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

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

d) The MSCA/CP shall perform necessary undertakings to maintain and provide continuous access to record archives by handing them over to ERCA.

## 10.2 Transfer of MSCA or CP responsibility

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

[r225]The MSA shall ensure that orderly transfer of responsibilities and assets is carried out.

[r226]The old MSCA shall transfer all root keys to the new MSCA in the manner decided by the MSA.

[r227]The old MSCA shall destroy any copies of keys that are not transferred.

# 11 Audit

[r228]The MSA is responsible for ensuring that audits of the MSCA and CP take place.

## 11.1 Frequency of entity compliance audit

[r229] An MSCA/CP operating under this National CA policy shall be audited at least annually for conformance with the policy.

## 11.2 Topics covered by audit

[r230] The audit shall cover the MSCA/CP´s practices.

[r231] The audit shall cover the MSCA/CP´s compliance with this National CA policy.

[r232] The audit shall also consider the operations of any Service Agencies.

## 11.3 Who should do the audit

[r233] The MSA may consult an external certification or accreditation organization for approval of the MSCA/CP PS in order to increase relying parties' trust in the implementation. Otherwise the MSA shall undertake the auditing.

## 11.4 Actions taken as a result of deficiency

[r234] If irregularities are found in the audit the MSA shall take appropriate action depending on severity.

## 11.5 Communication of results

[r235] Results of the audits on a security status level shall be available upon request. Actual audit reports shall not be available except on need-to-know basis.

# 12 National CA policy change procedures

## 12.1 Items that may change without notification

[r236] The only changes that may be made to this specification without notification are

a) Editorial or typographical corrections
b) Changes to the contact details

## 12.2 Changes with notification

### 12.2.1 Notice

[r237] Any item in this certificate policy may be changed with **90** days notice.

[r238] Changes to items which, in the judgment of the policy responsible organization (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.

#### 12.2.2 Comment period

[r239]Impacted users may file comments with the policy administration organization within **15** days of original notice.

#### 12.2.3 Whom to inform

[r240]Information about changes to this policy shall be sent to:

- The European Commission
- ERCA
- MSCA and CP including Service Agencies
- All other MSAs
- Affected VU Manufacturers and Motion Sensor Manufacturers

#### 12.2.4 Period for final change notice

[r241]If the proposed change is modified as a result of comments, notice of the modified proposed change shall be given at least **30** days prior to the change taking effect.

### 12.3 Changes requiring a new National CA policy approval

[r242]If a policy change is determined by the MSA organization to have a material impact on a significant number of users of the policy, the MSA shall submit the revised National CA policy to the **Commission** for approval.

## 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**”.
**Card holder:** 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 (CPS):** A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual CA policy. The CPS is in this National CA policy replaced by a Practice Statement, because it has a broader view and connects to keys, 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.
**Service Agency:** An entity that undertakes to tasks on behalf of an MSCA, a subcontractor.

**Tachograph cards/Cards:** Four different type of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.
**User:** Users are equipment users and are either **Card Holders** for card or **manufacturers** for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

**In this document:**
**Signed:** Where this policy requires a signature, the requirement is met by a secure and verifiable digital signature.
**Written:** Where this policy requires information to be in writing, that requirement is met by a data message if the information contained therein 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** | Certification Practice Statement |
| **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** |