REPUBLIC  OF CYPRUS

The National Certification Authority Policy Document for Cyprus

(CY-MSA)

Keys, certificates and equipment management

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

For the digital tachograph system

for

CY-MSA, CY-CIA, CY-MSCA and CY-CP

Published by:

The Department of Electrical & Mechanical Services,
Ministry of Communication and Works
Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus

Information:

Section of Legislation
Telephone: 00357-22800530
Telefax : 00357-22348202
E-mail: mkylilis@ems.mcw.gov.cy
Contact person: Michael Kylilis

Version: 1.1_English
Date: January 17th 2007

This document is approved by:
ERCA, JRC of the European Commission, Directorate General

History of revisions and ERCA JRC approvals

Version: 1.0_English - Approved by ERCA JRC	*Date of approval: 28 December 2006*
Version: 1.1_English - Approved by ERCA JRC	*Date of approval: 17 January 2007*

The National Certification Authority Policy Document for Cyprus

(CY-MSA)

Keys, certificates and equipment management

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

For the digital tachograph system

for

CY-MSA, CY-CIA, CY-MSCA and CY-CP

Published by:

The Department of Electrical & Mechanical Services,
Ministry of Communication and Works
Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus

Information:

Section of Legislation
Telephone: 00357-22800530
Telefax : 00357-22348202
E-mail: mkylilis@ems.mcw.gov.cy
Contact person: Michael Kylilis

Version: 1.1_English
Date: January 17, 2007

This document is approved by:
ERCA, JRC of the European Commission, Directorate General

Table of Contents

The Republic of Cyprus
Certification Authority Policy Document - (CY-MSCA)

1. INTRODUCTION

This document is the **Certification Authority Policy** of the Republic of Cyprus (hereinafter, **CY-MSA**) for the Tachograph system. Parties involved in the life cycle of certificates, tokens and applications of the Cyprus Tachograph, must follow the requirements set out in this certificate policy.

This **CY-MSA** policy meets the requirements for the management of keys, certificates and associated equipment in relation with the Tachograph system. These requirements emanate from the documents stated below:

- The Council Regulation of the Tachograph System 2135/98 of 24 September 1998 (OJ L274, 09.10.98)
- The Commission Regulation 1360/2002 of 13 June 2002 (OJ, L07, 05.08.02)
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates
- Guidelines and Template National CA Policy_Version 1.0
- European Digital Tachograph Common Security Guidelines_Version 1.0 of 05.11.2002
- Digital Tachograph System European Root Policy, Version 2.0; European Commission Special Publication I.04.131; published at http://dtc.jrc.it.

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

Tachograph system overview and responsible organizations

Tachograph system overview

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

At Member State level, a **Member State Authority (MSA)** generates a key pair (MS.SK and MS.PK). A Member State key pair is also generated in Cyprus. The European Root Certification Authority certifies public keys generated by the Cyprus **MSA** (hereinafter **CY-MSA**). The Cyprus private key is used to certify public keys used with authorized Tachograph equipment (e.g. Tachograph cards). The **CY-MSA** also manages this **CY-MSCA** certificate policy that lays out the requirements for certificate management life cycle for the tachograph system in Cyprus.

At equipment level, one single key pair (EQT.SK and EQT.PK) is generated and inserted in each piece of authorized equipment. Motion sensor keys are

placed in the workshop card, vehicle unit and motion sensor for the purpose of mutual recognition of these devices. Vehicle units placed on board vehicles carry key pairs for authentication when cards are used. Additionally key pairs are used to digitally sign data downloaded from vehicle units or Tachograph cards to external media.

A **Member State Certification Authority** (hereinafter, **MSCA**) certifies equipment public keys within the Tachograph system. Equipment manufacturers, equipment personalizing agencies and Member State authorities manage the key pair generation and insertion. The equipment key pair is used for authentication, digital signature and encryption of data within the Tachograph system.

The **Card Issuing Authority** of **Cyprus** (hereinafter, **CY-CIA**) acts as the **Registration Authority** in the Tachograph system.

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

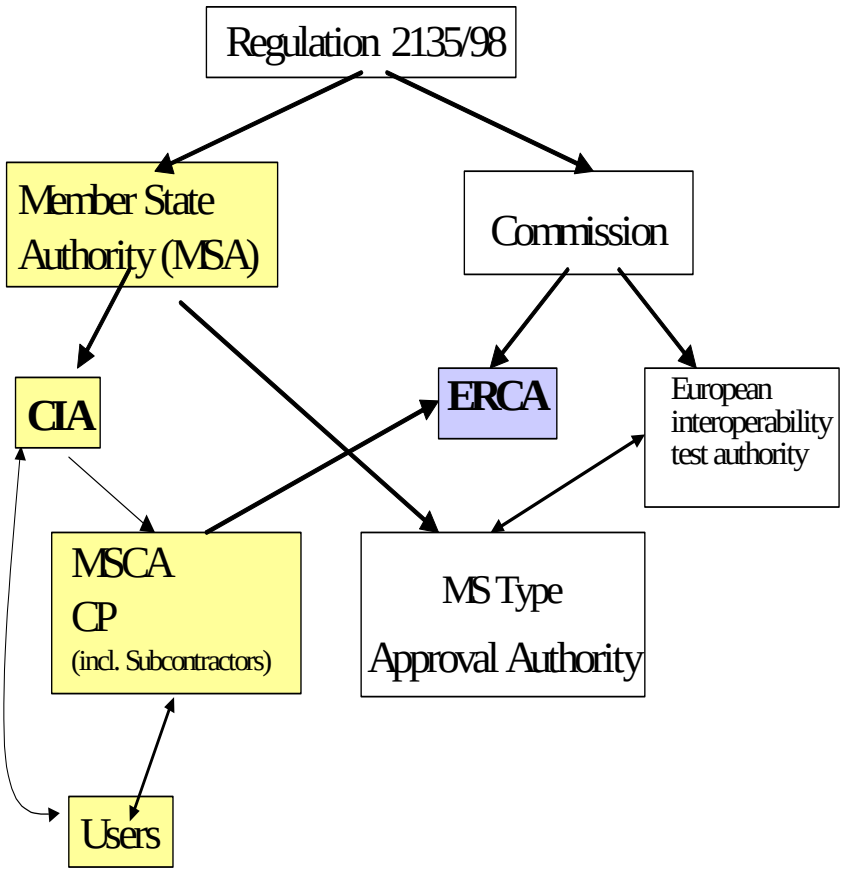

Figure 1: Tachograph system organization (coloured boxes are covered in this document)

1.1 Responsible organisations

Cyprus Member State Authority (CY-MSA)

The Republic of Cyprus has to implement the Tachograph system within its domain. The designated by the government of Cyprus organization, **Member State Authority** (hereinafter, **CY-MSA**), that has overall responsibility for issuing processes in the Tachograph system and of this **Member State Certification Authority** Policy (hereinafter, **CY-MSCA**), is:

- **The Department of Electrical and Mechanical Services**
  Ministry of Communication and Works
  Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus

Cyprus Card Issuing Authority (CY-CIA)

The Member State **Card Issuing Authority** for **Cyprus** (hereinafter, **CY-CIA**) is appointed by the **CY-MSA**, and is the organization responsible for carrying out the issuing processes. This is part of the **CY-MSA**. The appointed **Card Issuing Authority** for Cyprus is:

- **The Department of Electrical and Mechanical Services**
  Section of Legislation
  Ministry of Communication and Works
  Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus

Cyprus Member State Certification Authority (CY-MSCA)

The **Member State Certification Authority** for **Cyprus** (hereinafter, **CY-MSCA**) is also part of the **CY-MSA,** and is the organization responsible for carrying out certain parts of the issuing processes. The appointed **Member State Certification Authority** for Cyprus is:

- **The Department of Electrical and Mechanical Services**
  Section of Legislation
  Ministry of Communication and Works
  Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus

Cyprus Card Personalization (CY-CP)

The **CY-MSA** has appointed an external contractor for carrying out part of the functions of the **CY-MSA.** This contractor acts as the **Cyprus Card Personalization organization** (hereinafter, **CY-CP**), and is:

- **Chronoservices Imprimerie Nationale**
  750178Bd, Gouvion St. Cyr, 58
  Paris - France.

1.2 Approval

This **Member State Certification Authority Policy** for **Cyprus (CY-MSCA** Policy) has been approved by the **European Root Certification Authority** (hereinafter, **ERCA**), **Joint Research Center** (hereinafter, **JRC**), of the **European Commission, Directorate General, on 17 January 2007.** The complete address of the ERCA is:

- **Digital Tachograph Root Certification Authority**
  Traceability and Vulnerability Assessment Unit
  European Commission
  Joint Research Centre, Ispra Establishment (TP.360)
  Via E. Fermi, 1
  I-21020 Ispra (VA)

Table below provides a linkage of the corresponding articles of this Member State policy to the ERCA-CP §5.3 requirements.

Table

A/A	CY-MSA Ref.	Corresponding CY-MSA Title	ERCA-CP Ref.	Corresponding ERCA-CP Title
1	1.1	Responsible organisations	5.3.1	Formal requirements
2	6.2.1	Key pair generation of the CY-MSCA	5.3.2	Member State Key Pair Generation (RSA)
	6.4	Transport Keys	5.3.2	Transport Key Generation
3	6.2.1	Key pair generation of the CY-MSCA	5.3.3	Member State Key Pair Generation (RSA)
4	6.2.2	Member State keys' period of validity	5.3.4	Member State Key Pair Generation (RSA)
5	6.2.1 §10	Root Keys Management: European Root Key, Cyprus keys	5.3.5	Member State Key Pair Generation (RSA)
6	6 §6	Root Keys Management: European Root Key, Cyprus keys (Annex A of the ERCA policy)	5.3.6	ERCA Key Certification Requests and Motion Sensor Key Distribution Requests
7		Not applicable	5.3.7	ERCA Key Certification Requests and Motion Sensor Key Distribution Requests
8	6 §6	Root Keys Management: European Root Key, Cyprus keys (Annex B of the ERCA policy)	5.3.8	ERCA Key Certification Requests and Motion Sensor Key Distribution Requests
9	6 §6	Root Keys Management: European Root Key, Cyprus keys (Annex C of the ERCA policy)	5.3.9	ERCA Key Certification Requests and Motion Sensor Key Distribution Requests
10	6 §7	Root Keys Management: European Root Key, Cyprus keys	5.3.10	ERCA Key Certification Requests and Motion Sensor Key Distribution Requests
11	6.2.7	Member State Keys end of life	5.3.11	Member State Key Pair End of Life
12	6.2.1	Key pair generation of the CY-MSCA	5.3.12	Equipment RSA Keys
13	6.2.3	CY-MSCA Member State private key storage	5.3.13	RSA Key General
14	6.2	Member State key pair of the CY-MSCA	5.3.14	RSA Key General
15	6.2.4	CY-MSCA private key backup	5.3.15	RSA Key General
16	6 §6	Root Keys Management: European Root Key, Cyprus keys (Annex A of the ERCA policy)	5.3.16	RSA Key General
17	6.2.5	Member State private key escrow	5.3.17	RSA Key General
18	6.3	Motion Sensor Keys (KMwc)	5.3.18	Symmetric (TDES) Keys
19		Not applicable	5.3.19	Symmetric (TDES) Keys
20		Not applicable	5.3.20	Symmetric (TDES) Keys
21	6.3	Motion Sensor Keys (KMwc)	5.3.21	Symmetric (TDES) Keys
22		Not applicable	5.3.22	Symmetric (TDES) Keys
23	6.3	Motion Sensor Keys (KMwc)	5.3.23	Symmetric (TDES) Keys
24	6.3	Motion Sensor Keys (KMwc)	5.3.24	Symmetric (TDES) Keys
25	7	Equipment Keys (Asymmetric)	5.3.25	Certificate Generation
26	7.2	Equipment key generation	5.3.26	Certificate Generation

27	7.2	Equipment key generation	5.3.27	Certificate Generation
28	7.2	Equipment key generation	5.3.28	Certificate Generation
29	7.2	Equipment key generation	5.3.29	Certificate Generation
30	7.2	Equipment key generation	5.3.30	Certificate Generation
31	8.7	Dissemination of equipment certificates and information	5.3.31	Certificate Status Information
32	7.2.2	Equipment key validity	5.3.32	Component Personalisation
33	7.2.3	Equipment private key protection and storage-Cards	5.3.33	Component Personalisation
34		Not applicable	5.3.34	Component Personalisation
35	5.1.9	Card distribution to the user-handled by the CY-CP	5.3.35	User Registration
36	9.7	CY-MSCA and CY-CP continuity planning	5.3.36	Disaster Recovery
37	9.7	CY-MSCA and CY-CP continuity planning	5.3.37	Disaster Recovery
38	9	CY-MSCA and CY-CP Information Security Management	5.3.38	General Security Requirements
39	9.3	Personnel security controls of CY-MSCA/CY-CP	5.3.39	General Security Requirements
40	9.6	Record archiving	5.3.40	General Security Requirements
41	10	CY-MSCA or CY-CP Termination	5.3.41	General Security Requirements
42	12	CY-MSCA and CY-CP Certificate Policy change procedures	5.3.42	General Security Requirements
43	11.2	Topics covered by the Audit	5.3.43	Audit
44	11.1	Frequency of entity compliance audit	5.3.44	Audit
45	11.5	Communication of results	5.3.45	Audit
46	11.4	Actions taken as a result of deficiency	5.3.46	Audit

1.3 Availability and contact details

This **CY-MSCA** certificate policy is publicly available at:

- **Internet address: http//: www.mcw.gov.cy/ems**

Questions concerning this **CY-MSCA** certificate policy may be addressed to the designated **CY-MSA** to the following address:

- **The Department of Electrical and Mechanical Services**
  Section of Legislation
  Ministry of Communication and Works
  Ayiou Ilarionos, Pallouriotissa, 1426 Nicosia-Cyprus
  Tel. 00357-22800530, Fax. 00357.22348202
  E-mail: mkylilis@ems.mcw.gov.cy

2. SCOPE AND APPLICABILITY

- This policy applies to the domain of the **CY-MSCA** that carries out certificate management operations within the Tachograph system in Cyprus.
- The **CY-MSCA** certificates can be used within the Tachograph system only to the exclusion of any other. The certificates issued in the Tachograph system can be used for specific electronic Tachograph purposes within the Tachograph system.
- The keys and certificates issued by the **CY-MSCA** are exlusively intended to be used within the Tachograph system.
- The cards issued by the **CY-CIA** are exlusively intended to be used within the Tachograph system.

The scope of the Cyprus Certification Authority Policy **(CY-MSCA)** within the Tachograph system is presented in figure 2 below.

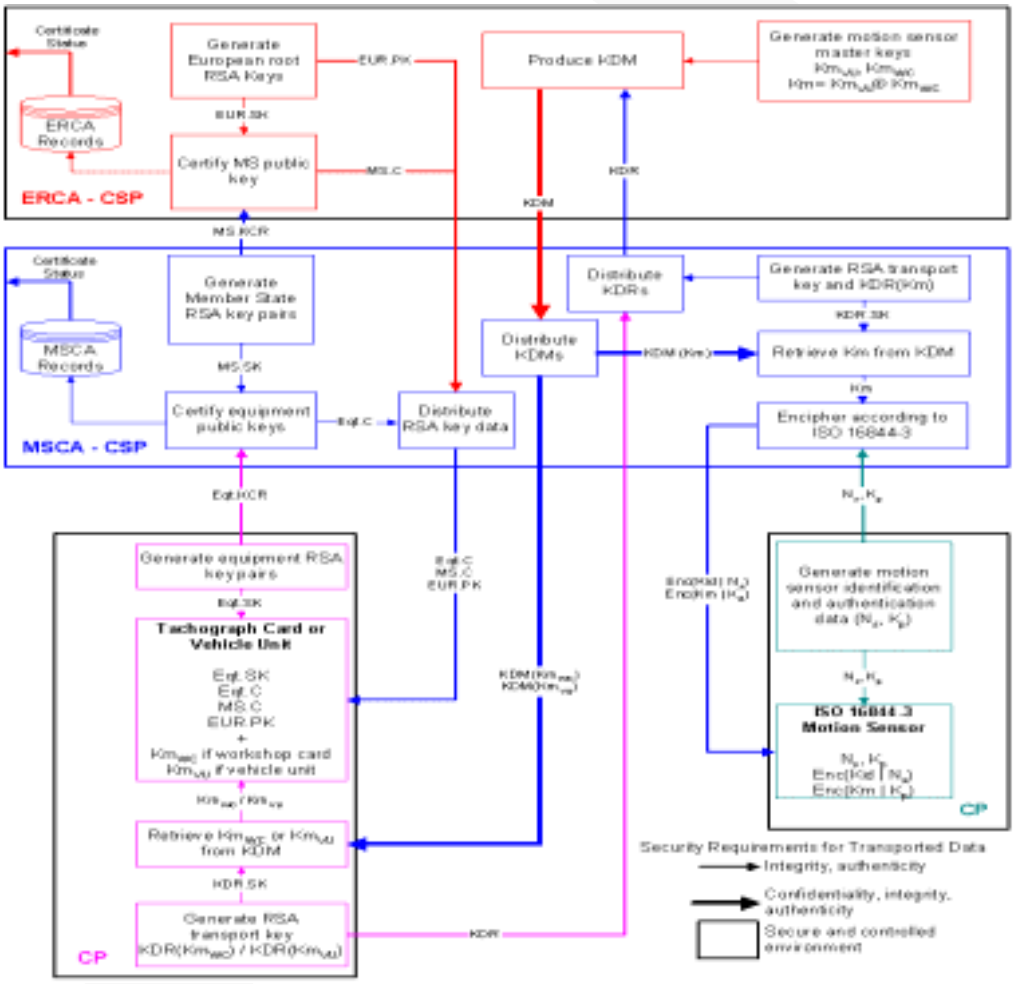

Figure 2: Tachograph system keys, certificates and equipment management. (Scope of policy is marked with bold lines.)[1]

[1] *Not applicable at the moment for Vehicle Unit and Motion Sensor.*

Four entities are depicted: the **ERCA** certification service provider (hereinafter, **ERCA CSP**); the Cyprus **MSCA** certification service provider (**CY-MSCA CSP**); and the two types of component personaliser (hereinafter, **CP**); tachograph card (**CY-CP**). With the exeption of the **ERCA**, assertions in this **CY-MSCA** policy are binding to all these entities.

The **ERCA** and the **CY-MSCA** create and maintain appropriate secret encryption keys and use them to validate digital tachograph security data, only after verifying that the data to encrypt are complete, correct, and duly authorized. The card **CP** inserts validated security data into digital tachograph equipment by appropriately secured means.

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

- Authentication of transmissions between vehicle units and cards.
- Transport of session keys between vehicle units and Tachograph cards.
- Digital signature of data downloaded from vehicle units or Tachograph cards to external media.

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

Within the Tachograph system the policy components follow the layout and interactions that are presented in figure 3 below:

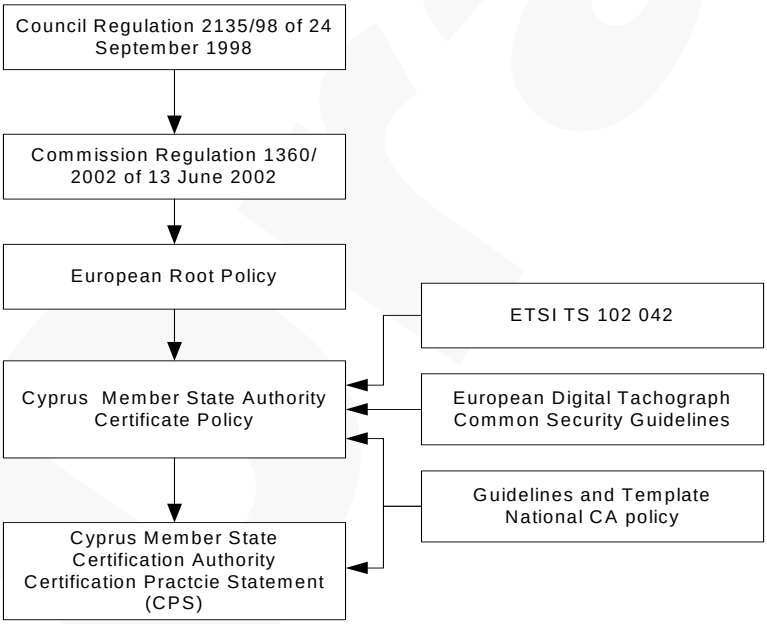

Figure 3: Tachograph system policy components

At European level the **European Root Policy** sets out the conditions to be followed by Member State Authorities with competence over the Tachograph system within their respective states. Within Cyprus this **CY-MSA CP** provides guidance with regard to the conditions prevailing in the lifecycle management of

the Tachograph system components. The **CY-MSCA CPS** stipulates the conditions for the lifecycle management of certificates and components of the Tachograph system in Cyprus.

Normative input is provided through the following documents:

- The Council and Commission's Regulations (Annex 1B–Requirements for construction, testing, installation and inspection) as detailed in Commission Regulation (EC) No. 1360/2002 of 13 June 2002, adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport.
- The European Digital Tachograph Common Security Guideline_V1.0 of 5 Nov. 2002) and the Guidelines and Template for National CA Policy_V1.0 of 31st Oct. 2002.
- The standard ETSI_TS 102 042_V1.1.1 (April 2002), Policy requirements for certification authorities issuing public key certificates.

3. GENERAL PROVISIONS

This section contains provisions relating to the respective obligations of **CY-MSA, CY-CIA, CY-MSCA, CY-CP, end-users**, and **other issues** pertaining to law and dispute resolution. Discreet references to the **CY-MSA** are made in order to meet with the requirements of the operational environment.

3.1 Obligations

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

- **CY-MSA** and **CY-CIA**
- **CY-MSCA**
- **CY-CP**
- Users (Cardholders)

3.1.1 CY-MSA and CY-CIA obligations

With regard to this policy the **CY-MSA** and the **CY-CIA** has the following obligations:

The CY-MSA shall:

- Maintain the **CY-MSA** Policy.
- Appoint a **CY-MSCA** and a **CY-CP**.
- Audit the appointed **CY-MSCA** and **CY-CP**.
- Approve the Certification Practice Statement of the **CY-MSCA** and the **CY-CP**.
- Inform the appointed parties about this policy.
- Submit this policy to the **European Commission** to seek approval.

The CY-CIA shall:

- Ensure that correct and pertinent user information is input to the **CY-MSCA** and the **CY-CP**.
- Inform the **users** of the requirements in this policy certificate policy connected to the use of the system, i.e. the Cardholders.

3.1.2 CY-MSCA obligations

The appointed CY-MSCA shall:

- Follow this **CY-MSA** Policy
- Publish a **CY-MSCA** Practice Statement (**MSCA PS**) that includes reference to this **CY-MSA** Policy and which is to be approved by the **CY-MSA**.
- Implement the requirements specified in the **CY-MSCA** Certification Practice Statement.
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in the **CY-MSA** Policy, in particular to bear the risk of liability damages.
- The **CY-MSCA** has the responsibility for conformance with the procedures prescribed in this certificate policy, also when subcontractors undertake certain functions pertaining to the role of the **CY-MSCA** in part or whole.
- The **CY-MSCA** will make certificate status information available for publication or through any other appropriate mechanism approved by **ERCA**.

The **CY-MSCA** has no further obligations.

3.1.3 CY-CP obligations

The appointed CY-CP (card personalization organization) has to:

- Follow this **CY-MSA** Policy
- Publish a **CY-CP Practice Statement** (**CY-CP PS**) that includes reference to this **CY-MSA** Policy and which is to be approved by the **CY-MSA**.
- Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this **CY-MSCA** certificate policy, in particular to bear the risk of liability damages.
- The **CY-CP** shall ensure that all requirements on the Business Continuity Plan (BCP) addressed in this **CY-MSCA** certificate policy are implemented as appropriate.
- The **CY-CP** has the responsibility for conformance to the procedures prescribed in this certificate policy, even when external contractors undertake the **CP** functionality.

3.1.4 Service Agency obligations

Not applicable.

3.1.5 Cardholder obligations

The **CY-CIA** shall oblige, through agreement (see 5.1.2), the user (or user's organization) to fulfil the following obligations:

- To submit accurate and complete information to the **CY-CIA** in line with the requirements on registration or any other requirements set out in this certificate policy.
- To use the keys and certificates only within the Tachograph system.
- To use the Tachograph cards only within the Tachograph system.
- To exercise reasonable care in order to avoid unauthorized use of the equipment, including the Tachograph private key and the Tachograph card.
- To use only his personal keys, certificate and card (Regulation14.4.a).
- To only have one valid driver card at any time (Regulation14.4.a).

- A user may only under very special, and duly justified, circumstances have both a workshop card and a hauling company card (Annex 1B_VI:1); or both a workshop card and a driver card; or several workshop cards. The possession of multiple Tachograph cards has to be duly justified by the circumstances and it might be subject to specific authorisation by the designated **CY-CIA**.
- To refrain from using a damaged or expired card (Regulation14.4.a).
- To promptly notify the **CY-CIA** up to the end of the validity period indicated in the certificate if:
  - The equipment private key or card has been lost, stolen or potentially compromised (Regulation15.1); or
  - The certificate content is, or becomes, inaccurate.

3.1.6 VU manufacturers´ obligations

Not applicable

3.1.7 Motion Sensor manufacturers´ obligations

Not applicable

Relying parties

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

3.2 Liability

The **CY-MSCA** and **CY-CP** do not carry liability towards end users, only towards the **CY-MSA** and **CY-CIA**.

Liability issues towards end users are dealt with by of the **CY-MSA** and **CY-CIA**.

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

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

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

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

With regard to Tachograph certificates the **CY-MSCA** warrants that:

- The information contained in the certificate at the time of issuance is accurate and the same as the information delivered to the **CY-MSCA** by the **CY-MSA**.
- The certificate contains all information required for a Tachograph certificate at the time of issuance. The **CY-CIA** warrants correct input to the **CY-MSCA**.
- The **CY-CP** holds the private key corresponding to the public key identified in the certificate request. The **CY-CP** takes all precautions necessary to ensure correct input to the **CY-MSCA**.

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

The **CY-MSCA** takes adequate measures to meet its potential responsibilities, resulting from its activities, in particular to risk, including any financial risk, as a result of liability for damages. The **CY-MSCA** has adequate financial means and stability at its disposal to meet the requirements in accordance with this certificate policy.

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

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

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

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

3.2.1 Limitations of Liability

Within the limits permitted by law the total liability of the **CY-CA** is limited in accordance with the provision of section 3.1.1 of this certificate policy.

3.2.2 Severability

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

3.3 Interpretation and enforcement

3.3.1 Governing Law

The laws of the Republic of Cyprus govern this **CY-MSA** certificate policy.

Miscellaneous Provisions

The certificate policy incorporates by reference the following information:

- Terms and conditions in this certificate policy.

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

3.4 Confidentiality and personal data

Confidentiality is restricted according to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the movement of such data. The Tachograph services meet the requirements of the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L281, 23/11/1995 p. 0031 – 0050), and of the corresponding law of the Republic of Cyprus (Law 138(I)/2001), implementing this directive. The Tachograph services also meet the requirements of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and of the corresponding law of the Republic of Cyprus (Law 112(I)/2004), (OG App. I (I), No. 3850, 30/04/2004), implementing this directive. In general this legislation specifies that a person or organization, which collects personal identifiable information, is required to:

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

With regard to the current legislation of the Republic of Cyprus on the protection of personal data, further information can be obtained from the website of the Office of the Commissioner for Personal Data Protection:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/

3.4.1 Types of information to keep confidential

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

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

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

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

3.4.1.1 Disclosure of confidential information

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

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

Confidential information is not released without the prior consent of the user, or (where applicable) the prior consent of the user's employer or representative, unless required otherwise by Law.
Parties requesting and receiving confidential information are granted permission on the explicit assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

3.4.1.2 Confidential communications

All communications of personal or confidential information are encrypted including:

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

3.4.2 Types of information not considered confidential

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

3.4.2.1 Accessing non-confidential information

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

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

4. CERTIFICATE PRACTICE STATEMENT (CPS)

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

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

- The Certification Practice Statement shall identify the obligations of all external organizations supporting **CY-MSCA** and **CY-CP** services including the applicable policies and practices.
- The Certification Practice Statement shall be made available to the **CY-MSA**, to users of the Tachograph system, and to third parties (e.g. control bodies). The Certification Practice Statement of the **CY-MSCA** and the **CY-CP** does not necessarily make all details on practices publicly available to all users. Additional information regarding the policies and practices of the **CY-MSCA** and the **CY-CP** can be sought directly through the communication address provided elsewhere in this document.
- The management of the **CY-MSCA** and the **CY-CP** ensures that the Certification Practice Statement is properly implemented.
- The Certification Practice Statement of the **CY-MSCA** and the **CY-CP** shall define a review process.
  a) The **CY-MSCA** and the **CY-CP** shall give due notice on changes they make to the Certification Practice Statement and following approval make the revised certificate policy immediately available. Minor revisions may be released without **CY-MSA** approval.
  b) An approved Certification Practice Statement meets the requirements of **ERCA** and the **CY-MSA**. Additional policy limitations might apply as stipulated by Law or through agreements with **MSAs** from other member states.
- The Certification Practice Statement becomes binding for the applicant of the service, pursuant to an application for service according to the forms to be found in the Departments District Offices.

4.1 Review process

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

4.1.1 Versions

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

4.1.2 Policy updates

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

5. EQUIPMENT MANAGEMENT

The equipment in the Tachograph system includes the following items:

- Tachograph cards

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

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

The following functions are carried out by the **CY-MSA**:

- Quality control (type approval)

The following functions are carried out by the **CY-CIA**:

- Applications for cards
- Application approval registration
- Equipment registration and data storage (DB)

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

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

5.1 Tachograph cards

5.1.1 Quality control

The **CY-MSCA/CP** shall ensure that only type-approved cards according to the Council Regulation 2135/98 are personalized in the Tachograph system. See also 5.1.7.5

The card certificate for the hardware of the cards adopted is identified as: “CERTIFICAT 2003/12, ICitizen Tachograph: Carte tachygraphique version 0.9.0 (référence M256LFCHRON_SI_A5_05_01); Développeurs: Schlumberger Systèmes, Infineon Technologies AG, both issued by: Le Directeur central de la sécurité des systèmes d’information and dated 27 Aug. 2003 and rév. B dated 01 Mar. 2006.

5.1.2 Application for card – handled by the CY-CIA

The **CY-CIA** shall inform the user of the terms and conditions regarding the use of the card. This information is available in a readily understandable language being Greek and English.

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

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

5.1.2.1 User application

Applicants for a Tachograph card shall fill out a standard application form. The content of the application form is determined by the **CY-MSA**. To have a card

issued the following information is required unless it can be collected from other sources:

Driver card specific:

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

In case of replacement or renewal of the card:

- Card number.

Workshop card specific:

Workshop cards are issued to natural persons only in their capacity as agents of a legal person authorised to take part in the Tachograph system. Workshop cardholders must provide the following evidence:
Workshop data:
Full name and legal status of the associated legal person or other organizational entity;
Abbreviated name;
Postal address;
Phone number;
Fax number;
E-mail address;
Company identification number (when applicable)[3].
Card holder data:
Gender;
Full name (including surname and given names) of the user;
Date and place (city and country) of birth, reference to a nationally recognized identity document, or other attributes of the user which may be used to, as far as possible, distinguish the person from others with the same name;
Place of residence;
National identification number (if any);

In case of replacement or renewal of the card:

- Card number.

Control body card specific:

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

[3] The Department of Registrar of Companies and Official Receiver issues a unique identification number for each registered company in Cyprus.

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

In case of replacement or renewal of the card:

- Card number.

Company card specific:

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

Company data:
Full name and legal status of the associated legal person or other organizational entity;
Abbreviated name;
Postal address;
Phone number;
Fax number;
E-mail address;
Company identification number (when applicable)[4].
Amount of cards asked.
Card holder data:
Full name (including surname and given names) of the user;
Function;
Full name and legal status of the associated legal person or other organizational entity;

In case of replacement or renewal of the card:

- Card number.

5.1.2.2 Agreement

The applicant shall, by making an application for a card and accepting delivery of the card, make an agreement with the **CY-MSA** (or **CY-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 **CY-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 **CY-CIA** relevant for the information in the card is true.

[4] The Department of Registrar of Companies and Official Receiver issues a unique identification number for each registered company in Cyprus.

- The card is being conscientiously used in consistence with usage restrictions for the card

5.1.2.3 CY-CIA terms of approval - Driver card specific

- A Driver card shall only be issued to individuals having permanent residence in the country of application.
- The **CY-CIA** shall ensure that the applicant does not have a valid Driver card issued in another Member State.
- The **CY-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 CY-CIA

The validity period commences on the date of issuance of a card.

- Workshop cards are valid for no more than **one (1)** year from issuance (Regulation 12.1).
- Driver cards are valid for no more than **five (5)** years from issuance (Regulation 14.4.a).
- Company cards are valid for no more than **five (5)** years from issuance.
- Control Cards are valid for no more than **two (2)** years.
- An application for renewal follows section 5.1.2

5.1.3.1 Driver cards

- The user shall apply for a renewal card at least **15** working days prior to card expiration. (Regulation article 15.1)
- If the user complies with the above rule, the **CY-CIA** will issue a new driver card before the current card expires. (Regulation article 14.4.a).

5.1.3.2 Workshop cards

- The user shall apply for a renewal card at least **15** working days prior to card expiration.
- The **CY-CIA** will issue a renewal card within **5** working days of receiving a complete application. (Regulation article 12.1)

5.1.3.3 Company cards

- The user shall apply for a renewal card at least **15** working days prior to card expiration.
- If the user complies with the above rule, the CY-CIA will issue a new company card before the current card expires.

5.1.3.4 Control cards

- The user shall apply for a renewal card at least **15** working days prior to card expiration.
- The **CY-CIA** will issue a renewal card within **5** working days of receiving a complete application.

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

- A user who changes country of residence may request to have his/her driver card exchanged.
  If the current card is valid, the user shall only show proof of residence in order to have the application granted.

- The **CY-CIA** shall upon delivery of the new card take possession of the previous card and send it to the MSA of origin. (Regulation article 14.4.c)
- Card exchange due to changed country of residence shall otherwise follow the rules for new card issuing.

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

- If a card has been lost or stolen, the user shall report this to the local Police and receive a copy of the report. Loss of card may be reported by the user, or by the Police upon receiving a found card. The Police shall without delay notify the issuing **CY-CIA** of the report.
- Stolen and lost cards are reported on a directory put on a blacklist accessible by all Member States authorities.
- Damaged and malfunctioning cards are delivered to the issuing **CY-CIA**. They are subsequently visually and electronically cancelled and reported on a directory.
- If the card is lost, stolen, damaged or malfunctioning, the user applies for a replacement card within **7** days. (Regulation article 15.1)
- The CY-CIA then issues a replacement card with new key pairs and certificate within **5** working days from receiving a complete application. (Regulation article 14.4.a)
- The replacement card has the same validity period as the card that has been lost or stolen, unless the card has less than **four (4)** months remaining validity, in which case a replacement card is issued instead. (Regulation Annex 1B: VII).

5.1.6 Application approval registration – handled by the CY-CIA

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

5.1.7 Card personalization – handled by the CY-CP

- Cards are personalized both visually and electronically.

5.1.7.1 Visual personalization

- Cards are visually personalized according to Regulation Annex 1B, section IV.

5.1.7.2 User data entry

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

5.1.7.3 Key entry

- The private key will be created on the card during the personalisation. This solution will guarantee that no person, in any way whatsoever, can get control of the generated private key. See also equipment key management, 7.2.

5.1.7.4 Certificate entry

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

5.1.7.5 Quality Control

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

5.1.7.6 Cancellation (destruction) of non-distributed cards

- Cards that are damaged or destroyed (or for other reasons are not finalized and distributed) during personalization shall be physically and electronically destroyed (cancelled) (CRL).
- All destroyed cards shall be registered in a cancellation blacklist (CRL).

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

- The **CY-CP** is responsible for keeping track of which card and card number is given to which user. This linkage data is transferred from the **CY-CP** to the **CY-CIA** in a secure way.

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

- The personalisation cards are kept in a secure and safe environment. ISO 9000/2000 documented procedures are implemented for the exception handling, including outages in the production process, failure of delivery, and loss of or damage to cards.
- Personalized cards are immediately transferred to the place where they are delivered or distributed to the user, i.e. a district area.
- Personalized cards shall always be kept separated from non-personalized cards.
- The Tachograph cards shall be distributed in a manner that offers a reasonable guarantee of delivery to the end user.
- At the point of delivery of a card to a user, proof of that user's identity (e.g. name) is checked against a physical person.
- The user shall present valid means of identification.
- The user's signature shall acknowledge the reception of the card.

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

This section applies only to Workshop cards.

- Workshop cards have a PIN code, used for authenticating the card to the Vehicle unit (Regulation Annex 1B, App 10: Tachograph cards: 4.2.2)
- PIN codes consist of 4 digits (Regulation Annex 1B, App 10: Vehicle Units: 4.1.2).

5.1.10.1 PIN generation

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

5.1.10.2 PIN distribution

- PIN codes shall be distributed separately with the corresponding cards.
- At the point of delivery of the pin codes to a user, proof of that user's identity (e.g. name) is checked against a natural person.
- The pin code of a workshop card shall be distributed to the end user in a manner that minimizes the risk of unauthorized persons accessing the code without it being noticed by the end user.

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

- The **CY-CIA** may permanently deactivate cards and key pairs by using dedicated equipment and keeping appropriate records of its actions. The **CY-CIA** may permanently deactivate a card and any keys residing thereon. A decision of deactivation is taken and carried out by the **CY-MSA** or the **CY-CIA**, but the actual operation is carried out by the **CY-CP**.
- Deactivation of cards takes place in equipment suitable for the operation and it is verified that card functions and keys are destroyed. The card is also visually cancelled.
- Deactivation of cards is registered in the card database and the card number is recorded on a blacklist (CRL).

5.2 Vehicle Units and Motion Sensors

5.2.1 Quality control - CY-CIA function

Not applicable

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

Not applicable

5.2.2.1 Vehicle Units

Not applicable

5.2.2.2 Motion Sensors

Not applicable

5.2.3 Application approval registration – handled by the CY-CIA

Not applicable

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

Not applicable

5.2.5 VU personalization – handled by the VU manufacturers

Not applicable

5.2.5.1 Key entry

Not applicable

5.2.5.2 Certificate entry

Not applicable

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

Not applicable

5.2.7 VU distribution – handled by VU manufacturers

Not applicable

5.2.8 VU renewal

Not applicable

5.2.9 Replacement of lost, stolen, damaged or malfunctioning VUs

Not applicable

5.2.10 End of life of VUs

Not applicable

6. ROOT KEYS MANAGEMENT: EUROPEAN ROOT KEY, CYPRUS KEYS

This section contains provisions for the management of

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

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

The **CY-MSCA** keys are the Member State signing keys for Cyprus and may also be called **Member State Cyprus root keys**.

The **Transport keys** are the keys used for securely exchanging information between the **ERCA** and the **CY-MSCA**.

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

The **CY-MSA** shall follow the procedures, formats and/or media prescribed by **ERCA**[5] (see Annexes A, B, and C of the ERCA Policy) in:

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

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

The **CY-MSA** recognizes the **ERCA** public key in the prescribed distribution format.

The **CY-MSCA** follows strict audited guidelines with regard to the practices and operations associated with key management. For all keys it issues (i.e. **CY-MSA** keys, being **CY-MSCA** keys for the Tachograph cards) the following policies apply:

[5] *Digital Tachograph System European Root Policy Version 2.0, Special Publication I.04.131.*

- **CY-MSCA** Key Management policy
- **CY-MSCA** Key Management procedures
- **CY-MSCA** Security Policy

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

- Transportation of private keys during key certification request is forbidden.

6.1 ERCA public key

- The **CY-MSCA** ensures the integrity and availability of the **ERCA** public key (EUR.PK) at all times.
- The **CY-CP** ensures that EUR.PK is inserted in all Tachograph cards.

6.2 Member State key pair of the CY-MSCA

The Member State keys are the **CY-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 **CY-MSCA** generates its own key pair and submits it to **ERCA** for certification. The **MSCA** shall keep the **ERCA** public key (EUR.PK) in such a way as to maintain its integrity and availability at all times. If the EUR.PK is stored in the **CY-CP**, the same rule applies.

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

The **CY-MSCA** signs equipment certificates within the same device used to store the Member State Private Keys.

6.2.1 Key pair generation of the CY-MSCA

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

The Key pair of the **CY-MSCA** is generated in a device which meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]].

This is a security target or protection profile that meets the requirements of this certificate policy based on risk analysis and taking into account physical and other non-technical security measures.

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

The key generation system should be stand-alone.

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

The Key pair of the **CY-MSCA** is generated in a device identified as:
Secure Generic Sub-System (SGSS) Version 3.2, by Thales e-Security-UK, (Hardware Versions: 1213B130, Rev. 2 and 1213D130, Rev. 3a; Software Version: 2.0.2; Hardware), validated to FIPS 140-2. Security Policy Certificate,

Vendor Product Link: Hardware 09/07/2005; 10/13/2005; Overall Level:3-FIPS-approved algorithms:DSA/SHS(Cert.#24); RSA(Cert. #53)-Other algorithms: N/A; Multi-chip embedded "The Secure Generic Sub-System (SGSS) is a multi-chip embedded module used to provide secure cryptographic resources to a number of products in the Thales e-Security portfolio. This includes the Datacryptor 2000 family, WebSentry family, HSM 8000 family, P3CM family, PaySentry, 3D Security Module and SafeSign Crypto Module. The SGSS contains a secure bootstrap and authenticates application loading using the Digital Signature Algorithm (DSA) and the RSA algorithm."

The **CY-MSCA** key-pair generation requires the active participation of **three (3)** separate actors. At least one of them has a role as **CAA/PA** (a certification authority/personalization administrator) and the remaining have trusted roles (see section 9.3.1 for role descriptions).

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

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

The generation of replacement Member State key pairs shall take into account the one month turn-around time required for certification by **ERCA.**

6.2.2 Member State keys' period of validity

- The maximum usage period of private keys is set to **two (2)** years starting from the issuance of a certificate by **ERCA** certifying the corresponding public key. And shal not be used after its validity period for any purpose.
- The corresponding public key will have no end of validity.

6.2.3 CY-MSCA Member State private key storage

- The operational private keys are contained in and operated from inside a tamper resistant device that:
  - Meets the requirements of FIPS 140-2 (or 140-1) level 3 or higher [FIPS].
  - There are security targets or protection profiles that meet the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
  - Dual control is required to access the **CY-MSCA** private signing keys. This means that no single person shall posess 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 CY-MSCA private key backup

- The **CY-MSCA** private signing keys may be backed up. However, the solution used for Business Continuity, is to have several keys as stated in § 6.2.1.

6.2.5 Member State private key escrow

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

6.2.6 Member State keys compromise

- If the private keys for Cyprus are considered or suspected to be compromised documented guidelines outline the measures to be taken by users and security staff at the **CY-MSCA**.
- In such case the **CY-MSCA** informs the **CY-MSA, ERCA** and all other **MSCAs**.

6.2.7 Member State keys end of life

- The **CY-MSCA** has documented procedures to ensure that it always has a valid, certified signing key pair for Cyprus.
- Upon termination of use, the **CY-MSCA** signing keys are unloaded from the online production chain and are stored offline in a secure environment under dual control and split knowledge.
- The online production system software is designed to prevent use of expired keys by checking validity and usability periods of **CY-MSCA** keys prior to end entity certificate issuance.
- The **CY-MSCA** applies procedures to ensure that at end of life keys are handled in a physically secured environment by personnel in trusted roles under, at least dual control. Additional conditions apply as prescribed in the **CY-MSCA**:
  - **CY-MSCA** Key Management policy
  - **CY-MSCA** Key Management procedures
  - **CY-MSCA** Security Policy

6.3 Motion Sensor keys

The **CY-MSA** shall, as needed, request the workshop key KMwc from **ERCA** following the procedures defined in **ERCA** Policy Annex D.

The **CY-MSA** shall prevent the unauthorized use of the Motion Sensor Master Keys.

The **CY-MSA** shall ensure that the KMwc key is only forwarded, by appropriately secured means, to **CY-CP** for the sole purpose of insertion into workshop cards.

If a KMwc has been exposed or is otherwise considered or suspected to be compromised, the suspecting organization (**CY-MSCA** or **CY-CP**) shall inform the **CY-MSA** and ERCA without delay.

CY-MSA shall ensure that KMwc shall be stored within a device which is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher.

The **CY-CP** shall ensure that the workshop key KMwc is inserted into all workshop cards.

6.4 Transport keys

CY-MSA Key Pairs for motion sensor master key distribution (transport keys) shall be generated and stored within a device which is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher;
The Key Distribution Requests (**KDR**) needs accordingly to be generated by the Component Personalizer (**CP**) (Tachograph Cards manufacturers). The **MSCA** will validate the **CP KDR** by checking conformity as per European Root Policy Annex D and forward it to the **CY-CA** for further processing by **ERCA**. The **ERCA** shall ensure that **MSCA** public key certification requests are complete, accurate, and duly authorized.

CY-MSA Key Pairs for Motion Sensor Key distribution shall be generated in a physically secured environment by personnel in trusted roles under, at least dual control.

CY-MSA shall ensure the uniqueness, within its domain, of the Key Identifier (KID) and the Modulus (n) of the Key Pairs for Motion Sensor Key distribution.

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

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

7. EQUIPMENT KEYS (ASYMMETRIC)

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

- Tachograph cards

Symmetric Motion Sensor keys are not handled here.

7.1 General aspects CY-CP/ CY-MSCA

- Equipment initialisation, key loading and personalisation are carried out in a physically secure and controlled area. Entry to this area is strictly controlled and requires the presence of minimum two persons to operate the system. A log file is compiled with reference to the entries and the actions in the system.
- No sensitive information contained in the key generation systems may leave the system unless as provided in this certificate policy.
- Tachograph cards: No sensitive information in the card personalization system may leave the system in a way that violates this policy.
- **Organizations (Subcontractors)** that carry out key generation and card personalization on behalf of more than one Member State separate the processes for each one of them. A log is kept of each individual process and the **CY-MSA** has access to it on request.
- **CY-MSCA/ CY-CP:** Logs of the personalisation system contain a reference to the order, and list the corresponding equipment numbers and certificates. The **CY-MSA** has access to it.

7.2 Equipment key generation

Keys may be generated either by the **CY-CP** or by the **CY-MSCA**. (Annex 1B, Appendix 11:3.1.1)
The entity that performs the key generation makes sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

The Key generation is carried out within a device identified as: Secure Generic Sub-System (SGSS) Version 3.2, by Thales e-Security-UK, (Hardware Versions: 1213B130, Rev. 2 and 1213D130, Rev. 3a; Software Version: 2.0.2; Hardware), validated to FIPS 140-2. Security Policy Certificate, Vendor Product Link: Hardware 09/07/2005; 10/13/2005; Overall Level:3-FIPS-approved algorithms:DSA/SHS(Cert.#24); RSA(Cert. #53)-Other algorithms: N/A; Multi-chip embedded "The Secure Generic Sub-System (SGSS) is a multi-chip embedded module used to provide secure cryptographic resources to a number of products in the Thales e-Security portfolio. This includes the Datacryptor 2000 family, WebSentry family, HSM 8000 family, P3CM family, PaySentry, 3D Security Module and SafeSign Crypto Module. The SGSS contains a secure bootstrap and authenticates application loading using the Digital Signature Algorithm (DSA) and the RSA algorithm."

The device meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS].
This is assured be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
Keys are generated using the **RSA** algorithm having a key length of modulus *n* 1024 bits. (Annex 1B, Appendix 11:2.1/3.2)

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

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

7.2.1 Batch key generation

- Cryptographic key generation may be performed by batch processing in advance of certificate request, or in direct connection with certificate request.
- Batch processing must be performed in stand-alone equipment meeting the security requirements stated above. Key integrity has to be protected until certificate issuing is concluded.

7.2.2 Equipment key validity

7.2.2.1 Keys on cards

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

7.2.2.2 Vehicle units

Not applicable

7.2.3 Equipment private key protection and storage - Cards

- The **CY-CP** ensures that the card private key is protected by, and restricted to, a card that has been delivered to the user according to the procedures stated in this policy.
- Copies of the private key may only be kept on the Tachograph card.
- In no case may the card private key be exposed or stored outside the card.

7.2.4 Equipment private key protection and storage – VUs

Not applicable

7.2.5 Equipment private key escrow and archival

- Equipment private keys neither is escrowed nor archived.

7.2.6 Equipment public key archival

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

7.2.7 Equipment keys end of life

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

8. EQUIPMENT CERTIFICATE MANAGEMENT

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

8.1 Data input

8.1.1 Tachograph cards

Cardholding users have their certificates issued on the basis of information submitted with the application for a Tachograph card and captured from a **CY-CIA** register.

The **CY-CP** ensures that input data contains information that renders the Certificate Holder Reference (**CHR**) unique. The **CY-MSCA** ensures the uniqueness of the Certificate Holder Reference (**CHR**) within its own domain.

8.1.2 Vehicle units

Not applicable

8.2 Tachograph card certificates

8.2.1 Driver certificates

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

8.2.2 Workshop certificates

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

8.2.3 Control body certificates

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

8.2.4 Company certificates

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

8.3 Vehicle unit certificates

Not applicable

8.4 Equipment certificate time of validity

Not applicable

8.5 Equipment certificate issuing

- The **CY-MSCA** ensures the authenticity and integrity of the certificates it issues. Certificate contents are defined by Regulation Annex 1B, appendix 11.

8.6 Equipment certificate renewal and update

- See Equipment management (section 5). Certificates and cards have the same validity period; therefore, they are managed together. The lifetime of the equipment is shorter than that of the certificate.

8.7 Dissemination of equipment certificates and information

- The **CY-MSCA** exports all card related certificate data to a **CY-CP** register so that certificates, equipment and users are connected**.**
- The **CY-CIA** ensures users, relying parties and other stakeholders that:
  - Certificates are made available through an accessible directory.
  - Terms and conditions, as well as relevant parts of the **CY-MSCA** certificate policy are made available.

8.8 Equipment certificate use

- The Tachograph certificates are only used within the Tachograph system.

8.9 Equipment certificate revocation

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

8.10 Certificate Content

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

Data	Format	Bytes	Obs
CPI	INTEGER	1	Certificate profile identifier (¡01¡ for this version)
CAR	OCTET STRING	8	Certification authority reference
CHA	OCTET STRING	7	Certificate holder authorisation

EOV	*TimeReal*	4	Certificate end of validity. Optional, ¡FF¡ padded if not used
CHR	OCTET STRING	8	Certificate holder reference
n	OCTET STRING	128	Public key (modulus)
e	OCTET STRING	8	Public key (public exponent)
Total		**164**	

9 CY-MSCA AND CY-CP INFORMATION SECURITY MANAGEMENT

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

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

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

- The **CY-MSCA** and the **CY-CP** ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.
- The **CY-MSCA** and the **CY-CP** retain the responsibility for all aspects of key certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties are clearly defined by the **CY-MSCA** and the **CY-CP** and appropriate arrangements are made to ensure that third parties are bound to implement any controls required by the **CY-MSCA** and the **CY-CP**. The **CY-MSCA** and the **CY-CP** retain responsibility for the disclosure of relevant practices of all parties.
- The information security infrastructure necessary to manage the security within the **CY-MSCA** and the **CY-CP** are maintained at all times. Any changes that will impact on the level of security provided are approved by the **CY-MSA**.
- The **CY-MSCA** and the **CY-CP** meet the requirements of the standard ISO 17799:2005 with regard to security management. Formal accreditation is not mandated.

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

- The **CY-MSCA** and the **CY-CP** ensure that their assets and information receive an appropriate level of protection:
  - The **CY-MSCA** and the **CY-CP** carry out a risk assessment to evaluate business risks and determine the necessary security requirements levels and procedures.

- The **CY-MSCA** and **the CY-CP** maintain an inventory of all information assets and assign a classification for the protection requirements to those assets consistent with a risk assessment.

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

9.3.1 Trusted Roles

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

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

The CAA or PA role includes:

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

The SA role includes:

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

The ISSO role includes:

- Assigning security privileges and access controls of **CAA/PAs**.
- Assigning passwords to all new accounts.
- Performing archiving of required system records
- Review of the audit log to detect **CAA/PA** compliance with system security policy. Review of the audit log will be done at least once per week.
- Personally conducting or supervising an annual inventory of the **CY-MSCA/ CY-CP's** records.
- Participating in Member State key generation

Note that the **ISSO**, who is not directly involved in issuing certificates, performs a supervisory function in examining system records or audit logs to ensure that

other persons are acting within the realms of their responsibilities and within the stated security policy.

9.3.2 Separation of roles

- Within the **CY-MSCA** and the **CY-CP** several individuals fill each of the above-mentioned positions and **at least one** individual is appointed per task.
- All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.
- Where dual control is required **at least two** trusted members of the **CY-MSCA** staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.
- The **CY-MSCA** contains the following distinct work groups:
  - The **CY-MSCA** operating personnel that manages operations on certificates.
  - Administrative personnel to operate the platform supporting the **CY-MSCA.**
  - Security personnel to enforce security measures.

9.3.3 Identification and Authentication for Each Role

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

9.3.4 Background, qualifications, experience, and clearance requirements

- The role of **CAA/PA** (Certification Authority/Personalization Administrator), which involves creating and managing key information is a critical position. The individual assuming the **CAA/PA** role is a trusted person.
- The **CY-MSCA** and the **CY-CP** personnel in trusted roles including, at least, all **CAA/PA** and **ISSO** (Information System Security Officer):
  - Are not assigned duties that may lead to a conflict with their duties and responsibilities as **CAA/PA** and **ISSO**.
  - Have not been previously relieved of a past assignment for negligence or non-performance of duties.
  - Have received proper training to carry out their duties.
  - Can produce a certificate of good conduct.
  - Have no previous criminal conviction for a serious crime.

9.3.5 Training requirements

- Personnel have adequate training for the role and the function.

9.4 System security controls of the CA and personalization systems

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

In particular:

- The integrity of the system and information shall be protected against viruses, malicious and unauthorized software
  - Damage from security incidents and malfunctions are minimized through incident reporting and response procedures.
- The Cyprus Certification Authority System (CAS) and Personalization system provide sufficient system security controls for enforcing the separation of roles described in this certificate policy.
- The security controls provide access control and traceability to an individual level on all functions affecting the use of the **CY-MSCA's** private issuing keys.

9.4.1 Specific computer security technical requirements

- Initialising the system that operates the private certification keys of the **CY-MSCA** requires at least **two(2) operators**, which are securely authenticated.

9.4.2 Computer security rating

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

9.4.3 System development controls

- The **CY-MSCA** and the **CY-CP** use trustworthy systems and products that are protected against modification.
- An analysis of security requirements are carried out at the design and requirements specification stage of any systems development project undertaken by the **CY-MSCA** and the **CY-CP** or on behalf of the **CY-MSCA** and the **CY-CP** to ensure that security is built into IT systems.
- Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

9.4.4 Security management controls

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

9.4.5 Network security controls

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

9.5 Security audit procedures

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

9.5.1 Types of event recorded

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

  a) The creation of accounts (privileged or not).

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

9.5.2 Frequency of processing audit log

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

9.5.3 Retention period for audit log

- Audit logs are retained for at least **7** years.

9.5.4 Protection of audit log

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

9.5.5 Audit log backup procedures

- Two (2) copies of the consolidated log are made and stored in separate physically secured locations.
- Audit logs are stored in a way that makes it possible to examine the log during its retention period.
- Audit logs are protected from unauthorized access.

9.5.6 Audit collection system (internal vs. external)

- Only an internal audit collection system is required.

9.6 Record archiving

9.6.1 Types of events recorded by the CY-CIA

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

a) Certificate requests and all related messages exchanged with the **CY-MSCA** and the **CY-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 CY-MSCA and the CY-CP

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

  a) Contents of issued certificates.
  b) Audit journals including records of annual auditing of the **CY-MSCA** and the **CY-CP's** compliance with this certificate policy.
  c) Currently and previously implemented certificate policy documents and the certificate policy.

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

9.6.3 Retention period for archive

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

9.6.4 Procedures to obtain and verify archive information

- The **CY-MSCA** and the **CY-CP** act in compliance with requirements regarding confidentiality as stated in section 3.4
- Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.
- To the extent permitted by Law a fee may be charged against record retrieval costs. The **CY-MSCA** and the **CY-CP** ensure the availability of the archive and that archived information is stored in a readable format during its retention period, even if the **CY-MSCA** and the **CY-CP's** operations are interrupted, suspended or terminated.
- If the **CY-MSCA** or **CY-CP** services are interrupted, suspended or terminated, the **CY-MSCA** or the **CY-CP** notify all customer organizations to ensure the continued availability of the archive. All requests for access to archived information are sent to the **CY-MSCA** and the **CY-CP** or to the entity identified by the **CY-MSCA** and the **CY-CP** prior to terminating its service.

9.7 CY-MSCA and CY-CP continuity planning

- The **CY-MSCA** and the **CY-CP** have a business continuity plan (**BCP**) that includes but is not limited to addressing:
  - Key compromise
  - Catastrophic data loss due to e.g. theft, fire, failure of hardware or software
  - System failure of other kinds
- The **ERCA** will be notified of any disasters without any delay.
- Disaster response mechanisms do not depend on **ERCA** response time.

9.7.1 Member State keys compromise

- Cyprus keys compromise is dealt with in section 6.

9.7.2 Other disaster recovery

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

9.8 Physical security control of the CA and personalization systems

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

9.8.1 Physical access

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

- Access to other **CY-MSCA** or **CY-CP** premises is limited to personnel in trusted roles (see 9.3.1).
- The **CY-MSCA** CPS stipulates the controls implemented to ensure secure physical access.

10 CY-MSCA OR CY-CP TERMINATION

10.1 Final termination

- Termination of the **CY-MSCA** or **CY-CP** takes place when all service associated with a logical entity is terminated permanently. Before termination, the **CY-MSA** ensures that the tasks outlined below are carried out.
  a) Inform all users and parties with whom the **CY-MSC**A and the **CY-CP** have agreements or other form of established relations.
  b) Make publicly available information of its termination at least **3** months prior to termination.
  c) The **CY-MSCA** and the **CY-CP** terminate all authorization of subcontractors to act on behalf of the **CY-MSCA** and **CY-CP** in the process of issuing certificates.
  d) The **CY-MSCA** and the **CY-CP** maintain and provide continuous access to record archives by handing them over to the Ministry of Communication and Works of the Republic of Cyprus.

10.2 Transfer of CY-MSCA or CY-CP responsibility

- Transfer of **CY-MSCA** or **CY-CP** responsibility occurs when the **CY-MSA** appoints a new **CY-MSCA** or **CY-CP**. The **CY-MSA** ensures the transfer of responsibilities, assets and all root keys to the new **CY-MSCA**. In addition to the above:
  - The **CY-MSA** ensures the orderly transfer of responsibilities and assets.
  - The outgoing **CY-MSCA** transfers all root keys to the **CY-MSA**. The **CY-MSA** subsequently transfers all root keys to the new **CY-MSCA**.
  - The outgoing **CY-MSCA** destroys any copies of keys that are not transferred.

11. AUDIT

- The **CY-MSA** is responsible to carry out audits on the **CY-MSCA** and the **CY-CP**.

11.1 Frequency of entity compliance audit

- The **CY-MSCA** and the **CY-CP** are audited at least annually for conformance with the Cyprus certificate policy.

11.2 Topics covered by audit

- The audit shall include the requirements defined in **ERCA-CP** §5.3.
- The audit shall cover the **CY-MSCA** and **CY-CP** practices.
- The audit shall cover the **CY-MSCA** and **CY-CP** compliance with this policy

11.3 Who should do the audit

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

11.4 Actions taken as a result of deficiency

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

11.5 Communication of results

- Results of the audits on a security status level will be available upon request. Actual audit reports will not be available except on need-to-know basis.
- The CY-MSA shall provide a copy of the audit report, in English, to the ERCA. This report shall describe any corrective actions and their implementation schedule.

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

12.1 Items that may change without notification

- The only changes that may be made to this specification without notification are:
  a) Editorial corrections
  b) Changes to the contact details

12.2 Changes with notification

12.2.1 Notice

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

12.2.2 Comment period

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

12.2.3 Whom to inform

- All eligible changes are notified to the **CY-MSCA** and **CY-CP**.

12.2.4 Period for final change notice

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

12.3 Changes requiring a new Cyprus MSA Policy approval

- If a change in this certificate policy is deemed by the **CY-MSA** to impact the Cyprus CA policy, action is taken to make appropriate updates and

new version submitted for approval to ERCA on behalf of the European Commission.

13 REFERENCES

[BPM] Digital Tachograph Card Issuing Best Practice Manual; Card Issuing Group, 16 November 2001, 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: 2005. Information technology - Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project, owned by the Commission

Digital Tachograph System European Root Policy, Version 2.0; European Commission Special Publication I.04.131; published at http://dtc.jrc.it.

14. GLOSSARY/DEFINITIONS AND ABBREVIATIONS

14.1 Glossary/Definitions

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

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

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

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

Certification Authority System (CAS): A computer system in which certificates are issued by signing certificate (user) data with the CA private signing key.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual CA policy. The CPS takes a broader view to address key usage, certificates and equipment.

Equipment: In the Tachograph system the following equipment exists: Tachograph cards.

Practice Statement (PS). A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.

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

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

RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.

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

User: Users are equipment users and are **Card Holders**. All users will be uniquely identifiable entities.

In this document:

Signed: Where this policy requires a signature, a secure and verifiable digital signature meets the requirement.

Written: Where this policy requires information to be in writing, that requirement is met by a data message if the information contained there in is accessible so as to be usable for the parties concerned.

14.2 List of abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card personalizing organization
CPS	Certificate policy
CY-CIA	Cyprus Card Issuing Authority
CY-CP	Cyprus Card personalizing organization
CY -MSA	Cyprus MSA (Member State Authority)
CY -MSCA	Cyprus MSCA (Member State Certification Authority)
ERCA	European Root Certification Authority
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

Michael Kylilis