Customer : Hellenic Ministry of Transport and communication

Project : Hellenic Digital Tachograph System

Title : Hellenic Certification Practice Statement for the Smart Tachograph System

Customer ref. :

Cybertrust ref. :

Authors : Abdel Youssouf
☎ : +32 16 28 7443
✉ : Abdel.Youssouf@verizonbusiness.com

:

Verizon Business Security
Solutions powered by Cybertrust

4 New Square
Bedfont Lakes, Feltham,
Middlesex. TW14 8HA
P +44 20 8831 2600
F +44 20 8831 2900

Document Control

Reviewers (current version)

	NAME	DATE
Prepared by:	Abdel Youssouf,	09/10/2008
Checked by:	Krista Reynders	10/10/2008
Approved by:	Evangelia Tsagka	10/11/2008

Change Record

VERSION	DATE	AUTHOR	STATUS/DESCRIPTION
0.0		Andreas Mitrakas	Template
0.1	09/10/2008	Abdel Youssouf	1st draft
0.2	03/11/2008	Abdel Youssouf	Add Greek Ministry's comment
0.3	10/11/2008	Evangelia Tsagka	Comment approval

Distribution List and History

VERSION	COMPANY	NAME	ACTION
V1.00			

Table of Contents

DOCUMENT OWNERSHIP, CHANGE AUTHORITY AND CONFIDENTIALITY

This document remains the sole property of Cybertrust Holdings Inc. and/or its affiliates and licensors. Only Cybertrust may change it.

This document contains information that is confidential to the Customer, Cybertrust and third parties officially involved in this project. Information from this document may only be shown to other parties with the written permission of the Cybertrust. The document is issued to the recipient in strict confidence and may be used solely for the internal business purposes of the recipient. It may not be sold, copied or reproduced or provided to any third party in whole or in part in any manner or form without the prior written consent of Cybertrust.

Cybertrust has made every effort to ensure that the information contained in this report is accurate. However, the information may be based on data provided by third parties and/or their software products and as such Cybertrust is not liable for any problems that may occur as a result of any inaccuracies in this document.

NOTICE

1 Introduction

This document is the Certification Practice Statement for the Tachograph system in Greece (hereinafter, GR-MSCA CPS). Parties involved in the management of the life cycle of certificates and tokens of the Hellenic Tachograph follow the requirements set out in this CPS. This CPS has been approved for conformance with the requirements of the Hellenic Member State Authority Certificate Policy (hereunder, GR-MSA CP), (which can be found under http://www.yme.gr/getfile.php?id=1770 or which can be obtained upon request to: Ms. Evangelia TSAGKA, Directorate General of Transport, Ministry of Transport & Communications, Anastasseos 2 & Tsigante, Papagou 10191, Greece).

The GR-MSA CP has been approved by the European Root Certification Authority.

The Tachograph system comprises of several entities including the Hellenic Card Issuing Authority (hereinafter, GR-CIA), the Hellenic Card Personaliser (hereinafter, GR-CP), the Hellenic Member State Authority (hereinafter, GR-MSA) and the Hellenic Member State Certification Authority (hereinafter, GR-MSCA) as it is described below under Section 1.1.2 of this CPS. These entities act under the auspices of the GR-MSA, which is the organization in charge of the execution of the Tachograph system in Greece (Hellas). This CPS is final and binding between GR-CP, the GR-MSCA and the subscriber and/or relying parties, who use, rely or attempt to rely upon certification services that are made available by any of the above-mentioned parties that act as service providers within the Hellenic Tachograph system.

Subscribers of GR-MSCA certificates include but are not limited to drivers, garage operatives, operatives of equipment manufacturers, controllers (e.g. law enforcement agents etc.) who have a requirement to setup, access, modify, calibrate control or use data that is without limitation collected, stored or generated by the Tachograph system.

Relying parties are also those, who have a requirement to setup, access, modify, calibrate control or use data that is without limitation collected, stored or generated by the Tachograph system.

By adhering to the terms of this CPS, parties acknowledge that they may occur obligations towards all parties that deliver part of the service of the Hellenic Tachograph system. These parties include GR-CP, and the GR-MSCA, as it is explained hereunder. This CPS is directly applicable by virtue of the European and Hellenic legislation on the Tachograph system as listed below.

By applying for the service, the applicant is also bound to the conditions set out in this CPS. An application for service can be addressed to (a) the Directorate of Organisation and Informatics, Hellenic Ministry of Transport & Communications, or (b) the Hellenic Directorates of Transport of the Prefectures.
.

This CPS meets the requirements set out in the documents stated below:

- Council Regulation (EEC) n° 3820/85 of 20 December 1985 on the harmonization of certain social legislation relating to road transport
- Council Regulation (EEC) n° 3821/85 of 20 December 1985 on recording equipment on road transport
- 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)
- Decision No 1799/1999 of the European Parliament and of the Council of 12 July 1999 on a series of guidelines, including the identification of projects of common interest, for Trans-European networks for the electronic interchange of data between administrations (IDA).

- Decision No 1720/1999 of the European Parliament and of the Council of 12 July 1999, adopting a series of actions and measures in order to ensure interoperability of and access to Trans-European networks for the electronic interchange of data between administrations (IDA)
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates
- Guidelines and Template National CA policy –version 1.0.
- European Digital Tachograph Common Security Guidelines
- Digital Tachograph System, European Root Policy, version 2.0
- GR-MSA Certificate Policy version 1.1_English-revised
- Digital Tachograph Card Issuing Best Practice Guidelines v.1.0

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

1.1 System overview and responsible organizations

1.1.1 Tachograph system overview

A Tachograph is a device that is used to control driver activities such as driving and rest periods. It is used in professional vehicles such as buses, lorries etc. The Tachograph system aims at:

- Supporting transport companies in using the Tachograph as a management tool.
- Giving accurate data on work and rest periods of drivers.
- Supporting the enforcement of driving regulations.
- Combating fraud to enhance road safety and good business practices.

Within the Hellenic implementation of the Tachograph system, stakeholders include the following:

- European Root Certification Authority (ERCA)
- Hellenic Member State Authority (GR-MSA)
- Hellenic Card Issuing Authority (GR-CIA)
- Hellenic Directorates of Transport of the Prefectures (GR-DTPs)
- Hellenic Member State Certification Authority (GR-MSCA)
- Hellenic Card Personaliser (GR-CP)
- Card users
- Relying parties

At European level, the Tachograph system uses a single European key pair (EUR.SK and EUR.PK) to certify Member States public keys including those of Greece. A European Certification Authority operating under the authority and responsibility of the European Commission has responsibility for the management of the European key pair.

The GR-MSCA generates a key pair (MS.SK and MS.PK), the public key of which is certified by the European Certification Authority. The Hellenic private key is used to certify public keys used with other authorized Tachograph equipment i.e. Tachograph card.

At equipment level, one single key pair (EQT.SK and EQT.PK) is generated and inserted in each piece of authorized equipment. The GR-MSCA certifies equipment public keys for Greece. Equipment manufacturers, equipment personalizing agencies or Member State authorities manage the keys. The equipment keys are used for authentication, digital signature and encryption.

In the Tachograph system the GR-CP is the Registration Authority.

An illustration of the Tachograph system and its constituting entities is presented in the figure below:

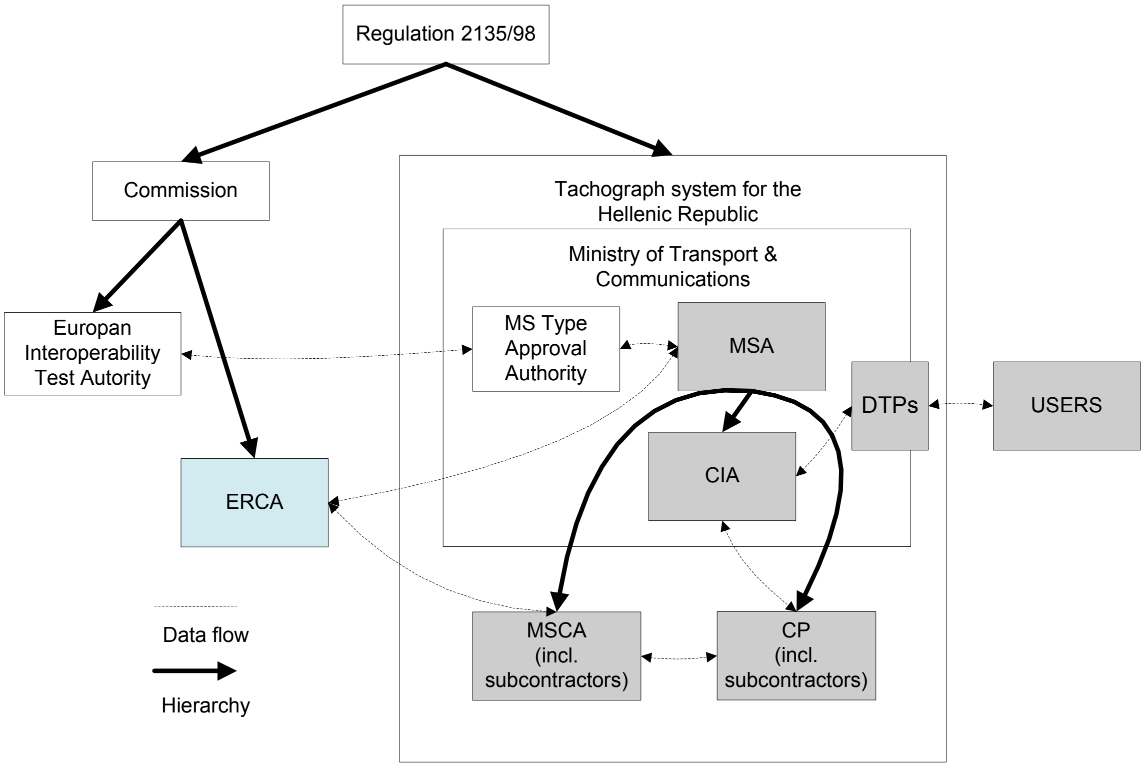
Regulation 2135/98
Commission
Europan Interoperability Test Autority
ERCA
Tachograph system for the Hellenic Republic
Ministry of Transport & Communications
MS Type Approval Authority
MSA
CIA
DTPs
USERS
MSCA (incl. subcontractors)
CP (incl. subcontractors)
Data flow
Hierarchy

Figure 1
Tachograph system organisation according to the ERCA Policy (coloured boxes are covered in this document)

1.1.2 Responsible organisations

In Greece, the Member State Authority (hereinafter, GR-MSA), which is in charge of this CPS is:

Digital Tachograph Project Manager
Ministry of Transport & Communications,
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

The appointed Card Issuing Authority for Greece (hereinafter, GR-CIA) is:

Digital Tachograph Card Issuing Authority
Directorate of Organisation and Informatics,
Ministry of Transport & Communications,
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

The appointed Card Personaliser for the Hellenic Tachograph project is:

Digital Tachograph Card Personaliser
Giesecke & Devrient SA/NV,
Leuvensesteenweg 573/11,
1930 Zaventem,
Belgium

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

Cybertrust NV
Philipssite 5
B-3001 Leuven
Belgium

1.2 Approval

This CPS has been approved by the GR-MSA by Evangelia TSAGKA, Directorate General of Transport, Ministry of Transport & Communications, on 10/11/2008.[1]

1.3 Availability and contact details

These practices are publicly available at: http://www.yme.gr/getfile.php?id=1900

Questions concerning this CPS should be addressed to the address of the appointed GR-MSA.

[1] To be filled in by the GR-MSA. This GR-MSCA CPS has been submitted for approval to the GR-MSA by the GR-MSCA on 24-10-2008.

2 Scope and applicability

The Tachograph system operates as a closed system. This CPS applies to the Tachograph system only to the exclusion of any other. The certificates issued in the Tachograph system can be used for specific purposes associated with the operation of the digital Tachograph system as mandated by Law regarding the Tachograph system in Greece. The keys and certificates issued by the GR-MSCA and the cards issued by the GR-CIA are only for use within the Tachograph system. Within the Tachograph system the scope of this CPS is presented in the figure below. Three entities are depicted in this figure i.e.: the ERCA certification service provider (CSP); the GR-MSCA; and the GR-CP.

With the exception of ERCA, GR-MSA, GR-DTPs and GR-CIA , all assertions in this GR-MSCA CPS are final and binding for the parties that they are addressed to. Assertions concerning the ERCA, GR-MSA and GR-CIA can be found as appropriate in the European and Hellenic Law, the ERCA Policy and the GR-MSA CP. Where appropriate, assertions concerning the ERCA, GR-MSA and GR-CIA are, indeed, maintained to serve guidance and information purposes only. Obligations regarding these three organisations emanate from the legal framework regarding the Tachograph system directly and the GR-MSA Certificate Policy.

The ERCA and the GR-MSCA create, maintain and use keys to validate digital Tachograph data, only after verifying that the data to encrypt are complete, correct, and duly authorized.

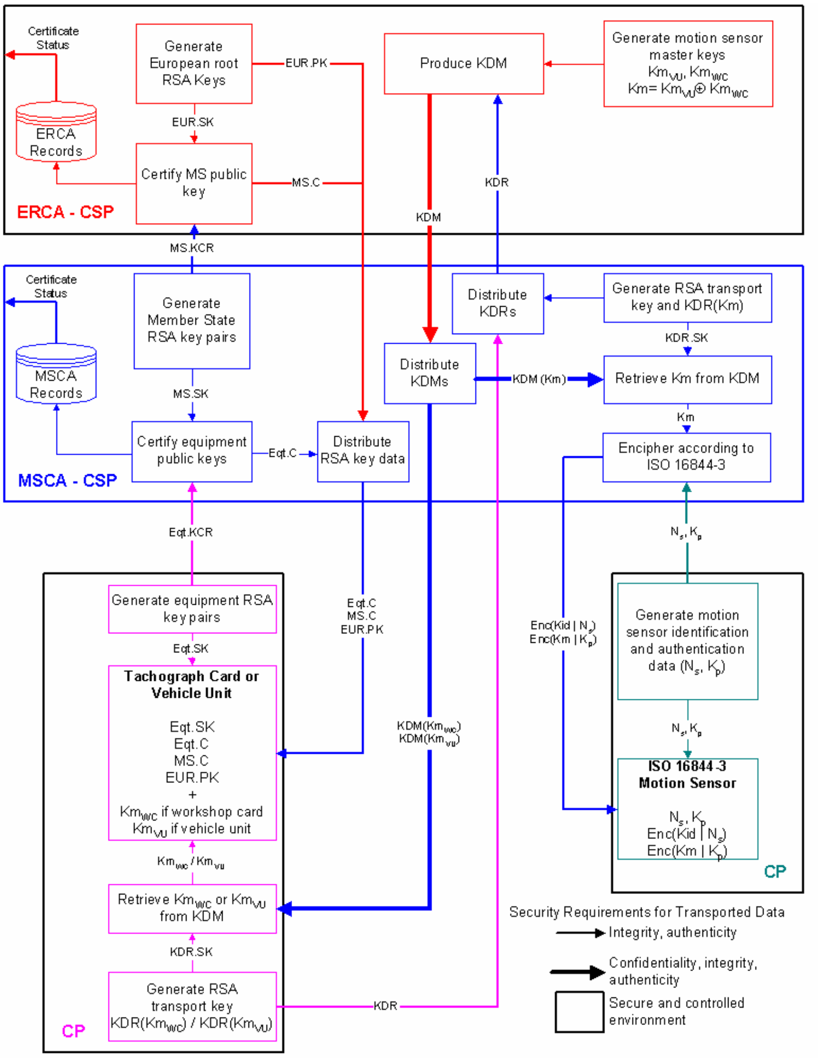
Certificate Status
ERCA Records
Generate European root RSA Keys
EUR.PK
EUR.SK
Certify MS public key
MS.C
Produce KDM
Generate motion sensor master keys
Km_VU, Km_WC
Km= Km_VU ⊕ Km_WC
KDM
KDR
ERCA - CSP
MS.KCR
Certificate Status
MSCA Records
Generate Member State RSA key pairs
MS.SK
Certify equipment public keys
Eqt.C
Distribute RSA key data
Distribute KDMs
KDM (Km)
Distribute KDRs
Generate RSA transport key and KDR(Km)
KDR.SK
Retrieve Km from KDM
Km
Encipher according to ISO 16844-3
MSCA - CSP
Eqt.KCR
N_s, K_p
Generate equipment RSA key pairs
Eqt.SK
Tachograph Card or Vehicle Unit
Eqt.SK
Eqt.C
MS.C
EUR.PK
+
Km_WC if workshop card
Km_VU if vehicle unit
Km_WC / Km_VU
Retrieve Km_WC or Km_VU from KDM
KDR.SK
Generate RSA transport key
KDR(Km_WC) / KDR(Km_VU)
CP
Eqt.C
MS.C
EUR.PK
KDM(Km_WC)
KDM(Km_VU)
KDR
Enc(Kid | N_s)
Enc(Km | K_p)
Generate motion sensor identification and authentication data (N_s, K_p)
N_s, K_p
ISO 16844-3 Motion Sensor
N_s, K_p
Enc(Kid | N_s)
Enc(Km | K_p)
CP
Security Requirements for Transported Data
Integrity, authenticity
Confidentiality, integrity, authenticity
Secure and controlled environment

Figure 2

Concept of communication presented by the ERCA -- Tachograph system keys, certificates and equipment management. (Scope of policy is marked with bold lines.)

At European level the ERCA policy sets out the conditions that member state authorities follow. In Greece the GR-MSA Certificate Policy that has been approved by ERCA provides guidance with regard to the conditions prevailing in the management of the lifecycle of the components of the Tachograph system. This CPS stipulates the conditions for the management of the lifecycle of certificates and components of the Tachograph system in Greece.

Normative input is provided through:

- The Council and Commission’s Regulations
- The ETSI TS 102 042 standard
- The European Digital Tachograph Security guidelines
- The Guidelines and Template for National CA Policy.

3 General provisions

This section contains provisions relating to the respective obligations of GR-MSA, GR-CIA, GR-MSCA and users, and other issues pertaining to law and dispute resolution. Discreet references to the GR-MSA are made for consistency and in order to keep up with the requirements of the operational environment and the GR-MSA Certificate Policy.

3.1 Obligations

This section contains provisions relating to the respective obligations of:

- GR-MSA
- GR-CP
- GR-MSCA
- End Users including Cardholders

3.1.1 GR-MSA obligations

According to the GR-MSA certificate Policy the GR-MSA has the following obligations:

a) Maintain the National CA Policy.
b) Appoint a GR-MSCA and CP.
c) Audit the appointed GR-MSCA and GR-CP.
d) Approve the MSCA/CP CPS according to the GR-MSA policy.
e) Inform the appointed parties about the GR-MSA policy.

With regard to this CPS the GR-CIA has the obligation to ensure that correct and pertinent user information is input to the GR-MSCA by the GR-CP.

It is hereby stated that this CPS does not assert any obligations upon the GR-MSA and GR-CIA, the legal basis of which can be found in the regulatory sources that are listed in Section 1 of this CPS.

3.1.2 GR-CP obligations

According to the GR-MSA certificate Policy the GR-CP has the following obligations:

a) Follow the GR-MSA CA Policy.
b) Publish the CP (Card Personaliser) Practice Statement that includes reference to GR-MSA Policy, to be approved by the GR-MSA.
c) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in GR-MSA CA Policy, in particular to bear the risk of liability damages as stated in the Hellenic legislation.
d) To implement all requirements as stated in the GR-MSA policy.
e) To conform to the procedures prescribed in the GR-MSA policy, even when its functionality is undertaken by subcontractor.

3.1.3 GR-MSCA obligations

The appointed GR-MSCA has the following obligations:

a) Follows the GR-MSA Certificate Policy.
b) Publishes this CPS that includes reference to the GR-MSA Certificate Policy. This CPS is subject to approval by the GR-MSA. This CPS meets the requirement of the publication of a practice statement by the GR-MSCA. The GR-MSCA bears all assertions it makes regarding its role, actions, practices and procedures.

c) Implements the operational conditions set out in this GR-MSCA CPS.
d) Maintains sufficient organizational and financial resources to operate in conformity with the requirements laid down in the GR-MSA CP, in particular to bear the risk of liability damages.
e) Make status information available for publication.

3.1.3.1 Service Agency obligations (MSCA)

Should third party Service Agencies or service providers be used it is hereby acknowledged that they meet their obligations towards the GR-MSCA and the users according to the requirements set out in service agreements as appropriate.

3.1.3.2 Service Agency obligations (CP)

Should third party Service Agencies or service providers be used it is hereby acknowledged that they meet their obligations towards the GR-CP and the users according to the requirements set out in service agreements as appropriate.

3.1.4 Cardholder obligations

The GR-CIA obliges, through agreement, the user (or the user's organization) to meet the following requirements:

a) To submit accurate and complete information to the GR-CIA in line with the requirements on registration or any other requirements set out in this CPS.
b) To use the keys and certificates only within the Tachograph system.
c) To use the Tachograph cards only within the Tachograph system.
d) To refrain from and take preventive measures to deter unauthorized use of the equipment, including the Tachograph private key and the Tachograph card.
e) To use only its own personal keys, certificate and card.
f) To only have one valid driver card at any time.
g) A user may only under very special, and duly justified, circumstances have both a workshop card and a hauling company card (Annex 1B VI:1); or both a workshop card and a driver card; or several workshop cards. The possession of multiple Tachograph cards has to be duly justified by the circumstances and it might be subject to specific authorisation by the designated member state authority in Greece.
h) To refrain from using a damaged, expired or not yet valid card
i) To promptly notify the GR-CIA up to the end of the validity period indicated in the card (which is the same as on the certificate) if the equipment private key or card has been lost, stolen or potentially compromised or the certificate content is, or becomes, inaccurate.

3.1.5 Relying parties

Within the Tachograph system third parties that rely on certificates are called, relying parties. Relying parties accept the terms of use of certificates included in this CPS. Within the Tachograph system, Control Bodies for example, are relying parties. Relying parties refrain from using Tachograph equipment including without limitations, keys, cards, certificates, components etc., for any purpose other than carrying out authorised Tachograph operations. Information obtained through or from the Tachograph system is only used as authorised.

3.2 Liability

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

The GR- MSA, GR-CIA and the GR-CP bear liability towards end users.
The GR-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 GR-MSCA informs the GR-MSA thereof

and upon a GR-MSA request, provides it with all resources necessary such that permit GR-MSA to meet its obligations.

Tachograph certificates are only intended for use within the Tachograph system to the exclusion of any other. Any other keys or certificates present on the Tachograph card or keys that might be used within the Tachograph system although they have not been certified by ERCA or GR-MSCA are not part of the Tachograph system and as such are and remain outside the scope and responsibility of the GR-MSCA.

The GR-MSCA is not liable for any keys or certificates other than those related to the Tachograph system.

With regard to Tachograph certificates, the GR-MSCA warrants that:

a) The information contained in the certificate at the time of issuance is the same as the information delivered to the GR-MSCA by the GR-CP.
b) The certificate contains all information required for a Tachograph certificate at the time of issuance. The GR-CP warrants correct input to the GR-MSCA.

The GR-MSCA issues a certificate after having received an Equipment Key Certification Request (EQT.KCR) from the GR-CP.

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

If the GR-MSCA reorganises its service delivery in a way that makes additional resources necessary, it seeks approval of any such changes by the GR-MSA.

If the GR-CP reorganises its service delivery in a way that makes additional resources necessary it seeks approval of any such changes by the GR-MSA.

3.2.1 Limitations of Liability

Within the limits permitted by law the total liability of the CA is limited in accordance with the provision of section 3.1.3 of this CPS.

3.2.2 Severability

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

3.2.3 Governing Law

This CPS is governed by the laws of the Hellenic Republic.

3.3 Miscellaneous Provisions

This CPS incorporates by reference the following information:

- Any other pertinent certificate policy including the ERCA certificate policy.
- The mandatory elements of applicable standards and mandated elements of the Tachograph system according to the Council Regulation of the Tachograph System 2135/98 and the Commission Regulation 1360/2002.
- 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

Within the Tachograph system Confidentiality of personal data is ensured according to the requirements of the 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 Hellenic Tachograph services also meet the requirements of the Hellenic law 2472/1997, on privacy protection in relation to the processing of personal data as amended by Laws 2819/2000 and 2915/2001, implementing the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 p. 0031 – 0050).

The Tachograph services also meet the requirements of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. This legislation stipulates that a person or organization, which collects personal identifiable information, is required to:

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

With regard to personal data, further information can be requested at the GR-MSCA address provided in Section 1.1.2 in this CPS.

3.4.1 Types of information to keep confidential

The GR-MSCA treats as confidential the following types of information:

- Any personal or corporate information held by the GR-MSCA that is not featured on issued cards or certificates is considered confidential, and are not 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 used by the GR-MSCA under this CPS.
- Any audit logs and records.

In addition to the above the GR-MSCA treats as confidential all:

- Transaction records.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of the GR-MSCA, certificate management and certificate request services and data.
- Any other type of information or document that is not explicitly made publicly available.

3.4.1.1 Disclosure of confidential information

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

- The party to which the GR-MSCA 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 otherwise required 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 links between the GR-MSCA and GR-CP.
- Sessions to deliver certificate validation information.

3.4.1.3 Non-confidential information

The following types of information are not considered to be confidential:

- Certificates.
- Identification information as well as any private or corporate piece of information that is featured on certificates.

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 the GR-CP.
- Subscribers can consult non-confidential information that the GR-CIA or GR-CP keeps on themselves.

3.5 Intellectual property rights

The GR-MSA owns reserves and enforces all intellectual property rights associated with its own databases and resources. The GR-MSA enforces these rights.

The GR-MSCA owns reserves and enforces any and all intellectual property rights it holds on its own infrastructure, databases, web site etc.

Service agencies own and reserve their respective rights on their databases infrastructure, etc.

3.6 Key Management Policy

Within the GR-MSCA, key pair generation is carried out according to a Key Management Policy. The GR-MSCA Key Management Policy addresses the following aspects:

- Describes the fundamental and generic security controls used by the GR-MSCA to securely carry out key management activities.
- Describes the security controls used by the GR-MSCA to generate GR-MSCA key pairs.

- Specifies the security controls implemented by the GR-MSCA when releasing, activating and deactivating CA keys.
- Describes the security controls used by the GR-MSCA to store, back up and recover GR-MSCA key pairs.
- Describes the security controls used by the GR-MSCA to renew, revoke, archive and destroy GR-MSCA key pairs.
- Describes the security controls used by the GR-MSCA when issuing certificates.

3.7 Business Continuity Plan

The scope of the Business Continuity Plan of the GR-MSCA is to ensure business continuity in the aftermath of a disaster. The Business Continuity Plan presents the plans and procedures for emergency response, back up operations, post disaster recovery that ensures the availability of critical resources and facilitates the continuity of operations in an emergency situation as well as measures to return matters to their normal operation.

- The Business Continuity Plan of the GR-MSCA covers the following pillars:
- Business Impact Assessment
- Risk Assessment
- Recovery Time Objectives
- Crisis Management Team
- Disaster Recovery Plan

4 Practice Statement (PS)

The GR-MSA publishes this CPS that is used to address all pertinent aspects identified in the GR-MSA policy. This CPS is subject to approval by the GR-MSA.

4.1 Policy Management Board

New versions and updates of the certification practice statement are approved by a Policy Management Board. The Policy Management Board consists of the following parties:

- One member representing each organisation involved in the delivery of services to the Tachograph system, being the GR-MSA, GR-MSCA and GR-CP. The representatives of the respective organisations must be involved (a) in the management of these organisations or (b) in the project management for the Tachograph system or (c) act under the authority of a party under categories (a) or (b).
- At least one and maximum three agent(s) or consultant(s) involved in the Tachograph system and the pertaining legal framework who is directly involved in the drafting and development of this CPS.

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

All members of the Policy Management Board have one vote. There are no other voting rights reserved for any other party.

In case of lock vote, the vote of the Chairperson of the Policy Management Board i.e. the representative of the GR-MSA counts double.

4.2 Review process

A maintenance process aims at handling updates of the CPS. 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 CPS.

4.2.1 Versions

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

4.2.2 Policy updates

Contributions to CPS updates are accepted by any organisation involved in the delivery of services to the Tachograph system, being the GR-MSCA, the GR-CP, GR-CIA, the GR-MSA or any other organisation acting upon authorisation of the above.

4.3 Change procedures

Changes to this CPS follow the procedure below.

4.3.1 Changes with notification

Changes to this CPS require notification to the GR-MSA.

4.3.2 Notice period

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

4.3.3 Comment period

Users that are affected by changes may file comments with the policy administration organization within 15 days from notice.

4.3.4 Whom to inform

All eligible changes that are submitted to the Policy Management Board are notified to the GR-MSA.

4.3.5 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.

4.3.6 Changes impacting the GR-MSA Certificate Policy

If a change is deemed to impact the GR-MSA Certificate Policy, action is taken to propose appropriate updates to the GR-MSA.

4.3.7 Changes without notification

Changes to this CPS must be filed to the GR-MSA for approval.
Changes to this CPS that may not require reporting to the GR-MSA include:

a) Minor editorial corrections
b) Changes to contact details

5 Keys and transport keys management

This section contains provisions for the management of:

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

The private key of an ERCA certificate is used to sign the certificate issued to the GR-MSCA.

The GR-MSCA keys are also called Member State Hellenic Root keys.

Motion Sensor keys are symmetric keys placed on the workshop card, VU and Motion Sensor for authentication.

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

Asymmetric key pairs at all levels feature the following lengths have a minimum length of 1024 bits.

Symmetric Triple DES keys have a minimum length of 64 bits.

The GR-MSCA does not handle any keys other than the Hellenic Root Keys, the GR-MSCA Transport keys and the Km motion sensor keys.

The GR-MSCA follows the procedure, formats and/or manages media prescribed by the GR-MSA in:

- Submitting GR-MSCA public keys to GR-MSA in order to forward them to the ERCA for subsequent certification as Hellenic root keys.
- Handling motion sensor master keys that are issued by the ERCA.

Within the Tachograph system keys cannot be changed over.

Transportation of private keys during key certification is forbidden.

5.1 Hellenic key pair of the GR-MSCA

The keys for Greece are the GR-MSCA signing key pair(s), which is/are used to sign all equipment certificates according to the ERCA CP, Annex A.

5.1.1 Key pair generation of the GR-MSCA

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

5.1.2 Member State keys' period of validity

The usage period of the corresponding public keys is undefined.

The usage period of private keys for Tachograph card certificate production is set to two (2) years by the validity of the corresponding public key certificate issued by the ERCA.

5.1.3 GR-MSCA private key backup

The GR-MSCA private signing keys are backed up, using a key recovery procedure requiring at least dual control. The procedure used is specified below:

GR-MSCA keys are backed up in encrypted form on WORM (write one, read many) storage media. GR-MSCA keys are backed up by the GR-MSCA members of staff in trusted roles, under, at least, dual control.

Between uses, key backups are stored in sealed, tamper-evident containers. GR-MSCA key backups are kept in containers that are entrusted for safekeeping to at a secure archival company for later retrieval. The integrity of CA key backups is controlled immediately after keys are backed up. The integrity of CA key backups is verified on a regular basis by GR-MSCA members of staff in trusted roles under dual control.

5.1.4 Member State keys end of life

The GR-MSCA ensures that it always has a valid, certified signing key pair for Greece in line with a Key Management Policy.

Upon termination of use of the signing key pair for Greece, the public key is securely archived and warranty is provided that it will never be used again in the future.

The GR-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 GR-MSCA:

- GR-MSCA Key Management policy.
- GR-MSCA Key Management procedures.
- GR-MSCA Security Policy.

5.2 Motion Sensor keys

The GR-MSCA manages keys in encrypted form.

The GR-MSCA forwards the workshop key to the GR-CP to insert it to Workshop cards.

The GR-CP undertakes the GR-MSCA's task to ensure that the workshop key Km_{WC} is inserted into all issued Workshop cards.

5.3 Transport keys

Member State Key Pairs for motion sensor master key distribution (transport keys) is 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.

Transport keys are symmetric keys.

The Key Distribution Request (KDR) has been generated and validated by the GR-CP, by checking its conformity with the European Root Policy Annex D and forward it to the ERCA. The ERCA has ensured that the motion sensor master key distribution request was complete, accurate, and duly authorized.

The resulting Key Distribution Message (KDM) has been returned to the GR-CP. The received KDM must be handled with the internal security requirements of the GR-CP, and loaded in the production environment so it can be used for the production.

It is the GR-CP 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.

6 Equipment keys (asymmetric)

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

- Tachograph cards

Symmetric Motion Sensor keys are addressed in section 5.2.

7 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.

7.1 Registration

Prior to any certification, the GR-CP ensures that evidence of subject's identification and accuracy of names and associated data are properly examined as part of the registration service (card issuing process).

Certificate requests are generated based on the information given in the application form of the Tachograph card. The public key to be certified is extracted from the key generation process. The GR-CP ensures that the input data contains information which renders the Certificate Holder Reference (CHR) unique. The GR-MSCA verifies the uniqueness of the CHR within its domain.

7.2 Equipment certificate issuing

The GR-MSCA ensures the authenticity of the certificates it issues. The GR-MSCA uses dedicated communication protocols, digital signatures for authentication and mutual authentication for devices. The GR-MSCA puts in place procedures to check GR-MSCA software and verify its integrity. The GR-MSCA provides a hash of all software packages or software updates.

The GR-MSCA uses trustworthy systems, which only authorised staff may access for the purposes of adding of changing data. All information is checked for authenticity. Any technical changes of the security requirements become apparent to the authorised operator.

The GR-MSCA takes measures to protect its own private key by using dedicated devices. The GR-MSCA signing keys are only used for signing certificates and blacklist data.

The GR-MSCA ensures systems integrity by using software against malicious code and viruses. Confidentiality and integrity of registration data are protected when exchanged between the GR-CP and the GR-MSCA with each party authenticating itself to the other.

7.3 Certificate Revocation

The Hellenic Tachograph Certificates will not be revoked, however, as stated in the GR- Certificate Policy non valid cards will be put on a blacklist which may be checked by the competent authorities.

7.4 Certificate Renewal

The Hellenic Tachograph Certificates are not renewed, since certificates and cards have the same time of validity period.

7.5 Tachograph card certificates

Applicants use a GR-CIA application as described in the introduction of this CPS. Applications are evaluated by the GR-CIA.

Driver certificates, Workshop certificates, Control body certificates and Company certificates are issued only to successful applicants for a card.

8 GR-MSCA Information Security management

This section describes the Information Security measures mandated for the Tachograph system.

Note: This section is complemented by the Information Security policy and Business Continuity Plan of each of the relevant entities.

8.1 Information security management of the GR-MSCA

The GR-MSCA applies adequate administrative and management procedures that meet the requirements of the recognized standards quoted in the Introduction of this CPS.

If the GR-MSCA outsources any of its responsibilities pertinent to the Tachograph system to any third parties they clearly define them in appropriate contractual arrangements to ensure that third parties are bound to implement required controls. The GR-MSCA retains joint responsibility for the disclosure of relevant practices of all parties.

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

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

Additional assertions apply to services delivered by the Service Agency for the GR-MSCA according to a confidential and documented security policy.

8.2 Physical Security Controls

The GR-MSCA implements physical controls on their own premises. These physical controls include the following:

The GR-MSCA secure premises are located in an area appropriate for high-security operations. These premises feature numbered zones and locked rooms, cages, safes, and cabinets.

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 the GR-MSCA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

Power and air conditioning operate with a high degree of redundancy.

Premises are protected from water exposures.

The GR-MSCA implements measures for the prevention of, protection from and 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 GR-MSCA implements a partial off-site backup.

The GR-MSCA hosts the infrastructure to provide the GR-MSCA services. The GR-MSCA 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.

Strict access control is enforced to all areas containing highly sensitive material and infrastructure including material and infrastructure pertaining to signing certificates, directories and archives.

8.3 Procedural Controls

The GR-MSCA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties.

The GR-MSCA obtains a signed statement from each member of the staff on not having conflicting interests with the GR-MSCA maintaining confidentiality and protecting personal data.

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.

The GR-MSCA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted-members of the GR-MSCA staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

The GR-MSCA ensures that all actions can be attributed to the system of the GR-MSCA and the member of the GR-MSCA staff that has carried out the action.

For critical GR-MSCA functions dual control is implemented.

The GR-MSCA separates among the following discreet work groups:

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

8.4 Personnel Security Controls

The GR-MSCA implements security controls with regard to the duties and performance of the members of their respective members of staff. These security controls are documented in a policy and include the areas below.

8.4.1 Qualifications, Experience, Clearances

The GR-MSCA performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.

8.4.2 Background Checks and Clearance Procedures

The GR-MSCA makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or signed self-declarations.

8.4.3 Training Requirements and Procedures

The GR-MSCA provides training to their personnel to perform their functions as expected.

8.4.4 Retraining Period and Retraining Procedures

Periodic training updates might also be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

8.4.5 Job Rotation

Job Rotation is not mandated; however it might occur from time to time subject to organisational requirements of the GR-MSCA.

8.4.6 Sanctions against Personnel

The GR-MSCA sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on personnel, as it might be appropriate under the circumstances.

8.4.7 Controls of subcontractors

Subcontractors, independent The GR-MSCA contractors and their personnel are subject to the same background checks as the GR-MSCA operator personnel. The background checks include:

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.
- Privacy protection.
- Confidentiality conditions.

8.4.8 Documentation for initial training and retraining

The GR-MSCA makes available documentation to personnel, during initial training, retraining, or otherwise.

8.5 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. The GR-MSCA implements the following controls:

The GR-MSCA event logging system records events that include but are not limited to:

- Issuance of a certificate.
- Revocation of a certificate.
- Publishing of directories.

The GR-MSCA audits all event-logging records.

Audit trail records contain:

- The identification of the operation.
- The data and time of the operation.
- The identification of the certificate, involved in the operation.
- The identity of the transaction requestor.

In addition, the GR-MSCA maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers.
- Outages and major problems.
- Physical access of personnel and other persons to sensitive parts of the GR-MSCA site.
- Back-up and restore.
- Report of disaster recovery tests.
- Audit inspections.
- Upgrades and changes to systems, software and infrastructure.
- Security intrusions and attempts at intrusion.

Other documents that are required for audits include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access control lists.

The GR-MSCA ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of the GR-MSCA, the GR-MSA and designated auditors. The log files are properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not given log notice.

8.6 Records Archival

The GR-MSCA keeps internal records of the following items:

- All certificates issued.
- Audit trails on the issuance of certificates.
- Audit trail of the revocation of a certificate.
- Any issued directories and blacklists.

The GR-MSCA keeps archives in a retrievable format.

The GR-MSCA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of the GR-MSCA and the GR-MSA.

8.6.1 Types of records

The GR-MSCA retains in a trustworthy manner records of digital certificates, audit data, systems information and documentation.

8.6.2 Protection of archives

Only an authorised GR-MSCA records administrator may access a GR-MSCA archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

8.6.3 Archive backup procedures

A differential back up of the GR-MSCA archives is carried out on a daily basis during working days.

8.6.4 Archive Collection

The GR-MSCA archive collection system is internal.

8.6.5 Procedures to obtain and verify archive information

Only GR-MSCA staff members with a clear hierarchical control and a definite job description may obtain and verify archive information.

The GR-MSCA retains records in electronic or in paper-based format.

8.7 Compromise and Disaster Recovery

In a separate internal document the GR-MSCA specifies applicable incident, compromise reporting and handling procedures. The GR-MSCA specifies the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The GR-MSCA operator establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data.

A business continuity plan is implemented to ensure business continuity following a natural or other disaster.

The GR-MSCA establishes:

- Disaster recovery resources in dual locations sufficiently distant from each other.
- Fast communications between the two sites to ensure data integrity
- A communications infrastructure from both sites to the GR-CIA supporting Internet communications protocols as well as agreed communication protocols used by the GR-MSA.

Disaster recovery infrastructure and procedures are tested at least yearly.

9 Audit

As a minimum, at annual intervals the GR-MSCA is audited for compliance against the GR-MSA Certificate Policy.

The audited parties may select how to best implement the audit findings and recommendations.

10 References

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

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

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

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

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

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

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

[Regulation Annex 1B]: Commission Regulation (EC) No 1360/2002 of 13 June 2002 Annex 1b: Requirements For Construction, Testing, Installation and Inspection

11 Glossary/Definitions and abbreviations

11.1 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.
Card personalisers: An entity that manages the personalisation of smart cards for the Tachograph system..
Control Bodies: Are public interest enforcement agencies that use Tachograph card information according to prescribed requirements, have responsibility for the authenticity of a Tachograph card, use Tachograph data in legal procedures and return withdrawn Tachograph cards to the GR-MSA.
Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.
Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.
Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.
Practice Statement (PS). A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.
Private Key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called Secret key.
Public Key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.
Service Agency: An entity that undertakes to tasks on behalf of a GR-MSCA, a subcontractor.
Tachograph cards/Cards: Four different types of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.
Tachonet: A dedicated pan European network to be used for purposes associated with the Tachograph system.
User: Users are equipment users and are either **Card Holders** for card or **manufacturers** for Vehicle units/Motion Sensors. All users will be uniquely identifiable entities.

<u>In this document:</u>
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.

11.2 List of abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CPS	Certification Practise Statement
GR-CIA	Hellenic CIA
GR-MSA	Hellenic State Authority
GR-MSCA	Hellenic CA
ERCA	European Root CA
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KG	Key Generation
MS	Member State
MSA	Member State Authority
MSCA	Member State CA
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	A specific Public key algorithm
SA	System Administrator