

HELLENIC REPUBLIC

NATIONAL CERTIFICATION AUTHORITY POLICY FOR GREECE

Keys, certificates and equipment management

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

For the Digital Tachograph System
for
GR-MSA, GR-CIA, GR-MSCA, and GR-CP

Version: 1.1_English-revised

Date: 4 September 2008

This document has been approved by:

ERCA, JRC of the European Commission, Directorate General

Published by:

Hellenic Ministry of Transport & Communications
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

Information:

Ms. Evangelia TSAGKA,
Directorate General of Transport
Phone: +30 210 6508461
Fax: +30 210 6508470

Revision History:

- Version 1.0_English, reviewed by ERCA on 12 April 2006
- Version 1.1_English, approved by ERCA on 28 July 2008 (reg. D19261)
- Version 1.1_English-revised, includes minor modifications suggested by ERCA

Table of Contents

| | | |
|----------|---|-----------|
| 1 | INTRODUCTION | 6 |
| 1.1 | RESPONSIBLE ORGANIZATION | 8 |
| 1.2 | APPROVAL..... | 8 |
| 1.2.1 | <i>Conformity of this Policy with ERCA.....</i> | <i>9</i> |
| 1.3 | AVAILABILITY AND CONTACT DETAILS | 10 |
| 2 | SCOPE AND APPLICABILITY | 10 |
| 3 | GENERAL PROVISIONS..... | 12 |
| 3.1 | OBLIGATIONS..... | 12 |
| 3.1.1 | <i>GR-MSA obligations</i> | <i>13</i> |
| 3.1.2 | <i>GR-CIA obligations</i> | <i>13</i> |
| 3.1.3 | <i>GR-MSCA obligations</i> | <i>13</i> |
| 3.1.3.1 | Service Agency obligations | 13 |
| 3.1.4 | <i>GR-CP obligations.....</i> | <i>14</i> |
| 3.1.4.1 | Service Agency obligations | 14 |
| 3.1.5 | <i>Cardholder obligations.....</i> | <i>14</i> |
| 3.1.5.1 | All card types | 14 |
| 3.1.5.2 | Driver card | 14 |
| 3.1.5.3 | Workshop card..... | 15 |
| 3.1.6 | <i>VU manufacturers' obligations (role as personalization organization)</i> | <i>15</i> |
| 3.1.7 | <i>Motion Sensor manufacturers' obligations (role as personalization organization)...</i> | <i>15</i> |
| 3.1.8 | <i>Relying parties</i> | <i>15</i> |
| 3.2 | LIABILITY | 15 |
| 3.2.1 | <i>Limitations of Liability.....</i> | <i>16</i> |
| 3.2.2 | <i>Severability.....</i> | <i>17</i> |
| 3.3 | INTERPRETATION AND ENFORCEMENT | 17 |
| 3.3.1 | <i>Governing Law</i> | <i>17</i> |
| 3.3.2 | <i>Miscellaneous Provisions</i> | <i>17</i> |
| 3.4 | CONFIDENTIALITY..... | 17 |
| 3.4.1 | <i>Types of information to keep confidential</i> | <i>18</i> |
| 3.4.1.1 | Disclosure of confidential information | 18 |
| 3.4.1.2 | Confidential communications | 18 |
| 3.4.2 | <i>Types of information not considered confidential</i> | <i>18</i> |
| 3.4.2.1 | Accessing non confidential information | 19 |
| 3.5 | KEY MANAGEMENT POLICY | 19 |
| 3.6 | BUSINESS CONTINUITY PLAN..... | 19 |
| 4 | PRACTICE STATEMENT (PS)..... | 20 |
| 4.1 | REVIEW PROCESS | 20 |
| 4.1.1 | <i>Versions.....</i> | <i>21</i> |
| 4.1.2 | <i>Policy updates</i> | <i>21</i> |
| 5 | EQUIPMENT MANAGEMENT | 21 |
| 5.1 | TACHOGRAPH CARDS | 22 |
| 5.1.1 | <i>Quality control – GR-MSCA/GR-CP function</i> | <i>22</i> |
| 5.1.2 | <i>Application for card – handled by the GR-CIA.....</i> | <i>23</i> |
| 5.1.2.1 | User application..... | 23 |
| 5.1.2.2 | Agreement | 24 |
| 5.1.2.3 | GR-CIA terms of approval - Driver card specific..... | 24 |
| 5.1.2.4 | GR-CIA terms of approval – Workshop card specific | 24 |
| 5.1.2.5 | GR-CIA terms of approval – Control card specific | 24 |
| 5.1.2.6 | GR-CIA terms of approval – Company card specific..... | 24 |
| 5.1.3 | <i>Validity period of cards</i> | <i>24</i> |

| | | |
|----------|---|-----------|
| 5.1.4 | Card renewal – handled by the GR-CIA | 25 |
| 5.1.5 | Card update or exchange – handled by the GR-CIA | 25 |
| 5.1.6 | Replacement of lost, stolen, damaged and malfunctioning cards – handled by the GR-CIA | 25 |
| 5.1.7 | Application approval registration – handled by the GR-CIA | 25 |
| 5.1.8 | Card personalization – handled by the GR-CP..... | 26 |
| 5.1.8.1 | Visual personalization | 26 |
| 5.1.8.2 | User data entry | 26 |
| 5.1.8.3 | Key entry | 26 |
| 5.1.8.4 | Certificate entry | 26 |
| 5.1.8.5 | Quality Control..... | 26 |
| 5.1.8.6 | Cancellation (destruction) of non-distributed cards | 26 |
| 5.1.9 | Card registration and data storage (DB) – handled by the GR-CP and the GR-CIA.... | 26 |
| 5.1.10 | Card distribution to the user – handled by the GR-CP and GR-CIA..... | 26 |
| 5.1.11 | Authentication codes (PIN) – generated by the GR-CP..... | 27 |
| 5.1.11.1 | PIN generation | 27 |
| 5.1.11.2 | PIN distribution (handled by the GR-CIA) | 27 |
| 5.1.12 | Card deactivation | 27 |
| 5.2 | VEHICLE UNITS AND MOTION SENSORS..... | 28 |
| 6 | KEY MANAGEMENT: EUROPEAN ROOT KEY, MEMBER STATE KEYS, MOTION SENSOR KEYS | 28 |
| 6.1 | ERCA PUBLIC KEY | 29 |
| 6.2 | GREECE MEMBER STATE KEYS OF GR-MSCA..... | 29 |
| 6.2.1 | Member State keys generation | 29 |
| 6.2.2 | Member State keys' period of validity..... | 30 |
| 6.2.3 | Member State private key storage | 30 |
| 6.2.4 | Member State private key backup | 30 |
| 6.2.5 | Member State private key escrow | 31 |
| 6.2.6 | Member State keys compromise..... | 31 |
| 6.2.7 | Member State keys end of life | 31 |
| 6.3 | MOTION SENSOR KEYS..... | 31 |
| 6.4 | TRANSPORTS KEYS..... | 32 |
| 7 | EQUIPMENT KEYS (ASYMMETRIC) | 33 |
| 7.1 | GENERAL ASPECTS GR-CP/GR-MSCA | 33 |
| 7.2 | EQUIPMENT KEY GENERATION | 33 |
| 7.3 | EQUIPMENT KEY VALIDITY | 34 |
| 7.3.1 | Keys on cards | 34 |
| 7.3.2 | Vehicle units..... | 34 |
| 7.4 | EQUIPMENT PRIVATE KEY PROTECTION AND STORAGE - CARDS..... | 34 |
| 7.5 | EQUIPMENT PRIVATE KEY PROTECTION AND STORAGE – VUS..... | 34 |
| 7.6 | EQUIPMENT PRIVATE KEY ESCROW AND ARCHIVAL | 34 |
| 7.7 | EQUIPMENT PUBLIC KEY ARCHIVAL | 35 |
| 7.8 | EQUIPMENT KEYS END OF LIFE | 35 |
| 8 | EQUIPMENT CERTIFICATE MANAGEMENT | 35 |
| 8.1 | DATA INPUT..... | 35 |
| 8.1.1 | Tachograph cards | 35 |
| 8.1.2 | Vehicle units..... | 35 |
| 8.2 | TACHOGRAPH CARD CERTIFICATES | 35 |
| 8.2.1 | Driver certificates..... | 35 |
| 8.2.2 | Workshop certificates | 36 |
| 8.2.3 | Control body certificates | 36 |
| 8.2.4 | Company certificates | 36 |
| 8.3 | VEHICLE UNIT CERTIFICATES | 36 |
| 8.4 | EQUIPMENT CERTIFICATE ISSUING | 36 |

| | | |
|-----------|--|-----------|
| 8.5 | EQUIPMENT CERTIFICATE RENEWAL AND UPDATE | 36 |
| 8.6 | DISSEMINATION OF EQUIPMENT CERTIFICATES AND INFORMATION..... | 36 |
| 8.7 | EQUIPMENT CERTIFICATE USE | 37 |
| 8.8 | EQUIPMENT CERTIFICATE REVOCATION | 37 |
| 9 | INFORMATION SECURITY MANAGEMENT | 37 |
| 9.1 | INFORMATION SECURITY MANAGEMENT OF THE GR-MSCA AND GR-CP | 37 |
| 9.2 | ASSET CLASSIFICATION AND MANAGEMENT OF THE GR-MSCA/GR-CP | 38 |
| 9.3 | PERSONNEL SECURITY CONTROLS OF THE GR-MSCA/GR-CP | 38 |
| 9.3.1 | <i>Trusted Roles</i> | 38 |
| 9.3.2 | <i>Separation of roles</i> | 39 |
| 9.3.3 | <i>Identification and Authentication for Each Role</i> | 39 |
| 9.3.4 | <i>Personnel Security Controls</i> | 39 |
| 9.3.4.1 | Qualifications, Experience, Clearances | 39 |
| 9.3.4.2 | Background Checks and Clearance Procedures | 39 |
| 9.3.4.3 | Training Requirements and Procedures | 40 |
| 9.3.4.4 | Sanctions against Personnel | 40 |
| 9.3.4.5 | Controls of subcontractors | 40 |
| 9.3.4.6 | Contract termination of personnel | 40 |
| 9.3.5 | <i>Procedural controls</i> | 40 |
| 9.4 | SYSTEM SECURITY CONTROLS OF THE CA AND PERSONALIZATION SYSTEMS | 41 |
| 9.4.1 | <i>Specific computer security technical requirements</i> | 41 |
| 9.4.2 | <i>System development controls</i> | 41 |
| 9.4.3 | <i>Security management controls</i> | 41 |
| 9.4.4 | <i>Network security controls</i> | 42 |
| 9.5 | SECURITY AUDIT PROCEDURES | 42 |
| 9.5.1 | <i>Types of event recorded</i> | 42 |
| 9.5.2 | <i>Frequency of processing audit log</i> | 42 |
| 9.5.3 | <i>Retention period for audit log</i> | 42 |
| 9.5.4 | <i>Protection of audit log</i> | 42 |
| 9.5.5 | <i>Audit log backup procedures</i> | 42 |
| 9.5.6 | <i>Audit collection system (internal vs. external)</i> | 43 |
| 9.6 | RECORD ARCHIVING | 43 |
| 9.6.1 | <i>Types of event recorded by the GR-CIA</i> | 43 |
| 9.6.2 | <i>Types of event recorded by the GR-MSCA/GR-CP</i> | 43 |
| 9.6.3 | <i>Retention period for archive</i> | 43 |
| 9.6.4 | <i>Procedures to obtain and verify archive information</i> | 44 |
| 9.7 | GR-MSCA/GR-CP CONTINUITY PLANNING..... | 44 |
| 9.7.1 | <i>Other disaster recovery</i> | 44 |
| 9.8 | PHYSICAL SECURITY CONTROL OF THE CA AND PERSONALIZATION SYSTEMS..... | 44 |
| 9.8.1 | <i>Physical access</i> | 45 |
| 10 | GR-MSCA OR GR-CP TERMINATION | 45 |
| 10.1 | FINAL TERMINATION - GR-MSA RESPONSIBILITY | 45 |
| 10.2 | TRANSFER OF GR-MSCA OR GR-CP RESPONSIBILITY | 46 |
| 11 | AUDIT..... | 46 |
| 11.1 | FREQUENCY OF ENTITY COMPLIANCE AUDIT | 46 |
| 11.2 | TOPICS COVERED BY AUDIT | 46 |
| 11.3 | WHO SHOULD DO THE AUDIT | 47 |
| 11.4 | ACTIONS TAKEN AS A RESULT OF DEFICIENCY..... | 47 |
| 11.5 | COMMUNICATION OF RESULTS | 47 |
| 12 | NATIONAL CA POLICY CHANGE PROCEDURES..... | 47 |
| 12.1 | ITEMS THAT MAY CHANGE WITHOUT NOTIFICATION | 47 |
| 12.2 | CHANGES WITH NOTIFICATION..... | 47 |
| 12.2.1 | <i>Notice</i> | 47 |

| | | |
|-----------|---|-----------|
| 12.2.2 | <i>Comment period</i> | 47 |
| 12.2.3 | <i>Whom to inform</i> | 47 |
| 12.2.4 | <i>Period for final change notice</i> | 48 |
| 12.3 | CHANGES REQUIRING A NEW NATIONAL CA POLICY APPROVAL | 48 |
| 13 | REFERENCES | 48 |
| 14 | GLOSSARY/DEFINITIONS AND ABBREVIATIONS | 49 |
| 14.1 | GLOSSARY/DEFINITIONS | 49 |
| 14.2 | LIST OF ABBREVIATIONS..... | 50 |
| 15 | EVIDENCE OF DEVICE CERTIFICATION | 51 |
| 15.1 | GR-MSCA DEVICE FOR MEMBER STATE GREEK KEYS | 51 |
| 15.2 | GR-CP DEVICE FOR EQUIPMENT AND MOTION SENSOR KEY..... | 52 |
| 15.3 | GR-CP SECURITY CERTIFICATION OF THE CARD | 54 |

1 INTRODUCTION

This document is the National CA Policy¹ for the Hellenic Republic for the Digital Tachograph System. 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 drivers accurate data on their work and rest periods.
- Permitting enforcement of driving regulations.
- Limiting fraud to enhance road safety and good business practices.

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

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

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 (ERCA) operating under the authority and responsibility of the European Commission has responsibility for the management of the European key pair.

In Greece, the GR-MSA is responsible for generating a key pair (MS.SK and MS.PK), the public key of which is certified by the European Certification Authority. The Greek private key is used to certify public keys used with other authorized Tachograph equipment, such as vehicle unit or 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.

An illustration of the Tachograph system and its constituting entities is presented in Figure 1. The function of entities in coloured boxes is discussed in more detail in §5.

¹ CA policy is a common terminology for a policy that states requirements to secure the management of digital keys, digital certificates and usually, cards, for a certain CA (Certificate Authority).

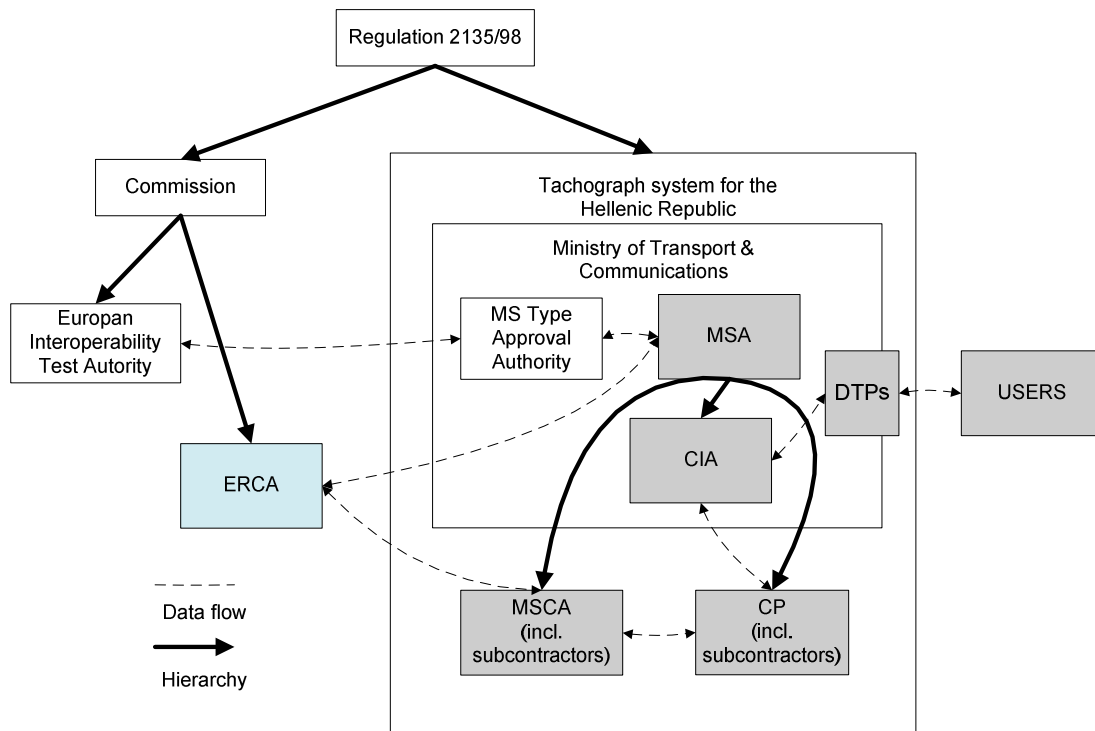


Figure 1: Overall organization of the tachograph system for the Hellenic Republic (coloured boxes are covered in this document).

This National CA Policy is in accordance with:

- 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.
- Digital Tachograph Card Issuing Best Practice Guidelines v.1.0.

Additional references, and a list of acronyms are provided at the end of this document.

1.1 RESPONSIBLE ORGANIZATION

The responsible body for this National CA Policy is the Ministry of Transport & Communications (MoT&C) of the Hellenic Republic, acting as the Member State Authority (GR-MSA). The address of MoT&C is:

Ministry of Transport & Communications,
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

The Card Issuing Authority (GR-CIA) is the Directorate of Organisation and Informatics (DOI) of MoT&C. The address of DOI is:

Directorate of Organisation and Informatics,
Ministry of Transport & Communications,
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

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

Cybertrust,
5, Philipssite,
3001 Leuven,
Belgium

GR-MSA has appointed a third party external contractor to carry out technical operations with regard to the personalisation of the Greek tachograph cards. The address of the appointed Greek Card Personaliser (GR-CP) is:

Giesecke & Devrient SA/NV,
Leuvensesteenweg 573/11,
1930 Zaventem,
Belgium

The use of appointed contractors for the roles of GR-MSCA and GR-CP in no way diminishes the GR-MSA overall responsibilities for these processes.

1.2 APPROVAL

This National CA Policy (GR-MSA Policy) has been approved (reg. D19261) by the European Root Certification Authority (ERCA), Joint Research Center (JRC) of the European Commission, Directorate General. The address of 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)
Italy

ERCA approved the National CA Policy of Greece on 28 July 2008.

1.2.1 Conformity of this Policy with ERCA

Table 1 provides links from the ERCA requirements in §5.3 of [ERCA] to the appropriate articles in this CA Policy.

| ERCA POLICY | GREECE CA POLICY |
|-------------|----------------------------------|
| 5.3.1 | 1.1 |
| 5.3.2 | 6.2.1, 6.2.3, 6.3 |
| 5.3.3 | 6.2.1, 9.3.1, 9.8 |
| 5.3.4 | 6.2.2 |
| 5.3.5 | 6.2.1, 9.7 |
| 5.3.6 | 6.2 |
| 5.3.7 | 6.3 |
| 5.3.8 | 6.1 |
| 5.3.9 | 6 |
| 5.3.10 | 6 |
| 5.3.11 | 6.2.7 |
| 5.3.12 | 5.1.1, 7.1, 7.2 |
| 5.3.13 | 3.1, 5, 5.1.8, 6.2.1, 6.2.3, 7.2 |
| 5.3.14 | 6.2.3, 7.1, 7.4 |
| 5.3.15 | 6.2.4 |
| 5.3.16 | 7.1, 7.4, 8.1.1 |
| 5.3.17 | 6.2.5, 7.6 |
| 5.3.18 | 6.3 |
| 5.3.19 | Not applicable |
| 5.3.20 | Not applicable |
| 5.3.21 | 6.3 |
| 5.3.22 | Not applicable |
| 5.3.23 | 6.3 |
| 5.3.24 | 6.3 |
| 5.3.25 | Not applicable |
| 5.3.26 | 6.2.1, 6.2.6, 6.2.7, 9.7 |
| 5.3.27 | 6.2 |
| 5.3.28 | 6.2.3 |
| 5.3.29 | 8.1.1 |
| 5.3.30 | 8.1.1 |
| 5.3.31 | 3.1.2, 5.1.9, 8.7 |
| 5.3.32 | 5.1.3, 7.3.1 |
| 5.3.33 | Not applicable |
| 5.3.34 | Not applicable |
| 5.3.35 | 5, 5.1.2.1, 5.1.10 |
| 5.3.36 | 6.2.6, 9.7 |
| 5.3.37 | 6.2.6, 9.7 |
| 5.3.38 | 9.1 |
| 5.3.39 | 9.3 |
| 5.3.40 | 9.5, 9.6 |

| | |
|--------|------|
| 5.3.41 | 10 |
| 5.3.42 | 12 |
| 5.3.43 | 11.2 |
| 5.3.44 | 11.1 |
| 5.3.45 | 11.5 |
| 5.3.46 | 11.4 |

Table 1: Conformity with ERCA requirements

1.3 AVAILABILITY AND CONTACT DETAILS

This National CA Policy is publicly available at:

<http://www.yme.gr/?getwhat=1&oid=668&id=&tid=668>

Questions concerning this National CA Policy should be addressed to:

Ms. Evangelia TSAGKA,
Directorate General of Transport,
Ministry of Transport & Communications,
Anastasseos 2 & Tsigante,
Papagou 10191,
Greece

Phone: +30 210 6508461

Fax: +30 210 6508470

2 SCOPE AND APPLICABILITY

This CA Policy applies to the Digital Tachograph system only, to the exclusion of any other.

The keys and certificates issued by the GR-MSCA are only for use within the Digital Tachograph system.

The cards issued by the GR-CIA are only for use within the Digital Tachograph system.

The scope of this CA Policy within the Tachograph system is presented in Figure 2. Four entities are depicted in this figure: the ERCA certification service provider (CSP); the GR-MSCA; and two Component Personalisers (GR-CP), for the card and for the vehicle unit / motion sensor. At the moment this CA Policy is only applicable for the Card Personaliser, since currently there is no need for personalising vehicle units / motion sensors in Greece.

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.

The Component Personaliser (card, vehicle unit or motion sensor) insert validated security data into digital Tachograph equipment by appropriately secured means.

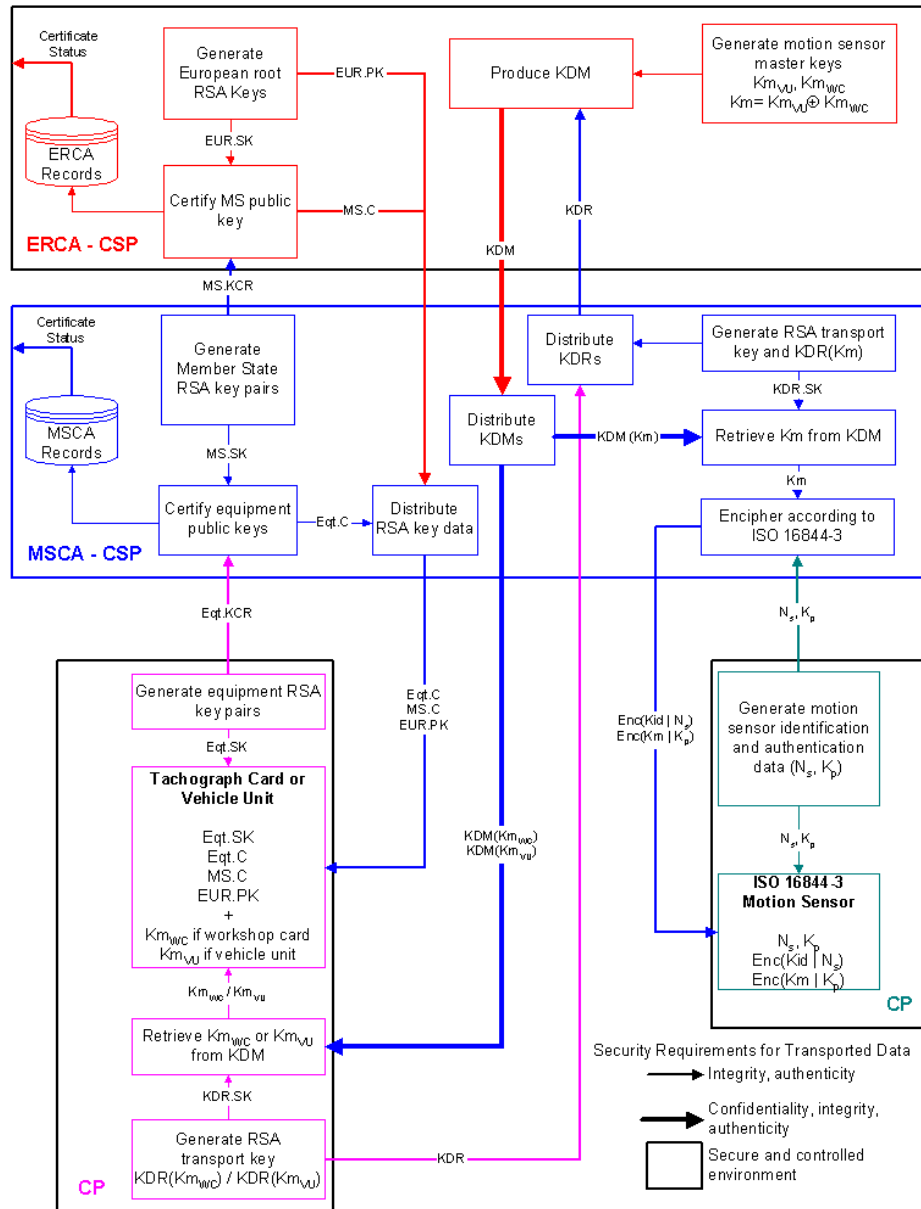


Figure 2: Tachograph system keys, certificates and equipment management. (Scope of policy is marked with bold lines.)²

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 Triple-DES 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 Triple DES symmetric cryptographic system to provide a mechanism for data integrity and authentication during user data exchange between vehicle units and Tachograph cards, and, where

² MS is Greece.

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

Within the Tachograph system, the policy components follow the lay out and interactions that are presented in Figure 3.

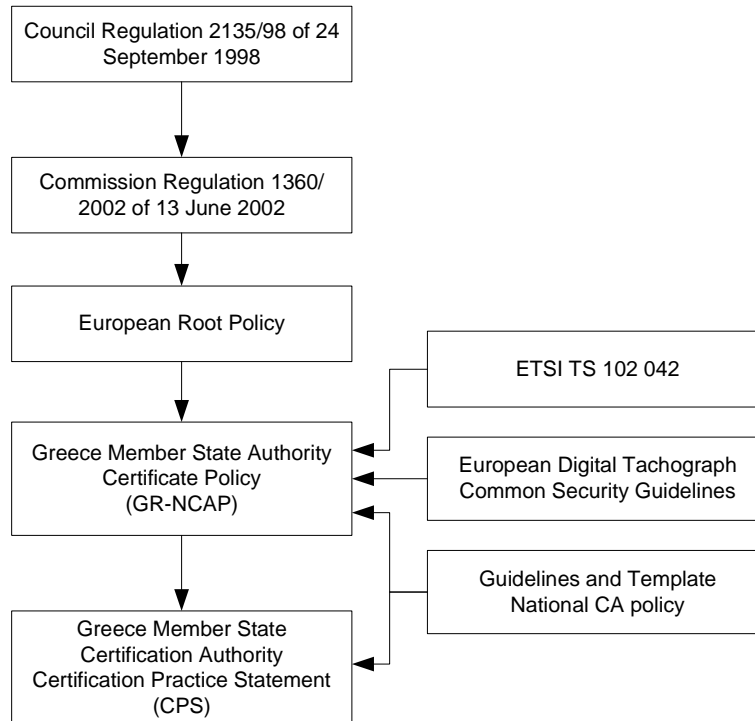


Figure 3: Overview of the regulatory framework of the Tachograph system

At European level, the ERCA policy sets out the conditions that member state authorities follow. In Greece, the CA Policy provides guidance with regard to the conditions prevailing in the management of the lifecycle of the components of the Tachograph system. The 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. Additionally, normative input is provided through the ETSI TS 102 042 standard, the European Digital Tachograph Security guidelines and the Guidelines and Template for National CA Policy.

3 GENERAL PROVISIONS

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

3.1 OBLIGATIONS

This section contains provisions relating to the respective obligations of:

- GR-MSA and GR-CIA
- GR-MSCA
- GR-CP
- Users (Cardholders)

3.1.1 GR-MSA obligations

With regard to this CA Policy, the GR-MSA has the following obligations. The GR-MSA shall:

- a. Maintain the National CA Policy;
- b. Appoint an GR-MSCA and GR-CP;
- c. Audit the appointed GR-MSCA and GR-CP;
- d. Approve the GR-MSCA/GR-CP PS;
- e. Inform the appointed parties about this policy;
- f. Let this policy be approved by the ERCA.

3.1.2 GR-CIA obligations

The GR-CIA shall:

- a. Follow this National CA Policy;
- b. Ensure that correct and relevant user information from the application process is passed to the GR-MSCA and GR-CP;
- c. Inform the users of the requirements in this policy related to the use of the system.
- d. Make status information available on Tachonet.

3.1.3 GR-MSCA obligations

The GR-MSCA shall:

- a. Follow this National CA Policy;
- b. Ensure that correct certificates are passed to the GR-CP;
- c. Maintain confidentiality of the GR-MSCA private key;
- d. Publish a GR-MSCA Practice Statement (GR-MSCA PS) that includes a reference to this National CA Policy, to be approved by the GR-MSA;
- e. Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this National CA Policy, in particular to bear the risk of liability damages as stated in chapter 3.2;
- f. The GR-MSCA shall ensure that all requirements for the GR-MSCA, as detailed in this policy, are implemented;
- g. The GR-MSCA has the responsibility for conformance with the procedures prescribed in this policy, even when the GR-MSCA's functionalities are undertaken by a subcontractor. The GR-MSCA is responsible for ensuring that the Subcontractor provides all its services consistent with its (GR-MSCA PS) and the National CA Policy.

3.1.3.1 Service Agency obligations

Should any third party Service Agencies or service providers be used to deliver Tachograph services, 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.

3.1.4 GR-CP obligations

The appointed subcontractor in its role as GR-CP shall:

- a. Follow this National CA Policy;
- b. Publish GR-CP Practice Statement (GR-CP PS) that includes reference to this National CA 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 this National CA Policy, in particular to bear the risk of liability damages as stated in the Hellenic legislation;
- d. The GR-CP shall ensure that all requirements on GR-CP, as detailed in this policy, are implemented;
- e. The GR-CP has the responsibility for conformance with the procedures prescribed in this policy, even when the GR-CP functionality is undertaken by subcontractor.

3.1.4.1 Service Agency obligations

Should any third party Service Agencies or service providers be used to deliver Tachograph services, 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.

3.1.5 Cardholder obligations

The GR-CIA obliges, through agreement (see 5.1.2.2), the user (or the user's organization) to fulfil the following obligations:

3.1.5.1 All card types

- a. accurate and complete information is submitted to the GR-CIA in accordance with the requirements of this policy, particularly with regards to registration;
- b. the keys and certificate are only used in the Tachograph system;
- c. the card is only used in the Tachograph system;
- d. reasonable care is exercised to avoid unauthorized use of the equipment private key and card;
- e. a user may only under very special, and duly justified, circumstances have both a workshop card and a company card; 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;
- f. a user shall not use a damaged or expired card;
- g. a user shall not tamper with or attempt to modify cards in any way;
- h. the user may only use his/her own keys, certificate and card;
- i. the user shall notify the GR-CIA without any delay if any of the following occurs up to the end of the validity period indicated in the certificate:
 - the equipment private key or card has been lost, stolen or potentially compromised; or
 - the certificate content is, or becomes, inaccurate.

3.1.5.2 Driver card

- a. A user may have only one valid driver card.

3.1.5.3 Workshop card

- a. a user must protect his/her PIN-code;
- b. the card should not leave the premises of workshop unless required by installation, calibration and repair operations.

3.1.6 VU manufacturers' obligations (role as personalization organization)

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

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

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

3.1.8 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 National CA Policy. 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.

Since the Tachograph system is a closed user group, all parties that are subscribers to it and hold a valid card with a certificate are also potential relying parties of the associated certificates. It is not permitted to use Tachograph certificates in any other domain.

3.2 LIABILITY

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

The GR-MSA and the GR-CIA 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 that permit GR-MSA to meet its obligations.

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

Tachograph keys, cards and 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 cards are in violation of this policy and remain outside the scope and responsibility of GR-MSA, GR-CIA, GR-MSCA, and GR-CP.

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-CIA.
- b. The certificate contains all information required for a Tachograph certificate at the time of issuance. The GR-CIA warrants correct input to the GR-MSCA.
- c. In public key certificates, the GR-CP holds the private key corresponding to the public key identified in the certificate request. The GR-CP takes all precautions necessary to ensure correct input to the GR-MSCA.

With regard to Tachograph certificates the GR-CP warrants that:

- a. The certificate request contains the data that match the data that has been loaded on the chip of the card used.
- b. The correct response received of the GR-MSCA is loaded on the chip that generates the request (online generation)
- c. The graphical personalisation of the card is in line with the loaded certificate data.

The GR-MSCA issues a certificate only after receiving an Equipment Key Certification Request (EQT.KCR) from the GR-CP. The GR-CP issues an EQT.KCR after receiving Equipment Key Certification Authorisation (EQT.KCA) from the GR-MSA.

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 CA policy.

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

The GR-CP loads a certificate after having checked if the response matches to the request (Batch-ID), if the received state from the GR-MSCA is correct (success/failed), a Verification of the certificate chain (EUR.PK -> MS.CERT -> EQT.CERT) and whether the CHR, CAR, CHA, EOVS match to the request.

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

If the GR-CP reorganise their 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 GR-MSA and GR-CIA is limited in accordance with the provision of section 3.1.1 and section 3.1.2 of this CA 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

This CA Policy is governed by the laws of the Hellenic Republic.

3.3.2 Miscellaneous Provisions

This CA Policy 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

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

3.4.1 Types of information to keep confidential

The GR-MSCA and the GR-CP consider as confidential the following types of information:

- Any personal or corporate information held by the GR-MSCA or the GR-CP that is not featured on issued cards or certificates, 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 or the GR-CP under this CA Policy.
- Any audit logs and records.

In addition to the above, the GR-MSCA and the GR-CP treat as confidential all:

- Transaction records.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of the GR-MSCA and the GR-CP, infrastructure, 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 and the GR-CP do not release, nor are they required to release, any confidential information without an authenticated and justified request specifying, as applicable:

- The party to whom the GR-MSCA and the GR-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 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 link between the GR-MSCA, the GR-CP, and the GR-CIA.
- Sessions to deliver certificate validation information.

3.4.2 Types of information not considered confidential

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

- Card numbers.
- Certificates.

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

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 a relying party.
- Subscribers can consult non-confidential information that the GR-CIA holds.

3.5 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 GR-MSCA certificates to itself or to other entities.

3.6 BUSINESS CONTINUITY PLAN

The GR-CIA maintains a business continuity plan aimed at ensuring the continuity of the services provided by the Greek Digital Tachograph Platform. This business continuity plan covers the management of the crisis by the GR-CIA and the continuity of the business processes related to the issuance of Greek Digital Tachograph Cards by the GR-CIA.

The GR-CP maintains a business continuity plan aimed at ensuring the continuity of the services relating to the production and personalization of Greek Digital Tachograph Cards. This business continuity plan covers the management of the crisis by the GR-CP and the continuity of the business processes related to the production, the personalization and the delivery of Greek Digital Tachograph Cards by the GR-CP.

The GR-MSCA maintains a business continuity plan aimed at ensuring the continuity of the services relating to the production, the issuance and management of the digital certificates for Greek Digital Tachograph Cards. This business continuity plan covers the management of the crisis by the GR-MSCA and the continuity the business processes related to the production, the issuance and the management of digital certificates for Greek Digital Tachograph Cards by the GR-MSCA.

The coordination between these business continuity plans is ensured at two levels:

- Coordination between the business continuity plans of GR-CIA and GR-CP.
- Coordination between the business continuity plans of the GR-CP and the GR-MSCA.

4 PRACTICE STATEMENT (PS)

The GR-MSCA and GR-CP have statements, called Certification Practice Statement³ (PS), describing practices and procedures used to address all the requirements identified in this National CA Policy. The Certification Practice Statement is subject to approval by the GR-MSA. In particular:

- a. The PS shall identify the obligations of all the external organizations supporting the GR-MSCA and GR-CP services including the applicable policies and practices.
- b. The PS shall be made available to the GR-MSA, to users of the Tachograph system, and to related parties (e.g. control bodies). However, the GR-MSCA/GR-CP do not necessarily make all the details of their practices public and available for the users. Additional information regarding the policies and practices of the GR-MSCA and the GR-CP can be sought directly through the communication address provided elsewhere in this document.
- c. The management of the GR-MSCA/GR-CP has responsibility for ensuring that the PSs are properly implemented.
- d. The Certification Practice Statement of GR-MSCA and GR-CP shall define a review process.
- e. The GR-MSCA, GR-CP shall give due notice of changes they intend to make in their PS and shall, following approval, make the revised PS immediately available.

4.1 REVIEW PROCESS

A maintenance process aims at handling updates of the PS. 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 GR-MSCA PS.

³ The statements of practices and procedures of GR-MSA, the GR-MSCA and GR-CP are consolidated in one single Practice Statement (PS) document managed by the GR-MSCA.

4.1.1 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 PS or the interpretation thereof. Changes are also indicated by a publication date.

4.1.2 Policy updates

Contributions to PS 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.

5 EQUIPMENT MANAGEMENT

The equipment in the Tachograph system is defined as:

- Tachograph cards
- Vehicle units
- Motion Sensors

Due to the fact that currently Vehicle units or Motion Sensors are not manufactured in the Hellenic Republic, this section of Policy only covers Tachograph cards.

The equipment is handled and managed by several roles:

- GR-CIA (cancellation of cards, card registration, renewal, etc.);
- GR-MSCA (Motion Sensor keys, certificates);
- GR-CP (visual and electronic personalization, keys).

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

- a. Ensure that only type approved cards will be used;
- b. Practice statements approvals.

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

- a. Receipt of the applications for cards. The users can submit their applications for cards to the Directorates of Transport of the Prefectures (DTP). The applications are then dispatched to the GR-CIA;
- b. Application approval registration;
- c. Provision of personalization data to GR-CP;
- d. Data storage (DB);
- e. Exchange of information with other Member States;
- f. User registration;
- g. Card issuing to users. Cards are dispatched to the Directorates of Transport of the Prefectures as appropriate, and are then delivered to users;
- h. Handling of lost and found cards;

- i. Quality control (test and samples).

The Directorate of Transport of each Prefecture (GR-DTP) is responsible for:

- a. Providing users with application documents and giving instructions;
- b. Receiving completed applications for cards from applicants;
- c. Checking the identity of the applicants and the completeness / correctness of the applications;
- d. Forwarding the applications to GR-CIA;
- e. Receiving the cards from GR-CIA and deliver them to the proper persons;
- f. Keeping records of applications received and cards delivered.

The following functions are carried out by the GR-MSCA:

- a. Generation of GR-MSCA keys for the Hellenic Republic and managing interface with the ERCA certification process;
- b. Generation of certificates for cards upon requests from GR-CP;
- c. Storing the issued certificates in DB;
- d. Maintaining the security of the GR-MSCA keys.

The following functions are carried out by the GR-CP:

- a. Quality control (test card samples);
- b. Sending certificate requests to GR-MSCA;
- c. Key and certificate insertion;
- d. Personalization of cards;
- e. Capability to Card functionality verification;
- f. Card delivery to the GR-CIA;
- g. Workshop card and PIN delivery to the GR-CIA.

5.1 TACHOGRAPH CARDS

5.1.1 Quality control – GR-MSCA/GR-CP function

The GR-MSCA/GR-CP shall ensure that only type approved cards, according to the Regulation 2135/98 are personalized.

With regard to application identification, the Tachograph system cards store Tachograph application identification and the type of Tachograph card.

With regard to integrated circuit (IC) identification data, Tachograph cards store the IC serial number and IC manufacturing references.

With regard to IC card identification, Tachograph cards store:

- Card serial number (including manufacturing references),
- Card type approval number,
- Card personalizing organization identification (ID),
- Embedded ID,
- IC identifier.

With regard to security elements, Tachograph cards store:

- European public key issued by ERCA.
- Greek GR-MSA certificate.
- Card certificate.

- Card private key corresponding to the public key listed in the card certificate.
- Workshop cards carry motion sensor keys together with the keys and certificates already listed.

5.1.2 Application for card – handled by the GR-CIA

The GR-CIA shall inform the user of the terms and conditions regarding use of the card. This information shall be available in Greek and English.

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

5.1.2.1 *User application*

Applicants for a Tachograph card shall submit an application in a form determined by the GR-CIA. As a minimum, the application shall include the data needed to ensure the correct identification of the user. For company, workshop and control cards, the necessary identity of the legal organization for which card is applied, shall be included.

The following information is required for issuing a card and will be included in the application:

Driver card specific

- Full name
- Date and place of birth
- Place of residence
- National registration number
- Postal address
- Photo
- Driving license number

Workshop card specific

Workshop cards shall be issued only to legal persons who can provide the following evidence:

- full name and legal status of the associated legal person or other organizational entity
- name of the technician
- photo of the technician
- postal address
- evidence of accreditation of the technician for the digital tachograph

Control card specific

Control cards shall be issued to legal persons who can provide the following evidence:

- full name and legal status of the associated legal person or other organizational entity

Company card specific

Company cards shall be issued to individual representatives of companies owning or holding vehicles fitted with a Digital Tachograph and who can provide evidence of:

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

5.1.2.2 Agreement

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

- a. the user agrees to the terms and conditions regarding use and handling of the Tachograph card;
- b. the user agrees to, and certifies, that from the time of card acceptance and throughout the operational period of the card, until GR-CIA is notified otherwise by the user:
 - the user will not allow unauthorized person to have access to the user's card;
 - all information given by the user to the GR-CIA relevant for the information in the card is true;
 - the card is being conscientiously used in consistence with usage restrictions for the card.

5.1.2.3 GR-CIA terms of approval - Driver card specific

A Driver card shall only be issued to individuals having permanent residence in Greece.

The GR-CIA shall ensure that the applicant does not have a valid Driver card issued by the Hellenic Republic or in another Member State.

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

5.1.2.4 GR-CIA terms of approval – Workshop card specific

Workshop card shall only be issued to a workshop having valid workshop accreditation for the Digital Tachograph.

5.1.2.5 GR-CIA terms of approval – Control card specific

Control card shall only be issued to a party nominated as an official control body.

5.1.2.6 GR-CIA terms of approval – Company card specific

Company card shall only be issued to a company registered according to the national legislation.

5.1.3 Validity period of cards

Workshop cards shall be valid for no more than one year from issuance.

Driver cards shall be valid no more than five years from issuance.

Company cards shall be valid no more than five years from issuance.

Control cards shall be valid no more than five years from issuance.

An application for renewal shall follow the procedures described in section 5.1.2.

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

5.1.4 Card renewal – handled by the GR-CIA

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

If the user complies with the above rule, the GR-CIA shall issue a new card:

- in the case of driver, control and company card before the current card expires,
- in the case of workshop card within 5 working days of receiving a complete application.

5.1.5 Card update or exchange – handled by the GR-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 Hellenic residence in order to have the application granted.

The GR-CIA shall upon delivery of the new card take possession of the previous card and send it to the MSA of origin.

Card exchange due to changed country of residence shall otherwise follow the rules for new card issuing (section 5.1.2).

5.1.6 Replacement of lost, stolen, damaged and malfunctioning cards – handled by the GR-CIA

If a card is lost or stolen, the user shall report this formally to the Police. The Police shall then inform the GR-CIA.

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

Damaged and malfunctioning cards shall be delivered to the issuing GR-CIA, by whom they shall be visually and electronically cancelled, and put on a blacklist.

If the card is lost, stolen, damaged or malfunctioning, the user shall apply for a replacement card within **7** days.

Provided that the user follows the above requirements, the GR-CIA shall issue a replacement card with new keys and certificate within 5 working days from receiving a complete application.

The replacement card shall inherit the time of validity from the original card. If the replaced card has less than three months remaining validity, the GR-CIA will issue a renewal card instead of a replacement card.

5.1.7 Application approval registration – handled by the GR-CIA

The GR-CIA shall register the approved applications in a database. This data shall be made available for the GR-MSCA/GR-CP, which uses the information as input to the certificate generation and card personalization processes.

5.1.8 Card personalization – handled by the GR-CP

Cards are personalized both visually and electronically.

5.1.8.1 *Visual personalization*

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

5.1.8.2 *User data entry*

Data shall be inserted in the card according to the structure in Regulation 1360/2002, Annex 1B, appendix 2 [REG-A], rules TCS_403, TCS_408, TCS_413 and TCS_418, depending on card type.

5.1.8.3 *Key entry*

The private key shall be inserted in the card without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection.

5.1.8.4 *Certificate entry*

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

5.1.8.5 *Quality Control*

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

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

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

5.1.9 Card registration and data storage (DB) – handled by the GR-CP and the GR-CIA

The GR-CP and GR-CIA are responsible for keeping track of which card and card number is given to which user. Data shall be transferred from the GR-CP to the GR-CIA database in a secure way.

5.1.10 Card distribution to the user – handled by the GR-CP and GR-CIA

The GR-CP and the GR-CIA assert that:

- a. The cards are kept in a secure and safe environment according to ISO 17799:2005.
- b. Personalized cards are immediately transferred to the delivery or distribution location.
- c. The Tachograph cards are distributed in a manner that provides a reasonable guarantee of delivery to the end user in protected dedicated envelopes while the PINs are distributed separately.

- d. At the point of delivery of a workshop card to a user, proof of user's identity (e.g. name) is required.
- e. Personalized cards shall always be kept separated from non personalized cards.
- f. At the point of delivery of the card to the user evidence of the user's identity (e.g. name) shall be checked against a physical person.
- g. The user shall present valid means of identification.
- h. The reception of the card shall be acknowledged by the user's signature.

5.1.11 Authentication codes (PIN) – generated by the GR-CP

This section applies only to Workshop cards.

The GR-CP will ensure that workshop cards shall have a PIN code, used for authenticating the card to the Vehicle unit.

PIN codes shall consist of at least 4 digits.

5.1.11.1 PIN generation

PIN codes are generated by GR-MSCA 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 140-1 Level 3 or higher.

5.1.11.2 PIN distribution (handled by the GR-CIA)

The pin code of a workshop card is distributed in a manner that minimizes the risk of unauthorized persons accessing the code without it being noticed by the end user.

PIN codes will be distributed by regular mail directly to the user. At the point of delivery of the pin codes to a user, proof of that user's identity (e.g. name) will be checked against a natural person.

Pin codes will be distributed separately with the corresponding cards. Cards will be collected by the user at the application reception points (Directorates of Transport of the Prefectures).

Pin codes are printed on special security paper so that the PIN will never be showed in clear during the production, and that the paper can be put in a regular envelope.

5.1.12 Card deactivation

It shall be possible to permanently deactivate a card and any keys residing thereon. A decision of deactivation shall be taken by the GR-MSA or the GR-CIA.

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

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

5.2 VEHICLE UNITS AND MOTION SENSORS

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

6 KEY MANAGEMENT: EUROPEAN ROOT KEY, MEMBER STATE KEYS, MOTION SENSOR KEYS

This section contains provisions for the management of

- European Root key - the ERCA public key;
- Member State keys, i.e. the Member State signing key pair(s);
- the Motion Sensor keys;
- the transport keys between ERCA and 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 the signing keys for the certification authority in Greece and may also be called Member State Greece root keys.

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

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

Asymmetric key pairs at all levels have a length of 1024 bits. Symmetric Triple DES keys have a length of 128 bits.

The GR-MSCA does not handle any keys other than the Greece 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 ERCA in:

- Submitting GR-MSCA public keys for certification by the ERCA.
- Handling motion sensor master keys that are issued by the ERCA.

The GR-MSCA will use the physical media for key and certificate transport that is described in ERCA CP, Annex C.

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

Within the Tachograph system keys cannot be changed over.

Transportation of private keys during key certification is forbidden.

6.1 ERCA PUBLIC KEY

The GR-MSCA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times.

The GR-CP shall ensure that EUR.PK is inserted in all Tachograph cards.

Both GR-MSCA and GR-CP will recognize the ERCA public key in the distribution format described in Annex B of the ERCA-CP.

6.2 GREECE MEMBER STATE KEYS OF 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.

The key pair consists of a public key (MS.PK) and a private key (MS.SK).

The GR-MSCA public key is certified by the ERCA using the key certification request (KCR) protocol described in Annex A of the ERCA-CP, but it is always generated by the GR-MSCA itself.

The GR-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.

6.2.1 Member State keys generation

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]. See §15.1 for evidence of certification.

The key generation device is a standalone one and meets the requirements stated in the GR-MSCA Certification Practice Statement.

GR-MSCA key-pair generation shall require the active participation of at least three separate individuals, who have trusted roles within the contractor in its role as GR-MSCA and the GR-MSA. At least one of these individuals shall have role of Certification Authority / Personalization Administrator who is responsible for GR-MSCA operations.

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

The GR-MSCA shall have at least two Member State key pairs with associated signing certificates to ensure continuity all the time.

The GR-MSCA will apply for a re-keying prior to the end of the current key pair usage period. The GR-MSCA will communicate a schedule 3 months in advance with estimated dates for re-keying.

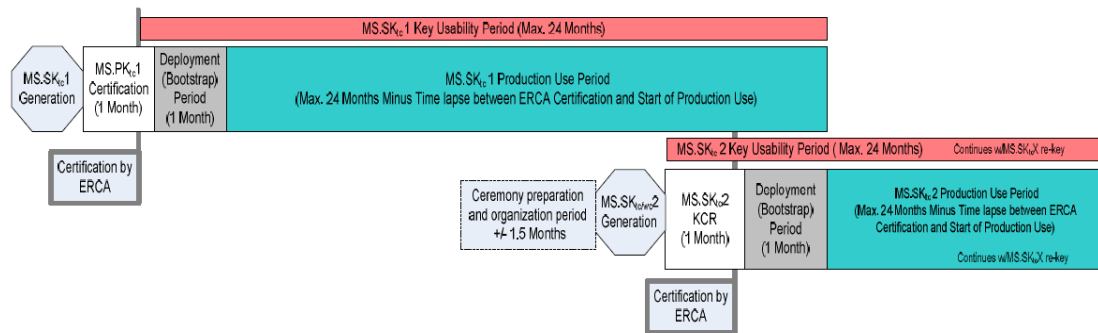


Figure 4: Tachograph National Key and Certificate Lifecycle

The GR-MSCA estimates that the re-keying procedure should start every 19 months from the national certificate creation by ERCA. The re-keying procedure shall start with the notification to GR-MSA for the next GR-MSCA ceremony occurrence. The 19 month estimation is based on: the time needed to schedule the GR-MSCA ceremony and to notify required attendees; time for certification by the ERCA and; time for production bootstrap. Figure 4 illustrates the lifecycle of tachograph keys.

6.2.2 Member State keys' period of validity

The usage period of the Member State private key shall be **2** years from the date of issuance of the corresponding public key's certificate, and shall not be used after this period for any purpose.

Actual validity for Member State public key certificates is 7 years from the date of issuance as defined and decided by the ERCA Root Policy.

6.2.3 Member State private key storage

The private keys shall be contained in and operated from inside a specific tamper resistant device, which meets the requirements identified in FIPS 140-2 level 3 [FIPS]. See §15.1 for evidence of certification.

This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non technical security measures.

For access to the GR-MSCA private signing keys, dual control is required. This means that no single person shall possess the means required to access the environment where the private key is stored. It does not mean that signing of equipment certificates must be performed under dual control.

6.2.4 Member State private key backup

The GR-MSCA private signing keys may be backed up, using a key recovery procedure requiring at least dual control. However, the solution used for continuity is to have at least two key pairs, as stated in §6.2.1. In case of key back up, 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 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 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.

6.2.5 Member State private key escrow

The private signing keys of Greece shall not be escrowed.

6.2.6 Member State keys compromise

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

The GR-MSCA will have a backup system with pre-generated and ERCA certified GR-MSCA key pairs, which allow continuing GR-MSCA operations without remarkable delays.

In case a primary key pair gets compromised and the secondary key pair has to be used, a new key pair will be generated and the corresponding public key will be submitted for certification by the ERCA.

6.2.7 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 private 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

6.3 MOTION SENSOR KEYS

The GR-CP shall request the motion sensor key KmWC from the ERCA using the key distribution request (KDR) protocol described in Annex B of the ERCA-CP. The GR-MSCA will validate the GR-CP KDR by checking conformity as per European Root Policy Annex D and forward it to the GR-MSA for further processing by ERCA. The resulting Key Distribution Message (KDM) is returned to the GR-MSCA that

hands it over to the GR-CP without validation or processing. The GR-CP has the responsibility to operate and manage the received Motion Sensor Key KmWC.

The GR-CP shall only use the workshop key KmWC for the exclusive purpose of insertion into Workshop cards.

The GR-CP shall ensure that the workshop key KmWC is inserted into all issued Workshop cards (Regulation Annex 1B [REG-A]: app 11:3.1.3).

During storage and use, the GR-CP protects the workshop key (KmWC) with high assurance physical and logical security controls. The keys are stored in a specific device which:

- Meets the requirements identified in FIPS 140-1 Level 4 [FIPS], for the HSM used by the GR-CP. See §15.2 for evidence of certification.
- Is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This is set to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

6.4 TRANSPORTS KEYS

The Key Distribution Requests (KDR) are generated by the GR-CP. The GR-MSCA validates the GR-CP KDR by checking conformity with the European Root Policy Annex D and forwards it to the GR-MSA for further processing by ERCA. The ERCA ensures that the GR-MSCA public key certification requests and motion sensor master key distribution requests are complete, accurate, and duly authorized.

The resulting Key Distribution Message (KDM) is returned to the GR-MSCA that hands it over to the GR-CP without validation or processing.

It is the responsibility of GR-CP 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.

For secure data communication the GR-CP issues special transport keys. Transport keys are asymmetric ones.

The GR-CP shall, during key generation, storage, use and distribution, protect these keys with high assurance physical and logical security controls. The keys shall be contained in and operated from a specific device which:

- Meets the requirements identified in FIPS 140-1 Level 4 [FIPS], for the HSM used by the GR-CP. See §15.2 for evidence of certification.
- Is a trustworthy system, which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This is set to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

7 EQUIPMENT KEYS (ASYMMETRIC)

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

- Tachograph cards.

Equipment includes Vehicle Units, which nevertheless are not applicable for the Hellenic Republic for the time being or in the foreseeable future.

The symmetric Motion Sensor keys are not handled here.

7.1 GENERAL ASPECTS GR-CP/GR-MSCA

Equipment initialization, key loading and personalization shall be performed in a physically secure and controlled environment. Entry to this area shall be strictly regulated, controllable at the individual level, and requiring a minimum of two persons to be present to operate the system. A log shall be kept of all the entries and actions in the system.

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

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

Organizations (subcontractors/Service Agencies) that perform key generation and card personalization on behalf of more than one Member State shall do this in a clearly separate process for each of these. A log shall be kept of each individual process and the GR-MSA shall have access to the log on request.

GR-MSCA/GR-CP: The log of the personalization system shall contain a reference to the order, and list the corresponding equipment numbers and certificates. The GR-MSA shall have access to the logs on request.

7.2 EQUIPMENT KEY GENERATION

Keys may be generated either by the GR-CP or by the GR-MSCA (Annex 1B [REG-A], Appendix 11:3.1.1). The entity that performs the key generation in the case of Greece is the GR-CP.

The GR-CP shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

The device used for key generation meets the requirements identified in FIPS 140-1 Level 4 [FIPS], for the HSM used by the GR-CP. See §15.2 for evidence of certification.

This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

The tachograph card adopted for use in Greece is assured to E3 in ITSEC. See §15.3 for evidence of certification.

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

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

GR-MSCA shall ensure the uniqueness of public keys in Tachograph card certificates within its domain.

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 the certificate issuing is performed.

7.3 EQUIPMENT KEY VALIDITY

7.3.1 Keys on cards

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

7.3.2 Vehicle units

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

7.4 EQUIPMENT PRIVATE KEY PROTECTION AND STORAGE - CARDS

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

Copies of the private key are not to be kept anywhere except in the Tachograph card.

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

7.5 EQUIPMENT PRIVATE KEY PROTECTION AND STORAGE – VUS

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

7.6 EQUIPMENT PRIVATE KEY ESCROW AND ARCHIVAL

Equipment private keys shall be neither escrowed nor archived.

7.7 EQUIPMENT PUBLIC KEY ARCHIVAL

All certified public keys shall be archived by the GR-MSCA.

7.8 EQUIPMENT KEYS END OF LIFE

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

8 EQUIPMENT CERTIFICATE MANAGEMENT

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

8.1 DATA INPUT

8.1.1 Tachograph cards

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

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

Certificate request protocol shall ensure the integrity and origin of a request without exposing the private key.

8.1.2 Vehicle units

Not applicable in the Hellenic Republic for the time being or in the foreseeable future.

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 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 in the Hellenic Republic for the time being or in the foreseeable future.

8.4 EQUIPMENT CERTIFICATE ISSUING

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

8.5 EQUIPMENT CERTIFICATE RENEWAL AND UPDATE

See Equipment management (section 5). Since certificates and cards have the same time of validity, they are dealt with together.

8.6 DISSEMINATION OF EQUIPMENT CERTIFICATES AND INFORMATION

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

The GR-CIA shall maintain and make certificate status information available as necessary to users and related parties.

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

8.7 EQUIPMENT CERTIFICATE USE

The Tachograph certificates are only for use within the Tachograph system.

The GR-MSCA exports all card related certificate data to a GR-CP register, so that certificates, equipment and users are connected. The GR-CIA ensures that certificate information is made available through an accessible directory.

8.8 EQUIPMENT CERTIFICATE REVOCATION

Certificates are not revoked; however non valid cards will be put on a blacklist which may be checked by the competent authorities.

9 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 GR-MSCA at the address provided elsewhere in this Certificate Policy.

Additional information regarding information security guidelines may also be obtained by the GR-CP at the address provided elsewhere in this Certificate Policy.

Additional information regarding information security guidelines may also be obtained by the GR-CIA at the address provided elsewhere in this Certificate Policy.

9.1 INFORMATION SECURITY MANAGEMENT OF THE GR-MSCA AND GR-CP

The GR-MSCA and the GR-CP shall apply adequate administrative and management procedures that meet the requirements of recognized standards.

If the GR-MSCA or the GR-CP outsource any of their 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 and the GR-CP retain 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 shall meet the requirements of the standard ISO 17799 with regard to security management. Formal accreditation is not mandated.

9.2 ASSET CLASSIFICATION AND MANAGEMENT OF THE GR-MSCA/GR-CP

The GR-MSCA/GR-CP shall ensure that its assets and information receive an appropriate level of protection.

In particular:

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

9.3 PERSONNEL SECURITY CONTROLS OF THE GR-MSCA/GR-CP

9.3.1 Trusted Roles

The GR-MSCA and the GR-CP use personnel in discrete roles that include:

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

The CAA/PA role includes:

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

The SA role includes:

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

The ISSO role includes:

- a. Assigning security privileges and access controls of CAA/PAs;

- b. Assigning passwords to all new accounts;
- c. Performing archiving of required system records;
- d. Review of the audit log to detect CAA/PA compliance with system security policy. Review of the audit log shall be done at least once per week;
- e. Personally conducting or supervising an annual inventory of the GR-MSCA/GR-CP's records;
- f. Participating in Member State key generation.

9.3.2 Separation of roles

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

9.3.3 Identification and Authentication for Each Role

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

9.3.4 Personnel Security Controls

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

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

- a. not be assigned other duties that may conflict with their duties and responsibilities as CAA/PA and ISSO;
- b. not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- c. have received proper training in the performance of their duties.

9.3.4.1 *Qualifications, Experience, Clearances*

The GR-CIA, GR-MSCA and GR-CP shall carry out 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.

9.3.4.2 *Background Checks and Clearance Procedures*

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

9.3.4.3 Training Requirements and Procedures

The GR-CIA, GR-MSCA and GR-CP shall make available training for their personnel to perform their functions. Periodic training updates might also be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

9.3.4.4 Sanctions against Personnel

The GR-CIA, GR-MSCA and GR-CP shall sanction 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.

9.3.4.5 Controls of subcontractors

Subcontractors, independent GR-MSCA and GR-CP contractors and their personnel shall be 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.

9.3.4.6 Contract termination of personnel

Appropriate measures shall be implemented by both the GR-MSCA and the GR-CP to securely manage contract termination of personnel.

9.3.5 Procedural controls

The GR-CIA, GR-MSCA and GR-CP shall follow 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 and GR-CP shall obtain a signed statement from each member of the staff on not having conflicting interests with the GR-MSCA and GR-CP, 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 shall be considered as serving in a trusted position.

The GR-MSCA shall conduct 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 and GR-CP staff will need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

The GR-MSCA shall ensure 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 shall be implemented.

The GR-MSCA and GR-CP shall separate among the following discreet work groups:

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

9.4 SYSTEM SECURITY CONTROLS OF THE CA AND PERSONALIZATION SYSTEMS

The GR-CIA/GR-MSCA/GR-CP shall ensure that the systems are secure and correctly operated, with minimal risk of failure.

In particular:

- a. the integrity of systems and information is protected against viruses, malicious and unauthorized software;
- b. damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.

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

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

9.4.1 Specific computer security technical requirements

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

9.4.2 System development controls

The GR-MSCA/GR-CP shall use trustworthy systems and products that are protected against modification.

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

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

9.4.3 Security management controls

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

9.4.4 Network security controls

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

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

9.5 SECURITY AUDIT PROCEDURES

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

9.5.1 Types of event recorded

The security audit functions related to the GR-MSCA/GR-CP computer/system shall log, for audit purposes:

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

9.5.2 Frequency of processing audit log

The log shall be processed regularly and analyzed against malicious behaviour. Log procedures shall be described in the PS.

9.5.3 Retention period for audit log

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

9.5.4 Protection of audit log

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

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

9.5.5 Audit log backup procedures

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

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

The audit log shall be protected from unauthorized access.

9.5.6 Audit collection system (internal vs. external)

Only internal audit collection system is required.

9.6 RECORD ARCHIVING

9.6.1 Types of event recorded by the GR-CIA

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

- a. Certificate requests and all related messages exchanged with the GR-MSCA/GR-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 GR-MSCA/GR-CP

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

- a. Contents of issued certificates.
- b. Audit journals including records of annual auditing of GR-MSCA/GR-CP's compliance with its PS.
- c. Currently and previously implemented certificate policy documents and their related PSs.

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

9.6.3 Retention period for archive

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

9.6.4 Procedures to obtain and verify archive information

The GR-MSCA/GR-CP shall 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.

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

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

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

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

9.7 GR-MSCA/GR-CP CONTINUITY PLANNING

GR-MSCA/GR-CP shall have a business continuity plan (BCP) with appropriate disaster recovery mechanisms which do not on the ERCA response time. This shall include (but is not limited to) events such as:

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

The ERCA will be notified of any disasters without delay.

9.7.1 Other disaster recovery

GR-MSCA/GR-CP (or subcontractors) shall have routines established to prevent and minimize the effects of system disasters, detailed in the BCP.

9.8 PHYSICAL SECURITY CONTROL OF THE CA AND PERSONALIZATION SYSTEMS

Physical security controls shall be implemented to control access to the GR-MSCA or GR-CP hardware and software. This includes the workstations and other parts of the CA and personalization hardware and any external cryptographic hardware module or card. A log shall be kept over all physical entries to this area (or areas).

The Greek keys for signing certificates shall be kept physically and logically protected as described in the PS.

- The GR-MSCA and GR-CP 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 and GR-CP implement 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.
- In addition to the maintenance of a hot contingency solution, the GR-MSCA implements a partial off-site backup of recently completed transactions.
- 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.

A security check of the facility housing the GR-MSCA/GR-CP's central equipment shall be made at least once every **24** hours.

9.8.1 Physical access

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

Access to other GR-MSCA/GR-CP facilities shall be limited to those personnel performing one of the roles described in section 9.3.1.

10 GR-MSCA OR GR-CP TERMINATION

10.1 FINAL TERMINATION - GR-MSA RESPONSIBILITY

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

The GR-MSA shall ensure that the tasks outlined below are carried out.

Before the GR-MSCA/GR-CP terminates its services the following procedures has to be completed as a minimum:

- Inform all users and parties with whom the GR-MSCA/GR-CP has agreements or other form of established relations;
- Make publicly available information of its termination at least **3** month prior to termination;
- The GR-MSCA/GR-CP shall terminate all authorization of subcontractors to act on behalf of the GR-MSCA/GR-CP in the process of issuing certificates;
- The GR-MSCA/GR-CP shall perform necessary undertakings to maintain and provide continuous access to record archives.

10.2 TRANSFER OF GR-MSCA OR GR-CP RESPONSIBILITY

Transfer of GR-MSCA or GR-CP responsibility occurs when the GR-MSA chooses to appoint a new GR-MSCA or GR-CP in place of the former entity(subcontractor/service agency).

The GR-MSA shall ensure that transfer of responsibilities and assets is carried out orderly.

The old GR-MSCA shall transfer all root keys to the new in the manner decided by the GR-MSA.

The old GR-MSCA shall destroy any copies of GR-MSCA keys.

11 AUDIT

The GR-MSA is responsible to carry out audits of the GR-CP and the GR-MSCA.

11.1 FREQUENCY OF ENTITY COMPLIANCE AUDIT

The GR-CP and the GR-MSCA shall be audited at least annually for conformance with this CA policy.

11.2 TOPICS COVERED BY AUDIT

The audit shall cover the requirements defined in ERCA-CP §5.3.

The audit shall cover the GR-MSCA/GR-CP practices.

The audit shall cover the GR-MSCA/GR-CP compliance with this National CA Policy.

The audit shall also consider the operations of possible Service Agencies / subcontractors.

11.3 WHO SHOULD DO THE AUDIT

The GR-MSA may use an external certification or accreditation organization or undertake the auditing itself.

11.4 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found in the audit the GR-MSA shall define any corrective actions, and their implementation schedule.

11.5 COMMUNICATION OF RESULTS

Results of the audits, on a security status level, shall be available upon request. The results of the audit shall be reported, in English, to the ERCA by the GR-MSA. Actual audit reports shall not be available, except on need-to-know basis.

12 NATIONAL CA POLICY CHANGE PROCEDURES

12.1 ITEMS THAT MAY CHANGE WITHOUT NOTIFICATION

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

- a. Editorial or typographical corrections.
- b. Changes to the contact details.

12.2 CHANGES WITH NOTIFICATION

12.2.1 Notice

Any item in this policy may be changed with **90** days notice.

Changes to items, which in the judgement of the policy responsible organization (the GR-MSA), **will not** materially impact a substantial majority of the users or related parties using this policy, may be changed with **30** days notice.

12.2.2 Comment period

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

12.2.3 Whom to inform

Information about changes to this policy shall be sent to:

- the ERCA
- GR-MSCA and GR-CP
- All other MSAs

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 shall be given at least **30** days prior to the change taking effect.

12.3 CHANGES REQUIRING A NEW NATIONAL CA POLICY

APPROVAL

If a policy change is determined by the GR-MSA organization to have a material impact on a significant number of users of the policy, the GR-MSA shall submit the revised National CA Policy to the ERCA for approval.

13 REFERENCES

[REG] Council Regulation 3821/85 as amended by Council Regulation (EC) No 2135/98 of 24th September 1998

[REG-A] Annex I(B) to Council Regulation 2135/98 Requirements for construction, testing, installation and inspection

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 15 December 2003, 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.

[ERCA] Digital Tachograph System European Root Policy version 2.0 Special Publication I.04.131

14 GLOSSARY/DEFINITIONS AND ABBREVIATIONS

14.1 GLOSSARY/DEFINITIONS

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

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

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

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

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

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual MSA policy.

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: 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 a Secret key.

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

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

Service Agency: An entity that undertakes to tasks on behalf of an GR-MSCA, GR-CIA or CP, a subcontractor.

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

User: Users are equipment users and are either **Card Holders** for card or **manufacturers** for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

14.2 LIST OF ABBREVIATIONS


CA Certification Authority
CAS Certification Authority System
CIA Card Issuing Authority
CC Common Criteria
CP Card Personalizer
CP PS Card Personalizer Practice Statement
MSCA PS Certification Practice Statement
DB Database
ERCA European Root CA
HSM Hardware Security Module
ISSO Information System Security Officer
ITSEC Information Technology Security Evaluation Criteria
KG Key Generation
MS Member State of Tachograph system
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

15 EVIDENCE OF DEVICE CERTIFICATION


15.1 GR-MSCA DEVICE FOR MEMBER STATE GREEK KEYS

Evidence of certification of the GR-MSCA device used for the management of the Greek keys:


FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America



TM



The Communications Security Establishment of the Government of Canada

Certificate No. 525

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

nShield F3 SCSL, nShield F3 Ultresign 32 SCSL, nShield F3 Ultresign SCSL, payShield SCSL, and payShield Ultra SCSL by nCipher Corporation Ltd.
(When initialized to Overall Level 3 per Security Policy – Only operates in FIPS mode at Level 3)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).




Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM. A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

15.2 GR-CP DEVICE FOR EQUIPMENT AND MOTION SENSOR KEY

Evidence of certification of the GR-CP device used for the management of card keys and the motion sensor key:

| | | |
|---|--|---|
|  FIPS 140-1 Validation Certificate |  <small>The National Institute of Standards and Technology of the United States of America</small> |  <small>The Communications Security Establishment of the Government of Canada</small> |
| Certificate No. 116 | | |
| <p>The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:</p> <p style="text-align: center;">IBM 4758-002 PCI Cryptographic Coprocessor (Miniboot Layers 0 and 1). (When configured for DSS Authentication)</p> <p>In accordance with the Derived Test Requirements for FIPS 140-1, Security Requirements for Cryptographic Modules, FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting <i>Sensitive But Unclassified Information</i> (United States) or <i>Designated Information</i> (Canada) within computer and communications systems (including voice systems).</p> <p>Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-1 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.</p> <p>This certificate includes details on the scope of conformance and validation authority signatures on the reverse.</p> | | |

This is a Certification Module of NIST, which shall not imply products developed by NIST, the U.S., or Canadian Government.

FIPS 140-1 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

IBM 4758-002 PCI Cryptographic Coprocessor (Miniboot Layers 0 and 1), by IBM Corp.

(ID: PN 04K9131, EC F72272D, Miniboot 0 version A, Miniboot 1 version A; Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: **InfoGuard Laboratories, NV/LAP LAB CODE 100432-0**

is as follows:

| | | | |
|---|---------|---|---------|
| Cryptographic Module Design: | Level 4 | Module Interfaces: | Level 4 |
| Roles and Services: | Level 4 | Finite State Machine Model: | Level 4 |
| Physical Security: (Multi-chip embedded) | Level 4 | Software Security: | Level 4 |
| EMI / EMC: | Level 4 | Self Tests: | Level 4 |
| Key Management: | Level 4 | | |
| Operating System Security Level | N/A | is met when used in the following configuration(s): | N/A |

The following FIPS approved Cryptographic Algorithms are used: **DES (Cert.#86), DES MAC, Triple DES (Cert.#4), DSA/SHA-1 (Cert.#34)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **RSA**
End user queries concerning the non-FIPS approved algorithms may be directed to their respective Cryptographic Module Validation Authority.

Overall Level Achieved: 4

Signed on behalf of the Government of the United States

Signature: [Signature]

Dated: 19 September 2000

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]

Dated: 14 Sep 2000

Director, Information Protection Group
The Communications Security Establishment

15.3 GR-CP SECURITY CERTIFICATION OF THE CARD

Evidence of the Security Certification for the tachograph card adopted for use in Greece:



BSI-DSZ-ITSEC-0287-2005

for

**STARCOS SPK 2.4 with Tachograph Card
Application (Tachosmart Card)**

from

Giesecke & Devrient GmbH



SOGIS-MRA

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, June 1991 and the *Information Technology Security Evaluation Manual (ITSEM)*, Version, 1.0, September 1993, extended by smart card specific guidance.

Evaluation Results: Functionality: according to Appendix 10 of Annex I (B) of Regulation (EC) no. 1360/2002, amending Regulation (EEC) no. 3821/85 on recording equipment in road transport;

Evaluation Level: E3

Minimum strength of mechanisms: high

The rating of the strength of mechanisms does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The confirmed evaluation level only applies on the condition that all stipulations regarding generation, configuration and operation as far as specified in the Certification Results are kept and that the product is operated in the environment described, where one is specified.

This certificate is only valid in conjunction with the complete Certification Report.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 28 January 2005

The President of the Federal Office
for Information Security


Dr. Helmbrecht

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111