

Portuguese MSA Policy

**Keys, certificates and equipment management
for
The Digital Tachograph System**

Version Control

Version	Date	Action	Names
1.0	March 2006	- Authoring - Sent for approval by the European Authority	Vítor Garcia José Amaral de Freitas Luísa Nunes
1.0	March 2006	- Approval	Eng.º Jorge Jacob
1.1	April 2006	- Text changes according to Review Findings letter G07-TRVA/JB/jb/(2006)D	Vítor Garcia
1.2	February 2008	- Text changes to reflect the replacement of DGTT by IMTT, IP	Luísa Nunes

Index

1.	Introduction	5
1.1.	Responsible organizations	5
1.2.	Approval	6
1.3.	Availability and contact details	6
2.	Scope and applicability	7
3.	General provisions	8
3.1.	Obligations	8
3.1.1.	P-MSA and P-CIA obligations	8
3.1.2.	P-MSCA obligations	8
3.1.3.	P-CP obligations	8
3.1.4.	Service agencies obligations	9
3.1.5.	Cardholder obligations	9
3.2.	Liability	9
3.2.1.	P-MSA and P-CIA liability towards users and relying parties	9
3.2.2.	P-MSCA and P-CP liability towards the P-MSA and P-CIA	9
3.3.	Interpretation and enforcement	10
3.3.1.	Governing Law	10
3.4.	Confidentiality	10
3.4.1.	Information to be kept confidential	10
3.4.2.	Information not considered confidential	10
4.	Practice Statement (PS)	11
5.	Equipment management: cards and tachographs	12
6.	Keys management	13
6.1.	ERCA public key	13
6.2.	Key pair of the P-MSA	13
6.2.1.	P-MSCA key pair generation	14
6.2.2.	Validity of the Portuguese key pair	14
6.2.3.	P-MSCA private key storage	14
6.2.4.	P-MSCA private key backup	14
6.2.5.	Portuguese private key escrow	15
6.2.6.	Portuguese keys compromise	15
6.2.7.	Portuguese keys end of life	15
6.3.	Motion Sensor keys	15
6.4.	Transport keys	16
7.	Equipment keys (asymmetric)	17
7.1.	General aspects about P-MSCA and P-CP	17
7.2.	Equipment key generation	17
7.2.1.	Equipment key validity	17
7.2.2.	Equipment private key protection and storage - cards	18
7.2.3.	Equipment private key escrow and archival	18
7.2.4.	Equipment public key archival	18
8.	Equipment certificate management	19
8.1.	Data input	19
8.2.	Tachograph card certificates	19
8.2.1.	Driver certificates	19
8.2.2.	Workshop certificates	19
8.2.3.	Control body certificates	19
8.2.4.	Hauling company certificates	19
8.3.	Equipment certificate time of validity	19
8.4.	Equipment certificate issuing	19
8.5.	Equipment certificate renewal and update	19
8.6.	P-MSCA informative tasks	20
9.	Information security management	21

9.1.	Information management of the P-MSCA and P-CP	21
9.2.	Asset classification and management of the P-MSCA/P-CP.....	21
9.3.	Personnel security roles of the P-MSCA/P-CP.....	21
9.3.1.	Trusted roles	21
9.3.2.	Separation of roles	22
9.3.3.	Identification and authentication for each role	22
9.3.4.	Background, qualifications, experience and clearance requirements.....	22
9.3.5.	Training requirements	23
9.4.	System security controls of the CA and personalization systems	23
9.4.1.	Specific computer security technical requirements	23
9.4.2.	Computer security rating.....	23
9.4.3.	System development controls	23
9.4.4.	Security management controls.....	23
9.4.5.	Network Security Controls	24
9.5.	Security audit procedures.....	24
9.5.1.	Types of event recorded.....	24
9.5.2.	Frequency of processing audit log.....	24
9.5.3.	Retention period for audit log	24
9.5.4.	Protection of audit log.....	24
9.5.5.	Audit log backup procedures.....	24
9.5.6.	Audit collection system (internal vs. external)	24
9.6.	Record archiving	25
9.6.1.	Types of event recorded by the P-CIA	25
9.6.2.	Types of event recorded by the P-MSCA/P-CP	25
9.6.3.	Retention period for archive	25
9.6.4.	Procedures to obtain and verify archive information	25
9.7.	Continuity planning	26
9.7.1.	Portuguese keys compromise.....	26
9.7.2.	Other disaster recovery	26
9.8.	Physical security control.....	26
9.8.1.	Physical access	26
10.	P-MSCA or P-CP termination	28
10.1.	Final termination.....	28
10.2.	Transfer of responsibility	28
11.	Audit	29
11.1.	Frequency of entity compliance audit	29
11.2.	Topics covered by audit	29
11.3.	Who should do the audit	29
11.4.	Actions taken as a result of deficiency.....	29
11.5.	Communication of results.....	29
12.	P-MSA policy change procedures	30
12.1.	Items that may change without notification	30
12.2.	Changes with notification	30
12.2.1.	Notice	30
12.2.2.	Comment period	30
12.2.3.	Whom to inform.....	30
12.3.	Changes requiring a new P-MSA policy approval	30
13.	Conformity to the ERCA policy	31
14.	References	39
15.	Glossary/Definitions and abbreviations.....	40
15.1.	Glossary/Definitions	40
15.2.	List of abbreviations	41

1. Introduction

This document establishes the Portuguese MSA policy¹, here below, P-MSA policy, for the digital tachograph system.

The MSA policy is a document that supports the requirements to secure the management of keys, certificates and associated equipment.

This P-MSA policy is in accordance with:

- the Council Regulation of the Tachograph System, 2135/98
- the Commission Regulation 1360/2002 about the adaptation to the technical progress of the Regulation (CEE) 3821/85
- the ERCA policy for the digital tachograph system
- the "Common Security Guidelines"

1.1. Responsible organizations

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

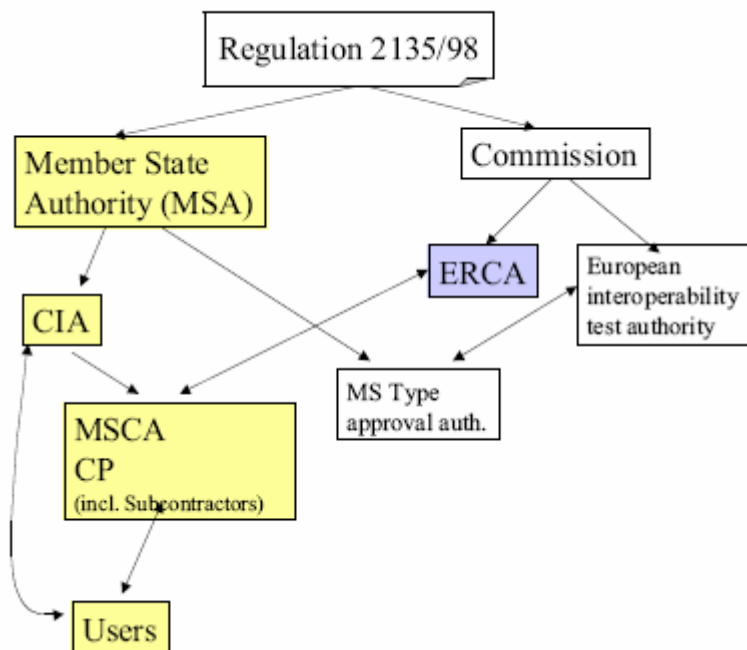


Figure 1 – Digital Tachograph system organization

Responsible for this National MSA policy is the Portuguese Member State Authority, P-MSA:

IMTT

Instituto da Mobilidade e dos Transportes Terrestres, I.P.

Av. das Forças Armadas, 40
 1649-022 Lisboa

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

The **IMTT** is also in charge of the P-CIA authority.

The appointed P-MSCA is:

ISQ – Instituto de Soldadura e Qualidade

TagusPark
Av. Prof. Dr. Cavaco Silva, 33
2740-120 Porto Salvo

The appointed P-CP is:

Imprensa Nacional-Casa da Moeda, SA

Av. António José de Almeida
1000-042 Lisboa

1.2. Approval

This P-MSA policy was approved by:

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

on April 4th, 2006.

1.3. Availability and contact details

The P-MSA policy is publicly available at <http://www.dggt.pt/>

Questions concerning this P-MSA policy should be addressed to:

IMTT

Instituto da Mobilidade e dos Transportes Terrestres, I.P.

Av. das Forças Armadas, 40
1649-022 Lisboa

2. Scope and applicability

- [1] The P-MSA policy is valid for the digital tachograph system only.
- [2] The keys and certificates issued by the P-MSCA are only for use within the digital tachograph system.
- [3] The cards issued by the system are only for use within the digital tachograph system.

The scope of the P-MSA Policy within the digital tachograph system is shown in the figure below:

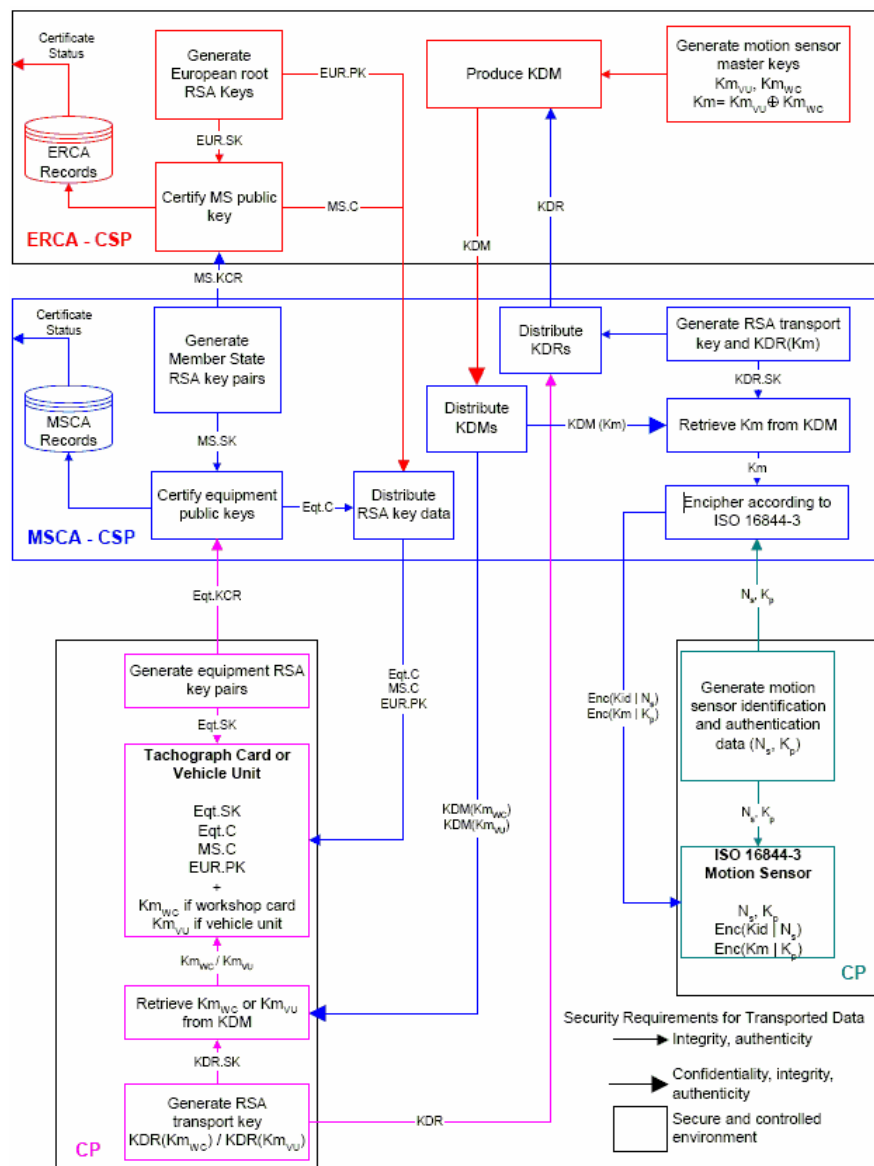


Figure 2 – Digital Tachograph system keys, certificates and equipment management

3. General provisions

3.1. Obligations

This section contains provisions relating to the respective obligations of:

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

3.1.1. P-MSA and P-CIA obligations

[4] The P-MSA will:

- a) Maintain the P-MSA Policy
- b) Appoint a P-MSCA and a P-CP
- c) Audit the appointed P-MSCA and P-CP
- d) Approve the P-MSCA/P-CP PS
- e) Inform the appointed parties about this policy
- f) Prevent unauthorised use of the private keys generated, stored and used under control of this P-MSA Policy
- g) Let this policy be approved by the Commission

[5] The P-CIA will:

- a) Ensure that correct and relevant user information from the application process is input to the P-MSCA and P-CP
- b) Inform the users of the requirements in this policy connected to the use of the system, i.e. the Cardholders

3.1.2. P-MSCA obligations

[6] The appointed P-MSCA will:

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

[7] The P-MSCA will ensure that all requirements on P-MSCA, as detailed in this policy, are implemented.

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

3.1.3. P-CP obligations

[9] The appointed P-CP (card personalization organization) has to:

- a) Follow this P-MSA Policy

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

[10] The P-CP will ensure that all requirements on it, as detailed in this policy, are implemented.

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

3.1.4. Service agencies obligations

[12] Service Agencies will have obligations towards the P-MSA or P-CP and the users according to contractual agreements.

3.1.5. Cardholder obligations

[13] The P-CIA will oblige, through a signed form, the user (or user's organization) to fulfil the following obligations:

- a) to give true information regarding the application data;
- b) to ensure in an appropriate manner, that his card is used for the stated purpose only and to prevent its misuse especially by third persons;
- c) the holders of driver card will be in possession of a single valid driver card;
- d) not to use damaged and expired cards;
- e) to inform the responsible authority about loss, theft, damage or misuse of the card and/or of the respective private key.

3.2. Liability

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

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

[14] Tachograph cards, keys and certificates are only for use within the digital tachograph system. Any other certificates present on Tachograph cards are in violation of this policy, and hence neither the P-MSA, the P-CIA, the P-MSA nor the P-CP carries any liability in respect to such use.

3.2.1. P-MSA and P-CIA liability towards users and relying parties

[15] The P-MSA and P-CIA are liable for damages resulting from failures to fulfil their obligations only if they have acted negligently. If the P-MSA or P-CIA has acted according to this P-MSA Policy, and any other governing document, it will not be considered to have been negligent.

3.2.2. P-MSA and P-CP liability towards the P-MSA and P-CIA

[16] The P-CP or P-MSA is liable for damages resulting from failures to fulfil these obligations only if it has acted negligently. If the organization has acted

according to this P-MSA Policy and the corresponding PS, it will not be considered to have been negligent.

3.3. Interpretation and enforcement

3.3.1. Governing Law

- [17] Any controversy arising from the interpretation or performance of this policy shall be settled according to the Portuguese Law.

3.4. Confidentiality

Confidentiality is restricted according to Portuguese Law 67/98, dated Oct 26th, which follows 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.

3.4.1. Information to be kept confidential

- [18] Any personal or corporate information held by the P-MSCA, or the P-CP that is not appearing on issued cards or certificates is considered confidential, and will not be released without the prior consent of the user, nor (where applicable) without prior consent of the user's employer or representative, unless required otherwise by law.
- [19] All private and secret keys used and handled within the P-MSCA/P-CP operation under this P-MSA Policy are to be kept confidential.
- [20] Audit logs and records will not be made available as a whole, except as required by law.

3.4.2. Information not considered confidential

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

4. Practice Statement (PS)

[23] The P-MSCA and P-CP will have statements of the practices and procedures used to address all the requirements identified in the P-MSA Policy, here below known as Practice Statements (PS). The P-MSA will approve the PS.

In particular:

- a) The PS will identify the obligations of all external organizations supporting the P-MSCA and P-CP services including the applicable policies and practices.
- b) The PS will be treated as restricted information and made available to the P-MSA. The contents of this PS shall be made available to users of the digital tachograph system, and to relying parties (e.g. control bodies) on a "need to know basis".

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

- c) The management of the P-MSCA/P-CP has responsibility for ensuring that the PS is properly implemented.
- d) The P-MSCA/P-CP will define a review process for the PS.
- e) The P-MSCA/P-CP will give due notice of changes it intends to make in its PS and will, following approval, make the revised PS immediately available.

5. Equipment management: cards and tachographs

- [24] The P-MSCA ensures as per the instructions of the P-MSA that the certificates produced and the secret keys correspond to their intended purpose, and are used in cards and recording equipment which meet the requirements of Regulation (EC) 2135/98 only.
- [25] The P-MSCA refuses to deliver keys and certificates if there is a risk of these keys and certificates being misused.
- [26] The P-CIA and the P-CP guarantees adherence to application and delivery procedures for recording equipment cards defined by the P-MSA according to the instructions of Regulation (EC) 2135/98.
- [27] The P-CIA and the P-CP ensures within its authority that issuing of replacement cards and card renewal takes place only as per the prerequisites mentioned in Regulation (EC) 2135/98 and that the prescribed time limits can be adhered to.
- [28] The P-CP ensures that the recording equipment cards are personalized logically according to the instructions of Regulation (EC) 2135/98. The integrity of the entered data must be especially maintained in this respect.
- [29] The P-MSCA and the P-CP ensure within their respective authority that private and secret keys are stored and used in a secured production environment.
- [30] The P-CIA makes the relevant data available so that it can be traced as to which card was issued to which bearer/user.
- [31] The P-CIA ensures that personalized cards are safely delivered within the time limits given by Regulation (EC) 2135/98 and that the bearer/user is personally identified at any time before hand over the card.
- [32] The P-CP ensures that the workshop cards are provided with a PIN as per the instructions of Regulation (EC) 2135/98.
- [33] The PIN is generated in a system secured against unauthorized access, which prevents the possibility of an assignment of the PIN and the workshop card later on. After generation, the PIN will be printed, sealed in an envelope (PIN letter) and delivered in a secure way only to that person to whom the workshop card was issued under separate cover and not along with the personalized cards.
- [34] The reconstruction of a PIN must be impossible.

6. Keys management

This section contains provisions for the management of:

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

The **ERCA public key** is used for verifying the Portuguese certificates.

The **Portuguese keys** are the Portuguese signed keys and may also be called Portuguese root keys.

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

The **transport keys** are the asymmetric key pairs used for securely exchanging information between the ERCA and the P-MSCA/P-CP.

If the P-MSCA has need for other cryptographic keys than the above, these will not be considered part of the digital tachograph system, and is not dealt with in this policy.

6.1. ERCA public key

- [35] The P-MSCA will keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times.
- [36] The P-MSA shall recognise the distribution of the ERCA public format described in the ERCA policy Annex B.
- [37] The P-CP and the equipment manufacturers will ensure that EUR.PK is inserted in all tachograph cards and vehicle units within their authority.

6.2. Key pair of the P-MSA

The Portuguese keys are used to sign all equipment certificates. The key pair consists of a public key (P.PK) and a private, or secret, key (P.SK).

- [38] The P-MSA public key will be certified by the ERCA, but will be generated by the P-MSCA.
- [39] The P-MSA shall take into account the turnaround time required by the ERCA to certificate its keys.
- [40] The P-MSA shall use the Key Certification Requests format in the ERCA policy Annex A.
- [41] The P-MSA ensures that the keys shall be exclusively used for:

- signing digital tachograph system equipment,
- production of the ERCA key certification request,
- issuing Certificate Revocation Lists.

6.2.1. P-MSCA key pair generation

- [42] The P-MSCA key pair generation will be carried out within a device which either:
- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher; or
 - meets the requirements identified in CEN Workshop Agreement 14167-2; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408, to E3 or higher in ITSEC, or
 - is demonstrated to provide an equivalent security criteria.
- [43] The P-MSCA shall sign equipment certificates within the same device used to store the Member State Private Keys.
- [44] The actual device used and requirements met will be stated in the P-MSCA PS.
- [45] P-MSCA key-pair generation will require the active participation of two separate individuals. At least one of these will have a role of CAA/PA (certification authority/ personalization administrator).
- [46] The P-MSCA will have at least two (2) and maximum five (5) Portuguese key pairs with associated signing certificates to ensure continuity.

6.2.2. Validity of the Portuguese key pair

- [47] The Portuguese key pair shall be used for a maximum period of two (2) years from certification of the corresponding public key, and will be destroyed by the P-MSCA to prevent any future use.

6.2.3. P-MSCA private key storage

- [48] The private keys will be contained in and operated from inside a specific tamper resistant device which:
- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408, to E3 or higher in ITSEC, or
 - is demonstrated to provide an equivalent security criteria.
- [49] No single person will possess the means required to access the environment where the private key is stored.

6.2.4. P-MSCA private key backup

- [50] The P-MSCA private signing keys may be backed up, using a key recovery procedure requiring at least dual control. The procedure used will be stated in

the P-MSCA PS. However, if key pairs according to [46] are used, no backup is needed.

6.2.5. Portuguese private key escrow

[51] The Portuguese private keys will not be escrowed.

6.2.6. Portuguese keys compromise

[52] A written instruction will exist, included in the P-MSCA PS, which states the measures to be taken by users and security responsible persons at the P-MSCA if the Portuguese private keys have become exposed, or are otherwise considered or suspected to be compromised.

[53] In such case, the P-MSCA, as a minimum will inform, without delay of loss, the P-MSA, the ERCA and all other MSCAs.

6.2.7. Portuguese keys end of life

[54] The P-MSCA will have routines to ensure that it always has a valid, certified Portuguese signing key pair.

[55] Upon termination of use of a Portuguese signing key pair, the public key will be archived, and the private key will be destroyed such that it cannot be retrieved.

6.3. Motion Sensor keys

[56] The P-CP will, as needed, request the motion sensor key Km_{wc} from the ERCA (Regulation Annex 1B, app 11:3.1.3).

[57] The P-MSA shall request motion sensor master keys using the key distribution request (KDR) protocol described in the ERCA policy Annex D.

[58] The P-MSCA will forward the encrypted Key Distribution Message to the P-CP, by appropriately secured means, for insertion of the Km_{wc} into Workshop cards.

[59] The P-CP will undertake the P-MSCA's task to ensure that the workshop key Km_{wc} is inserted into all issued Workshop cards (Regulation Annex 1B, app 11:3.1.3).

[60] The P-CP shall assure the confidentiality, integrity, availability and prevent unauthorised use of the motion sensor key Km_{wc} , and will, during storage, use and distribution, protect the motion sensor key with high assurance physical and logical security controls. The key should be contained in and operated from a specific tamper resistant device which:

- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408, to E3 or higher in ITSEC, or
- is demonstrated to provide an equivalent security criteria.

6.4. Transport keys

- [61] For secure data communication the P-CP issues special, asymmetric transport key pairs. The P-CP will, during storage, use and distribution, protect private keys of the pair with high assurance physical and logical security controls. The keys should be contained in and operated from a specific tamper resistant device which:
- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher;
or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408, to E3 or higher in ITSEC, or
 - is demonstrated to provide an equivalent security criteria.
- [62] The P-MSA shall ensure that the Key Identifier (KID) and modulus (n) of the P-MSCA keys submitted to the ERCA for certification and of the transport keys for motion sensor key distribution are unique within its domain.
- [63] The P-MSA shall use the physical media to transport P-MSCA key certification requests, P-MSCA certificates, the ERCA public key, and the motion sensor master keys described in the ERCA policy Annex C.

7. Equipment keys (asymmetric)

Equipment keys are asymmetric keys generated somewhere in the issuing/manufacturing process, and certified by the P-MSCA for the tachograph cards in the digital tachograph system.

7.1. General aspects about P-MSCA and P-CP

- [64] In the equipment (Card) initialization, key loading and personalization will be performed in a physically secure and controlled environment. Entry to this area will be strictly regulated, controllable at the individual level, and requiring a minimum of two persons to be present to operate the system. A log will be kept of the entries and the actions in the system.
- [65] No sensitive information contained in the key generation systems leaves the system in a way that violates this policy.
- [66] No sensitive information in the equipments' personalization systems must leave them in a way that violates this policy.

7.2. Equipment key generation

- [67] The entity that performs the key generation will make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.
- [68] Key generation will be carried out within a device which either:
 - meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher; or
 - meets the requirements identified in CEN Workshop Agreement 14167-2; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408, to E3 or higher in ITSEC, or
 - is demonstrated to provide an equivalent level of security.
- [69] The generation procedure and storage of the private key will prevent it from being exposed outside of the system that created it. Furthermore, it will be erased from the system immediately after having been inserted in the device.
- [70] Key certification requests that rely on transportation of private keys are not allowed.
- [71] It is the responsibility of the key generation entity to undertake adequate measures to ensure that the public key is unique within its domain before certificate binding takes place.

7.2.1. Equipment key validity

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

7.2.2. Equipment private key protection and storage - cards

- [73] The P-CP will 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.

- [74] Copies of the private key will be kept in the tachograph card only. Should its use be necessary during the personalization process, the keys will be kept encrypted.

7.2.3. Equipment private key escrow and archival

- [75] Equipment private keys will be neither escrowed nor archived.

7.2.4. Equipment public key archival

- [76] All certified public keys will be archived by the certifying P-MSCA.

8. Equipment certificate management

This section describes the certificate life cycle, containing registration function, certificate issuing, distribution, use, renewal, and end of life.

8.1. Data input

[77] The key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.

[78] The P-MSCA will verify the uniqueness of the CHR in the issue of the certificates

8.2. Tachograph card certificates

8.2.1. Driver certificates

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

8.2.2. Workshop certificates

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

8.2.3. Control body certificates

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

8.2.4. Hauling company certificates

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

8.3. Equipment certificate time of validity

[83] Certificates will not be valid longer than the corresponding equipment:

- Driver certificates will not be valid more than 5 years (Regulation 14.4.a).
- Workshop certificates will not be valid for more than 1 year (Regulation 12.1).
- Control body certificates will not be valid more than 5 years.
- Hauling company certificates will not be valid more than 5 years.
- Vehicle Unit certificates will not be valid more than 30 years.

8.4. Equipment certificate issuing

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

8.5. Equipment certificate renewal and update

Since certificates and cards have the same time of validity, they are dealt with together. It is assumed that the lifetime of the equipment is shorter than that of the certificate.

8.6. P-MSCA informative tasks

- [85] The P-MSCA will be responsible to transfer all certificate data to the P-CP and the manufacturers, so that certificates, equipment as well as cards and cardholders are interlinked.
- [86] If certain authorities have a legitimate interest in special, non-public information on the functioning of the P-MSCA or its external contractors, and no rules or security considerations are against giving this information, the P-MSCA makes the right information available as quickly as possible in coordination with the P-MSA.
- [87] The operation of the P-MSCA has to be treated as confidential. Information contained in it may be viewed in agreement with the P-MSA on location at P-MSCA, when there is a proven, legitimate interest and when the confidentiality of the information is also adequately protected at the receiver.
- [88] The P-MSCA shall maintain and make certificate status information available.

9. Information security management

9.1. Information management of the P-MSCA and P-CP

- [89] The P-MSCA/P-CP shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.
- [90] The P-MSCA/P-CP shall retain responsibility for all aspects of the provision of key certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the P-MSCA/P-CP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the P-MSCA/P-CP. The P-MSCA/P-CP shall retain responsibility for the disclosure of relevant practices of all parties.
- [91] The information security infrastructure necessary to manage the security within the P-MSCA/P-CP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the P-MSA.
- [92] The P-MSCA/P-CP shall adopt a security management system equivalent to ISO 17799. Formal certification is not required.

9.2. Asset classification and management of the P-MSCA/P-CP

- [93] The P-MSCA/P-CP will ensure that its assets and information receive an appropriate level of protection.

In particular:

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

9.3.1. Trusted roles

- [94] The P-MSCA/P-CP, supporting this P-MSA Policy, should recognize three distinct roles, as outlined below.
- [95] To ensure that one person acting alone cannot circumvent safeguards, responsibilities in P-MSCA/P-CP systems need to be attended by multiple roles and individuals. Each account on the systems will have limited capabilities, commensurate with the role of the account holder.
- [96] The roles are:
 - a) Certification Authority Administrator or Personalization Administrator (CAA/PA)

- b) System Administrator (SA)
- c) Information System Security Officer (ISSO)

[97] The CAA/PA role includes:

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

[98] 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.

[99] 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 P-MSCA/P-CP's records;
- f) Participating in Member State key generation.

9.3.2. Separation of roles

[100] For the P-MSCA/P-CP, different individuals shall fill each of the three roles described above

9.3.3. Identification and authentication for each role

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

9.3.4. Background, qualifications, experience and clearance requirements

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

- 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 a clean criminal record and satisfactory credit check;
- d) have received proper training in the performance of their duties.

[103] P-MSCA/P-CP organizations may also specify special requirements such as requirements for citizenship, rank and qualifications. Such requirements should be stated in the applicable PS.

9.3.5. Training requirements

[104] Personnel will have adequate training for the role and job.

9.4. System security controls of the CA and personalization systems

[105] The P-MSCA/P-CP will ensure that the systems are secure and correctly operated, with minimal risk of failure.

In particular:

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

[106] The P-MSCA/P-CP systems will provide sufficient system security controls for enforcing the separation of roles described in this policy or the relevant PS.

9.4.1. Specific computer security technical requirements

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

9.4.2. Computer security rating

[108] The P-MSCA/P-CP systems do not require formal rating as long as they fulfil all requirements in this section.

9.4.3. System development controls

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

[110] Change control procedures will exist for releases and modifications for any operational software.

9.4.4. Security management controls

[111] The system roles will be implemented and enforced.

9.4.5. Network Security Controls

- [112] Controls (e.g., firewalls) shall be implemented to protect the P-MSCA/P-CP's internal network domains from external network domains accessible by third parties.
- [113] 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 that affect the outcome of keys, certificates and equipment issuing processes under this policy.

9.5.1. Types of event recorded

- [114] The security audit functions related to the P-MSCA/P-CP computer/system will 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

- [115] The log will be processed regularly and analyzed against malicious behaviour. Log procedures will be described in the PS.

9.5.3. Retention period for audit log

- [116] Audit log will be retained for at least 2 years.

9.5.4. Protection of audit log

- [117] Audit logs will be appropriately integrity protected. All entries will be individually time stamped (system time is sufficient).
- [118] Audit logs shall be verified and consolidated at least monthly. At least two people in SA or ISSO roles shall be present for such verification and consolidation.

9.5.5. Audit log backup procedures

- [119] The audit log will be protected from unauthorized access.

9.5.6. Audit collection system (internal vs. external)

- [120] Only internal audit collection system is required.

9.6. Record archiving

9.6.1. Types of event recorded by the P-CIA

- [121] The records will include all relevant evidence in the P-CIA's possession including, but not limited to:
- a) Certificate requests and all related messages exchanged with the P-MSCA/P-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) 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 P-MSCA/P-CP

- [122] The records will include all relevant evidence in the P-MSCA/P-CP's possession including, but not limited to:
- a) Contents of issued certificates;
 - b) Audit journals including records of annual auditing of P-MSCA/P-CP's compliance with its PS;
 - c) Currently and previously implemented certificate policy documents and their related PSs.
- [123] Records of all digitally signed electronic requests made by P-MSCA/P-CP personnel (CAA/PA) will 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

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

9.6.4. Procedures to obtain and verify archive information

- [125] The P-MSCA/P-CP will act in compliance with requirements regarding confidentiality as stated in section 3.4.
- [126] Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.
- [127] P-MSCA/P-CP will make available on justified request, produced documentation of the P-MSCA/P-CP's compliance with the applicable PS according to section 11.5.
- [128] Subject to statute, a reasonable handling fee may be charged to cover the cost of record retrieval.

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

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

9.7. Continuity planning

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

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

9.7.1. Portuguese keys compromise

Portuguese keys compromise is dealt with in section 6.2.6.

9.7.2. Other disaster recovery

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

9.8. Physical security control

[133] Physical security controls will be implemented to control access to the P-MSCA and P-CP hardware and software. A log will be kept over all physical entries to this area (or areas).

[134] The Portuguese keys for signing certificates will be kept physically and logically protected as described in the PS.

[135] The P-MSCA/P-CP's facility will also have a place to store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. Backup media will also be stored at a site different from where the P-MSCA/P-CP system resides, to permit restoration in the event of a natural disaster to the primary facility.

[136] A security check of the facility housing the P-MSCA/P-CP's central equipment will be made at least once every week.

9.8.1. Physical access

[137] Access may be controlled through the use of an access control list to the room housing the systems. A person will escort anyone not on the access control list. If an access control list is not feasible for a particular site, the P-MSCA and

P-CP related material will be locked in a secure room or storage area when it is not being used.

10.P-MSCA or P-CP termination

10.1. Final termination

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

[138] The P-MSA will ensure that the tasks outlined below are carried out.

[139] Before the P-MSCA/P-CP terminates its services the following procedures have to be completed as a minimum:

- a) Inform all users and parties with whom the P-MSCA/P-CP has agreements or other form of established relations;
- b) Make publicly available information of its termination at least 3 month prior to termination.
- c) The P-MSCA/P-CP will terminate all authorization of subcontractors to act on behalf of the P-MSCA/P-CP in the process of issuing certificates.
- d) The P-MSCA/P-CP will perform necessary undertakings to maintain and provide continuous access to record archives by handing them over to P-MSA on request.

10.2. Transfer of responsibility

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

[140] The P-MSA will ensure that orderly transfer of responsibilities and relevant assets is carried out.

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

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

11. Audit

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

11.1. Frequency of entity compliance audit

[144] A P-MSCA/P-CP operating under this P-MSA Policy will be audited at least annually for conformance with this policy. At the time of auditing the P-MSCA/P-CP operation, the concurrence of the current operation with the requirements of the ERCA must be especially verified.

11.2. Topics covered by audit

[145] The audit will cover the P-MSCA/P-CP´s practices.

[146] The audit will cover the P-MSCA/P-CP´s compliance with this P-MSA Policy.

[147] The audit will cover the P-MSCA/P-CP´s compliance with the requirements defined in ERCA-CP § 5.3

11.3. Who should do the audit

[148] The P-MSA may ask an external certification or accreditation organization to approve the P-MSCA/P-CP PS. Otherwise the P-MSA will undertake the auditing.

11.4. Actions taken as a result of deficiency

[149] If irregularities are found in the audit the P-MSA will take appropriate action depending on severity.

11.5. Communication of results

[150] The P-MSA includes the results of the audit in a report that defines corrective actions including an implementation schedule, required to fulfil the P-MSA obligations. The report will be provided, in English, to the ERCA.

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

12.P-MSA policy change procedures

12.1. Items that may change without notification

[152] The only changes that may be made to this document without notification are:

- a) Editorial or typographical corrections;
- b) Changes to the contact details or names of the organizations.

12.2. Changes with notification

12.2.1. Notice

[153] Any item in this P-MSA policy may be changed with 90 days notice.

[154] Changes to items which, in the judgment of the policy responsible organization (the P-MSA), will not materially impact a substantial majority of the users or relying parties using this policy may be changed with 30 days notice.

12.2.2. Comment period

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

12.2.3. Whom to inform

[156] Information about changes to this policy will be sent to:

- ERCA
- P-MSCA and P-CP including Service Agencies

[157] 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 P-MSA policy approval

[158] If a policy change is required by the P-MSA, the P-MSA will submit the revised P-MSA Policy to the Commission for approval.

13. Conformity to the ERCA policy

The table below provides the rationale addressing required in the ERCA Policy paragraph 5.2.3.

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.1	The MSA Policy shall identify the entities in charge of operations.	1.1. Responsible organizations.
5.3.2	The MSCA key pairs for equipment key certification and for motion sensor master key distribution shall be generated and stored within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC; or equivalent security criteria. These evaluations shall be to a protection profile or security target, d) is demonstrated to provide an equivalent level of security.	6.2.1. P-MSCA key pair generation. [42] 6.4. Transport keys. [61]
5.3.3	Member State Key Pair generation shall take place in a physically secured environment by personnel in trusted roles under, at least dual control.	6.2.1. P-MSCA key pair generation. [45] 9.3.1. Trusted Roles. [94] to [99] 9.4. System security controls of the CA and personalization systems. [105] and [106] 9.8. Physical security control. [133] to [136] 9.8.1. Physical access. [137]
5.3.4	The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.	6.2.2. Validity of the Portuguese key pair. [47]

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.5	The generation of new Member State Key Pairs shall take into account the one month turnaround time required for certification by the ERCA	6.2. Key pair of the P-MSA. [39]
5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in its Annex A.	6.2. Key pair of the P-MSA. [40]
5.3.7	The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.	6.3. Motion Sensor keys. [57]
5.3.8	The MSA shall recognize the ERCA public key in the distribution format described in Annex B.	6.1. ERCA public key. [36]
5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C.	6.4. Transport keys. [63]
5.3.10	The MSA shall ensure that the Key Identifier (KID) and modulus (n) of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of the MSCA.	6.4. Transport keys. [62]
5.3.11	The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either: destroyed so that the private key cannot be recovered or retained in a manner preventing its use.	6.2.2. Validity of the Portuguese key pair. [47]

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.12	<p>The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall:</p> <ul style="list-style-type: none"> • ensure that any relevant prescription mandated by security certification of the equipment is met. • ensure that both generation and insertion (if not onboard) takes place in a physically secured environment; • unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used; <p>The last two of these requirements on generation shall be met by generating equipment keys within a device which either:</p> <p>a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher;</p> <p>b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2;</p> <p>c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC; or equivalent security criteria. These evaluations shall be to a protection profile or security target.</p> <p>d) is demonstrated to provide an equivalent level of security.</p>	<p>5. Equipment management: cards and tachographs. [29]</p> <p>7.1. General aspects about P-MSCA and P-CP. [64]</p> <p>7.2. Equipment key generation. [67] and [68]</p>

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.13	The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA Policy.	<p>3.4.1. Information to be kept confidential. [19]</p> <p>5. Equipment management: cards and tachographs. [29]</p> <p>6.2.1. P-MSCA key pair generation. [43] and [46]</p> <p>6.2.3. P-MSCA private key storage. [48] and [49]</p> <p>6.4. Transport keys. [61]</p> <p>7.1. General aspects about P-MSCA and P-CP. [65] and [66]</p> <p>7.2. Equipment key generation. [67] to [70]</p> <p>7.2.2. Equipment private key protection and storage - Cards. [73] and [74]</p>
5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	3.1.1. P-MSA and P-CIA obligations. [4] g).
5.3.15	The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.	6.2.4. P-MSCA private key backup. [50]
5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	7.2. Equipment key generation. [70]
5.3.17	Key escrow is strictly forbidden	<p>6.2.5. Portuguese private key escrow. [51]</p> <p>7.2.4. Equipment private key escrow and archival. [75]</p>
5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	<p>3.4.1. Information to be kept confidential. [19]</p> <p>6.3. Motion Sensor keys. [60]</p>

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.19	The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO / IEC 16844-3 standard.	Not applicable.
5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	Not applicable.
5.3.21	The MSA shall forward the workshop card motion sensor key (KmWC) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	6.3. Motion Sensor keys. [58]
5.3.22	The MSA shall forward the vehicle unit motion sensor key (KmVU) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	Not applicable.
5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	6.3. Motion Sensor keys. [60]
5.3.24	<p>The MSA shall ensure that its motion sensor key copies are stored within a device which either:</p> <p>a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher;</p> <p>b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC ; or equivalent security criteria. These evaluations shall be to a protection profile or security target.</p>	6.3. Motion Sensor keys. [60]

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.25	The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.	Not applicable. No VU manufacturer is included in the Portuguese system organisation.
5.3.26	The MSA shall ensure availability of its equipment public key certification service.	6.2.1. P-MSCA key pair generation. [46]
5.3.27	The MSA shall only use the Member State Private Keys for: a) the production of Annex I(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in Annex I(B) Appendix 11 Common Security Mechanisms; b) production of the ERCA key certification request as described in Annex A. c) issuing Certificate Revocation Lists if this method is used for providing certificate status information (see 5.3.30).	6.2. Key pair of the P-MSA. [41]
5.3.28	The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).	6.2.1. P-MSCA key pair generation. [43]
5.3.29	Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B).	8.1. Data input. [78]
5.3.30	Unless key generation and certification is performed in the same physically secured Environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.	8.1. Data input. [77]
5.3.31	The MSA shall maintain and make certificate status Information available.	8.7. P-MSCA informative tasks. [88]

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.32	The validity of a tachograph card certificate shall equal the validity of the tachograph card.	8.4. Equipment certificate time of validity. [83]
5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	8.4. Equipment certificate time of validity. [83]
5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	Not applicable
5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	5. Equipment management: cards and tachographs. [31]
5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	6.2.6. Portuguese keys compromise. [53]
5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	6.2.1. P-MSCA key pair generation. [46] 9.7. Continuity planning. [131]
5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	9.1. Information management of the P-MSCA and P-CP. [92]
5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	9.3. Personnel security controls of the P-MSCA/P-CP. [94] to [104]
5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	9.6.2. Types of event recorded by the P-MSCA/P-CP. [122] and [123]
5.3.41	The MSA shall include provisions for MSCA termination in the MSA Policy.	10.1. Final termination. [138] and [139]
5.3.42	The MSA Policy shall include change procedures.	12. P-MSA policy change procedures. [152] to [158]
5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	11.1. Frequency of entity compliance audit. [147]
5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.	11.1. Frequency of entity compliance audit. [144]

Reference ERCA policy	Requirement	Reference P-MSA policy
5.3.45	The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit report, in English, to the ERCA.	11.5. Communication of results. [150]
5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfil the MSA obligations.	11.5. Communication of results. [150]

14. References

- [1] Council Regulation (EC) No 2135/98 of 24th September 1998; Official Journal of the European Communities L274, 09.10.98.
- [2] Commission Regulation (EC) No 1360/2002 of 13th June 2002; Official Journal of the European Communities L207, 05.08.2002.
- [3] Common Security Guidelines, v1.0; Card Issuing Group SWG3.
- [4] Guideline and Template National CA Policy for the Digital Tachograph System, v1.0; Card Issuing Group SWG3.
- [5] ETSI TS 102 042 V1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates
- [6] Commission Regulation (EC) No 1360/2002, Annex I(B) Appendix 11 - Common security mechanisms
- [7] ISO / IEC 17799:2005 Information technology – Code of practice for information security management
- [8] FIPS PUB 140-2 Security Requirements for Cryptographic Modules NIST, 2001
- [9] CEN Workshop Agreement 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)
- [10] ISO / IEC 15408 (Parts 1 to 3) Information technology – Security techniques – Evaluation criteria for IT security.
- [11] ITSEC Information Technology Security Evaluation Criteria 1991 v1.2
- [12] ISO / IEC 9794-8 | ITU-T Recommendation X.509 Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- [13] PKCS#1 v2.0: RSA Cryptography Standard, RSA Laboratories, October 1, 1998.
- [14] Digital Tachograph System European Root Policy, Version 2.0; European Commission Special Publication I.04.131; published at <http://dte.jrc.it>.

15. Glossary/Definitions and abbreviations

15.1. Glossary/Definitions

P-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".

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

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

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

Equipment: In the digital tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.

Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.

Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.

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

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

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

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

Service Agency: An entity or subcontractor that undertakes to tasks on behalf of the P-MSA or P-CP.

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

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

In this document:

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

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

15.2. List of abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card Personalizing Organization
CPS	Certification Practice Statement
ERCA	European Root CA
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KG	Key Generation
KCR	Key Certification Request
KDR	Key Distribution Request (for motion sensor master keys)
KDM	Key Distribution Message (encrypted motion sensor master key)
MS	Member State
MSA	Member State Authority
MSCA	Member State CA
P-CIA	Portuguese CIA
P-CP	Portuguese CP
P-MSA	Portuguese State Authority
P-MSCA	Portuguese 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

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.