Ministero dello Sviluppo Economico

Italian Tachograph MSA Policy v.1.1

Amendment History

Version Control	**Issue Date**	**Status**
Version 1.0	May 2004	Approved by the European Authority
Version 1.1	Feb 2011	Approved by the European Authority

Table of Contents

0 Introduction

This document is the Italian Tachograph MSA Policy for the Tachograph system in Italy, here in after referred to as I-MSA Policy.

This I-MSA Policy is in accordance with:

- Council Regulation (EC) No 2135/98; Official Journal of the European Communities L274, 09.10.98.
- Commission Regulation 1360/2002; Official Journal of the European Communities L207, 05.08.2002.
- European Root CA Policy [ERCA Policy].
- Decree of Italian Ministero delle Attività Produttive (2003, 31st of October, n.361).

0.1 Responsible organization

The authority responsible for implementing the Council Regulation 2135/98 in Italy, referred to as I-MSA (Italian - Member State Authority), is the

Ministero dello Sviluppo Economico
Via Molise, 2 – 00187 Roma
Italy

The I-MSA is responsible for this I-MSA Policy.

The appointed I-CIAs are the Italian Chambers of Commerce

The appointed I-CA and I-CP is

InfoCamere S.C.p.A.
Corso Stati Uniti, 14 - 35127 Padova
Italy

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

0.2 Approval

This I-MSA Policy version 1.1 is approved by the European Commission, namely by the Digital Tachograph Root Certification Authority (ERCA).

0.3 Availability and contact details

The I-MSA Policy is publicly available at www.sviluppoeconomico.gov.it.

Questions concerning this I-MSA Policy should be addressed to:

Ministero dello Sviluppo Economico
Direzione Generale per il Mercato, la Concorrenza, il Consumatore, la Vigilanza e la Normativa Tecnica
Via Sallustiana, 53 -00187 Roma
Italy

1 Scope and applicability

[r1.5] This I-MSA Policy is valid for the Tachograph system only.

[r1.10] The keys and certificates issued by the I-CA are only for use within the Tachograph system.

[r1.15] The cards issued by the system are only for use within the Tachograph system.

The scope of the I-MSA Policy within the Tachograph system is shown in the figure below in bold. The shaded area is outside the scope of this Policy.

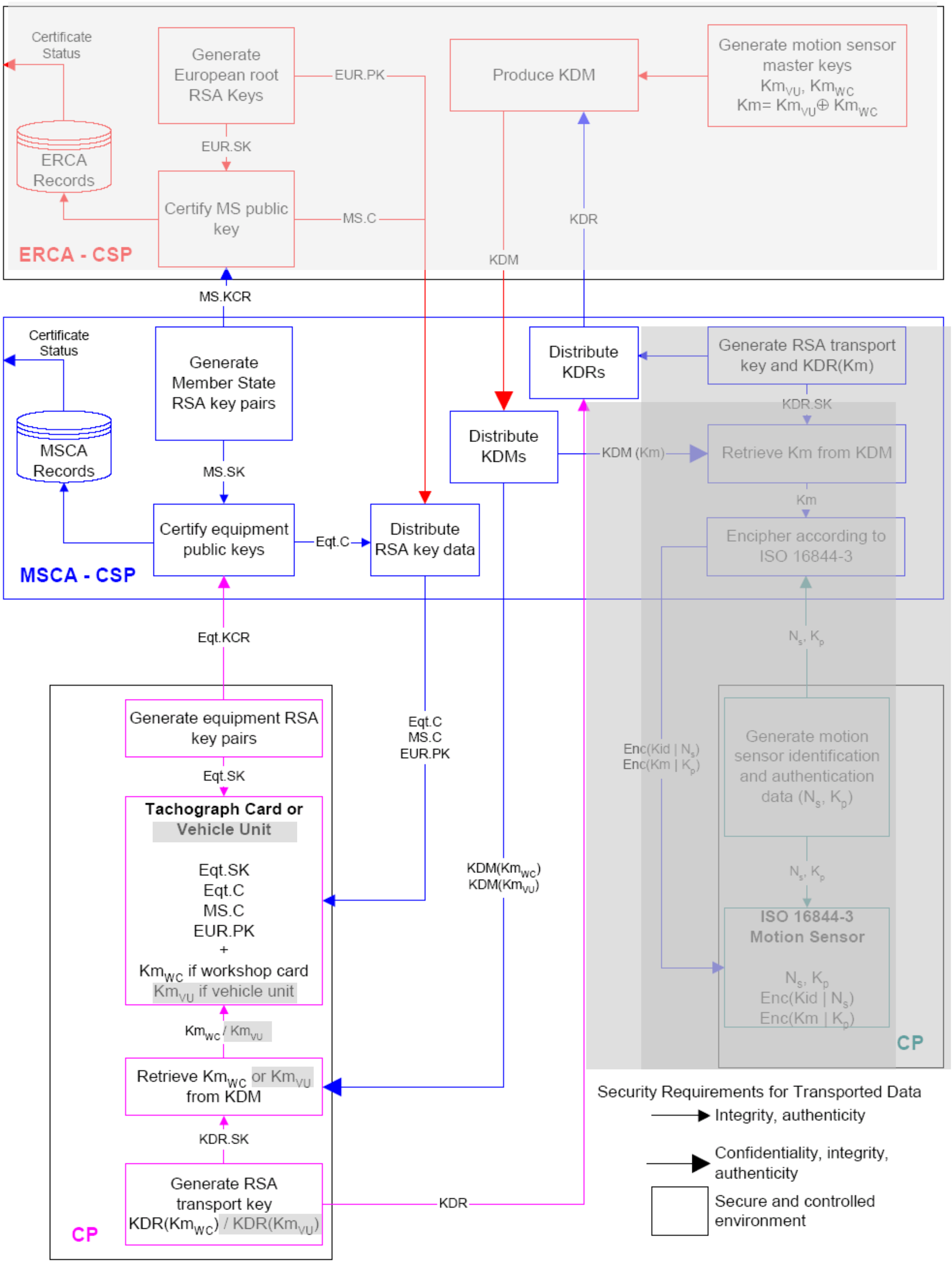
Certificate Status
Generate European root RSA Keys
EUR.PK
Produce KDM
Generate motion sensor master keys Km_{VU}, Km_{WC} $Km= Km_{VU} \oplus Km_{WC}$
ERCA Records
EUR.SK
Certify MS public key
MS.C
KDR
KDM
ERCA - CSP
MS.KCR
Certificate Status
Generate Member State RSA key pairs
Distribute KDRs
Generate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

Figure1. Description of Annex I(B) Key management (scope of this Policy)

2 General provisions

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

2.1 Obligations

This section contains provisions relating to the respective obligations of:

- I-MSA and I-CIA.
- I-CA and Service Agency (if any).
- I-CP and Service Agency (if any).
- Users (Cardholders).

2.1.1 MSA and CIA obligations

With regard to this Policy, the I-MSA and I-CIA have the following obligations.

[r2.05] The I-MSA:

a) Maintains the I-MSA Policy (this document).
b) Appoints an I-CA and a I-CP.
c) Audits the appointed I-CA and I-CP including Service Agencies.
d) Approves the I-CA/I-CP PS.
e) Informs the appointed parties about this Policy.
f) Submits this Policy to be approved by the Commission.
g) Informs the users of the requirements in this Policy connected to the use of the system.

[r2.10] The I-CIA:

a) Ensures that correct and relevant user information from the application process is input to the I-CA and I-CP.
b) Treats and protects all the personal data in conformity with the national legislation.

2.1.2 CA obligations

[r2.15] The appointed I-CA shall:

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

[r2.20] The I-CA shall ensure that all requirements on I-CA, as detailed in this Policy, are implemented.

[r2.25] The I-CA has the responsibility for conformance with the procedures prescribed in this Policy, even when the I-CA functionality is undertaken by subcontractors, Service Agencies. The I-CA is responsible for ensuring that any Service Agency provides all its services consistent with its Practice Statement (PS) and the I-MSA Policy .

[r2.26] When a cooperation administrative arrangement exists between Italy and another State, the I_CA is authorised by the I_MSA to use the Italian national keys to produce public key certificates for all tachograph cards issued by the CIA of this State.

2.1.3 CP obligations

[r2.30] The appointed I-CP (card personalization organization) shall:

a) Follow this I-MSA Policy.

b) Produce a CP Practice Statement (CP PS) that includes reference to this I-MSA Policy , to be approved by the I-MSA.

c) Maintain sufficient organizational and financial resources to operate in conformity with the requirements laid down in this I-MSA Policy , in particular to bear the risk of liability damages.

[r2.35] The I-CP shall ensure that all requirements on it, as detailed in this Policy, are implemented.

[r2.40] The I-CP has the responsibility for conformance with the procedures prescribed in this Policy, even when the I-CP functionality is undertaken by subcontractors, Service Agencies.

[r2.41] When a cooperation administrative arrangement exists between Italy and another State, the I_CP is authorised by the I_MSA to perform personalization services for the CIA of this State.

2.1.4 Service Agency obligations

[r2.45] Service Agencies (if applicable) have obligations towards the I-CA or I-CP and the users according to contractual agreements.

2.1.5 Cardholder obligations

[r2.50] The I-CIA will oblige, by means of a signed agreement (see 4.1.2), the user (or user's organization) to fulfill the following obligations:

a) accurate and complete information is submitted to the I-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) the user may only use his own keys, certificate and card;

f) a user may have only one valid driver card;

g) a user may not have both a workshop card and a hauling company card; but under very special, and duly justified, circumstances, a user may have both a workshop card and a driver card;

h) the user does not use a damaged or expired card;

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

the equipment private key or card has been lost, stolen or potentially compromised.

2.2 Liability

The I-CA and I-CP do not carry liability towards end users, but only towards the I-MSA and I-CIAs.

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

[r2.55] Tachograph cards, keys and certificates are only for use within the Tachograph system. Any other certificates stored on Tachograph cards are in violation of this Policy, and hence neither the I-MSA, the I-CIA, the I-CA nor the I-CP carries any liability in respect to such use.

2.2.1 MSA and CIA liability towards users and relying parties

[r2.60] The I-MSA and I-CIA are liable for damages resulting from failures to fulfill their obligations only if they have acted negligently. If the I-MSA or I-CIA has acted according to this I-MSA Policy , and any other governing document, it will not be considered to have been negligent.

2.2.2 CA and CP liability towards the MSA and CIA

[r2.65] The I-CP or I-CA is liable for damages resulting from failures to fulfill these obligations only if it has acted negligently. If the organization has acted according to this I-MSA Policy and the corresponding PS, it will not be considered to have been negligent.

2.3 Interpretation and enforcement

2.3.1 Governing law

All trusted third parties who will act according to this national Policy shall fulfill the Italian law “Legislative Decree n.196 (2003, 30th of June) and following modifications with its security regulations on matters which have to do with protection of individuals and personal data.

2.4 Confidentiality

Confidentiality is enforced according to the above cited decree on the protection of individuals with regard to the processing and storing of personal data and on the movement of such data.

2.4.1 Types of information to be kept confidential

[r2.70] Any personal or corporate information held by the I-CA, the I-CP or Service Agencies 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.

[r2.75] All private and secret keys used and handled within the I-CA/I-CP operation under this I-MSA Policy are to be kept strictly confidential.

[r2.80] Audit logs and records shall not be made available as a whole, except as required by law.

2.4.2 Types of information not considered confidential

[r2.85] Certificates are not considered confidential.

[r2.90] 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.

3 Practice Statement (PS)

[r3.05] The I-CA and I-CP shall have statements of the practices and procedures used to address all the requirements identified in the I-MSA Policy.

In particular:

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

b) This Practice Statements (PS) shall be submitted to and approved by the I-MSA.

c) The Practice statement shall be treated as restricted information. The content shall be made available to the users of the Tachograph system, and to relying parties on a “need to know basis”.

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

d) The management of the I-CA/I-CP has responsibility for ensuring that the PS is properly implemented.

e) The I-CA/I-CP shall define a review process for the PS.

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

4 Equipment management

4.1 Tachograph cards

4.1.1 Quality control – CA/CP function

[r4.05] The I-CP shall ensure that only type approved cards according to the Regulation are personalized in the Tachograph system. See also 4.1.5.5.

4.1.2 Application for card – handled by the CIA

[r4.10] The I-MSA informs the user of the terms and conditions regarding use of the card.

[r4.15] The user will, by applying for a card, and accepting delivery of the card, accept the terms and conditions.

[r4.20] The I-CIA shall guarantee adherence to application procedures for cards, defined by the I-MSA according to the EC Regulation 2135/80.

[r4.25] The applicant shall, by making an application for a card and accepting delivery of the card, sign an agreement with the I-MSA (or I-CIA), stating as a minimum the following:

- the user accepts the terms and conditions regarding use and handling of the Tachograph card;
- the user accepts that, under his/her own responsibility, from the time of card acceptance and throughout the operational period of the card, until I-CIA is notified otherwise by the user:
    - ○ no unauthorized person has ever had access to the user's card;
    - ○ all information given by the user to the I-CIA relevant for the information in the card remains valid;
    - ○ the card is being conscientiously used in consistence with usage restrictions for the card.

4.1.3 Card renewal, replacement and exchange handled by the CIA

[r4.30] Workshop cards shall be valid for no more than **one** year from issuance.

[r4.35] Driver cards shall be valid for no more than **five** years from issuance.

[r4.40] Company cards shall be valid for no more than **five** years from issuance.

[r4.45] Control cards shall be valid for no more than **five** years from issuance.

[r4.50] The I-CIA shall establish routines to remind the user of pending expiration. The I-CIA shall guarantee that issuing of replacement cards, card renewal and card exchange or update take place according to the requirements in EC Regulation 2135/80.

4.1.4 Application approval registration – handled by the CIA

[r4.55] The I-CIA shall register approved applications in a database. This data is made available for the I-CA/I-CP, which uses the information as input to the certificate generation and card personalization.

4.1.5 Card personalization – handled by the CP

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

4.1.5.1 Visual personalization

[r4.60] Cards shall be visually personalized according to Regulation Annex 1B, section IV.

4.1.5.2 User data entry

[r4.65] Data shall be inserted in the card according to the structure in Regulation Annex 1B, appendix 2, rules TCS_403, TCS_408, TCS_413 and TCS_418, depending on card type.

4.1.5.3 Key entry

[r4.70] The private key shall be inserted in the card without ever having left the key generation environment. This environment must guarantee that no person, in any way what so ever, can get control of the generated private key without detection. See also equipment key generation, 6.2.

4.1.5.4 Certificate entry

[r4.75] The user certificate shall be inserted in the card before distribution to the user.

4.1.5.5 Quality Control

[r4.80] Documented routines shall exist to ensure that the visual information on users' cards and the electronic information in issued cards and certificates matches each other and also matches the validated owner. The routines shall be described in the personalization PS.

4.1.5.6 Cancellation (destruction) of non-distributed cards

[r4.85] All cards that are damaged or destroyed (or for other reasons are not finalized and distributed) during personalization shall be physically and electronically destroyed (cancelled).

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

[r4.95] The I-CP is responsible for keeping track of which card and card number is given to which user. Data shall be transferred from the I-CP to the I-CIA register.

4.1.7 Card distribution to the user – handled by the CP or CIA

[r4.100]

a) The personalization shall be scheduled so as to minimize the time that the personalized card require safe-keeping before delivery to the user. Documented routines shall exist for exception handling,

including disturbances in the production process, failure of delivery, and loss of or damage to cards.
b) Personalized cards shall be transferred to the place where they are to be delivered or distributed to the user, i.e. a controlled area, without significant delay
c) Personalized cards shall always be kept separated from non-personalized cards.
d) The Tachograph card shall be distributed in such a manner as to minimize the risk of loss.
e) At some stage of the card issuing process, evidence of the user's identity (e.g. name) shall be checked against a physical person.
f) The user shall present valid means of identification.

4.1.8 Authentication codes (PIN) – generated by the CP

This section applies only to Workshop cards.

[r4.105] Workshop cards shall have a PIN code, used for authenticating the card to the Vehicle unit (Regulation Annex 1B, App 10: Tachograph cards: 4.2.2).

[r4.110] PIN codes shall consist of at least 4 digits (Regulation Annex 1B, App 10: Vehicle Units:4.1.2).

4.1.8.1 PIN generation

[r4.115] PIN codes shall be generated in a secure system, securely transferred to workshop cards, and direct-printed to PIN-envelopes. The PIN generation system shall meet the requirements of ITSEC E3, CC EAL4 or equivalent security criteria.

4.1.8.2 PIN distribution

[r4.120] PIN codes may be distributed by regular mail.

[r4.125] PIN codes shall not be distributed in connection with the corresponding cards.

4.2 Vehicle Units and Motion Sensors

The issuing of certificates, symmetric keys and encrypted motion sensor data to type approved VUs and Motion Sensors is out of the scope of this Policy.

5 Key management

This section contains provisions for the management of

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

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

The **Member State keys** are the Member State signing keys.

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

The **Transport keys** are the keys used for securely exchanging information between the ERCA and the CA.

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

[r5.01] The I-CA shall use the physical media described in Annex C of the ERCA Policy to transport I-CA certification requests, MSCA certificates, the ERCA public key, and the motion sensor master keys.

5.1 ERCA public key

[r5.05] The I-CA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times.

[r5.06] The I-CA shall recognize the ERCA public key (EUR.PK) in the distribution format described in Annex B of the ERCA Policy.

[r5.10] The I-CP shall ensure that EUR.PK is inserted in all Tachograph cards.

5.2 Member State keys

The I-CA key pair consists of a public key (MS.PK) and a private, or secret, key (MS.SK).

The I-CA public key is certified by the ERCA, but is always generated by the I-CA itself.

When a cooperation administrative arrangement exists between Italy and another State, the I_CA is authorized to use the Italian national keys to produce public key certificates for all tachograph cards issued by the CIA of this State, following the key-sharing scheme.

[r5.15] The I-CA shall ensure that MS keys will not be used for any other purposes than signing Tachograph equipment certificates and for production of the ERCA key certification request.

[r5.16] MS.PK shall be submitted to ERCA using the key certification request (KCR) protocol described in Annex A of the ERCA Policy.

5.2.1 Member State keys generation

[r5.20] Member State key pair generation shall be carried out within a device which either:

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

[r5.25] The actual device used and requirements met shall be stated in the I-CA PS.

[r5.30] I-CA key-pair generation shall require the active participation of two separate individuals. At least one of these shall have a role of CAA.

[r5.35] Keys shall be generated using the RSA algorithm with a key length of modulus conforming the Commission Regulation 1360/2002.

[r5.36] The I-CA shall ensure that the Key Identifier (KID) and modulus (*n*) of keys submitted to the ERCA for certification are unique within the domain of the CA.

[r5.40] The I-CA shall have more than one Member State key pair with associated signing certificates to ensure continuity, since the ERCA cannot issue replacement Member State certificates rapidly.

5.2.2 Member State keys' period of validity

[r5.45] The Member State private keys usage period is **2** years from the date of issuance of the corresponding public key certificate. The Member State private keys shall be destroyed after their expiry date.

[r5.50] The corresponding public key shall have no end of validity.

[r5.51] The I-CA shall generate different Member State key pairs, and shall request the corresponding MS certificates to the ERCA, for each of the four type of the Tachograph cards.

[r5.52] Because of the expected lifetime of the Driver, Company, and Control cards of a maximum of 5 years, Member State certificates, for the corresponding cards and for the Workshop card, shall have a validity of 7 years.

5.2.3 Member State private key storage

[r5.55] The private keys shall be contained in and operated from inside a specific tamper resistant device which:

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

[r5.60] For access to the I-CA private signing keys, dual control is required. This means that no single person will possess the means required to access the environment where the private key is stored.

5.2.4 Member State private key backup

[r5.65] The Member State private signing keys may be backed up, using a key recovery procedure requiring at least dual control. The procedure used shall be stated in the I-CA PS. However, if key pairs are used according to §5.2.1, no backup is needed.

5.2.5 Member State private key escrow

[r5.70] The Member State private signing keys shall not be escrowed.

5.2.6 Member State keys compromise

[r5.75] A written instruction shall exist, included in the I-CA PS, which states the measures to be taken by users and security responsible persons at the I-CA and/or Service Agencies if the Member State private keys has become exposed, or is otherwise considered or suspected to be compromised.

[r5.80] In such case the I-CA shall as a minimum inform without delay the I-MSA , the ERCA and the MSAs/CPAs eventually supported if a cooperation administrative arrangement between countries is in place (section 2.1.2).

5.2.7 Member State keys end of life

[r5.85] The I-CA shall have routines to ensure the permanent existence of a valid, certified Member State signing key pair.

[r5.90] Upon termination of use of a Member State signing key pair, the public key shall be archived, and the private key shall be destroyed such that it cannot be retrieved.

5.3 Motion Sensor keys

[r5.95] The I-CA shall, as needed, request motion sensor key Km_{WC} from the ERCA according to the key distribution request (KDR) protocol described in Annex D 1.5 of ERCA Policy.

[r5.100] The I-CA shall forward the workshop key ($Km_{WC)}$ to the I-CP for the sole purpose of insertion into the Workshop cards.

[r5.105] The I-CP shall undertake the I-CA's task to ensure that the workshop key KmWC is inserted into all issued Workshop cards.

[r5.110] The I-CA and/or I-CP shall, during storage, use and distribution, protect the motion sensor keys with high assurance physical and logical security controls. The keys shall be contained in and operated from a specific tamper resistant device which:

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

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

5.4 Transport keys

[r5.115] For secure data communication the I-CA issues special, asymmetric, transport key pairs. The I-CA shall protect these keys with high assurance physical and logical security controls. The keys should be contained in and operated from a specific tamper resistant device which:

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

[r5.116] The I-CA shall ensure that the Key Identifier (KID) and modulus (*n*) of the transport keys submitted to the ERCA for motion sensor key distribution are unique within the domain of the CA.

6 Equipment keys

Equipment keys are asymmetric keys generated somewhere in the issuing/manufacturing process, and certified by the I-CA for the equipment (Card) in the Tachograph system.

6.1 General aspects

[r6.05] 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. A log shall be kept of the entries and the actions in the system.

[r6.10] No sensitive information contained in the key generation systems may leave the system in a way that violates this Policy.

[r6.15] No sensitive information in the card personalization system may leave the system in a way that violates this Policy.

[r6.20] Organizations that perform card personalization on behalf of more than one Member State shall do this in a clearly separate process for each of these.

6.2 Equipment key generation

[r6.30] The entity that performs the key generation shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

[r6.35] Key generation shall be carried out within a device which either:

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

- meets the requirements identified in CEN Workshop Agreement 14167-2 [CEN]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria.

[r6.40] Keys shall be generated using the RSA algorithm having a key length of modulus conforming the Commission Regulation 1360/2002.

[r6.45] 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 after having been inserted in the device.

[r6.50] It is the responsibility of the I-CA to undertake adequate measures to ensure that the public key is unique within its domain before certificate binding takes place.

6.2.1 Equipment key validity

[r6.55] Usage of an equipment private key in connection with certificates issued under this Policy shall never exceed the end of validity of the certificate.

6.2.2 Equipment private key protection and storage

[r6.60] The I-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.

[r6.65] Copies of the private key are not to be kept anywhere except in the Tachograph card, unless required during key generation and device personalization.

6.2.3 Equipment private key escrow and archival

[r6.75] Equipment private keys shall be neither escrowed nor archived.

6.2.4 Equipment public key archival

[r6.80] All certified public keys shall be archived by the certifying I-CA.

6.2.5 Equipment keys end of life

Upon termination of use of a Tachograph card, no key archival is foreseen.

7 Equipment certificate management

7.1 Data input

7.1.1 Tachograph cards

Cardholding users do not apply for certificates, their certificates are issued based on the information given in the application for a Tachograph card (section 4.1.2) and captured from the I-CIA register. The public key to be certified is extracted from the key generation process.

[r7.05] The I-CP shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique.

[r7.06] The I-CA shall verify the uniqueness of the CHR within its domain.

[r7.07] The certificate request process shall ensure that the I-CP has possession of the private key associated with the public key presented for certification.

7.2 Tachograph card certificates

7.2.1 Driver certificates

[r7.10] Driver certificates are issued only to successful applicants for a Driver card.

7.2.2 Workshop certificates

[r7.15] Workshop certificates are issued only to successful applicants for a Workshop card.

7.2.3 Control body certificates

[r7.20] Control body certificates are issued only to successful applicants for a Control body card.

7.2.4 Hauling company certificates

[r7.25] Hauling company certificates are issued only to successful applicants for a Hauling Company card.

7.3 Vehicle unit certificates

[r7.30] Vehicle unit certificates are out of the scope of this Policy (section 4.2).

7.4 Equipment certificate time of validity

[r7.35] Certificates shall not be valid longer than the corresponding equipment:

- Driver certificates shall not be valid for more than **5** years.
- Workshop certificates shall not be valid for more than **1** year.
- Control body certificates shall not be valid for more than **5** years.
- Hauling company certificates shall not be valid for more than **5** years.

7.5 Equipment certificate issuing

[r7.40] The I-CA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by the Commission Regulation 1360/2002..

[r7.41] The I-CA shall sign equipment certificates within the same device used to store the MS Private keys.

7.6 Equipment certificate renewal and update

See Equipment management (section 4). Since certificates and cards have the same time of validity, they are dealt with together. Renewal and update affects solely equipment; certificates are never renewed or updated.

7.7 Dissemination of information

[r7.45] The I-CA shall export all certificate data to the I-CIA register so that certificates, equipment and users are linked together.

[r7.55] The I-CIA shall ensure that all terms and conditions and other relevant information, are made readily available to all users, relying parties and other relevant groups (section 4.1.2).

[r7.56] The I-CIA shall maintain and make certificate status information available.

7.8 Equipment certificate use

[r7.60] The tachograph certificates are only for use within the Tachograph system.

7.9 Equipment certificate revocation

[r7.65] Certificates are not revoked. Non-valid Tachograph equipment are put on a "black list".

8 CA and CP Information Security management

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

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

8.1 Information security management of the CA and CP

[r8.05] The I-CA/I-CP shall ensure that administrative and management procedures applied are adequate and correspond to recognized standards.

[r8.10] The I-CA/I-CP retains 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 I-CA/I-CP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the I-CA/I-CP.

[r8.15] The information security infrastructure necessary to manage the security within the I-CA/I-CP shall be maintained at all times. Any changes that will impact on the level of security provided will be approved by the I-MSA.

[r8.20] The I-CA/I-CP shall adopt a security management system. Formal certification is not required.

8.2 Asset classification and management of the CA/CP

[r8.25] The I-CA/I-CP shall ensure that its assets and information receive an appropriate level of protection. In particular The I-CA/I-CP shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with this Policy.

8.3 Personnel security controls of the CA/CP

8.3.1 Trusted Roles

[r8.30] A CA/CP, supporting this I-MSA Policy , should recognize distinct roles. Different arrangements of separation of duties may be acceptable, provided the resilience to insider attack is at least as strong as with the recommended model and provided the roles are described in the I-CA/I-CP PS.

[r8.35] To ensure that one person acting alone cannot circumvent safeguards, responsibilities in I-CA/I-CP systems need to be attended by multiple roles and individuals. Each account on the systems shall have limited capabilities, commensurate with the role of the account holder.

[r8.40] The recommended roles are:

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

The ISSO, not directly involved in issuing certificates, performs a supervisory function in examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security Policy.

8.3.2 Separation of roles

[r8.60] For the I-CA/I-CP, different individuals shall fill each of the three roles described above and at least one individual shall be appointed per task.

8.3.3 Identification and Authentication for Each Role

[r8.65] Identification and authentication of CAA/PA, SA and ISSO shall be appropriate and consistent with practices, procedures and conditions stated in this Policy.

8.3.4 Background, qualifications, experience, and clearance requirements

[r8.70] The individual assuming the CAA/PA role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

[r8.75] All I-CA/I-CP personnel in sensitive positions, including, at least, all CAA/PA and ISSO (Information System Security Officer) positions, shall:

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

[r8.80] The I-CA/I-CP personnel in trusted roles, as detailed in the PS, shall have an appropriate background screening, with positive results.

8.3.5 Training requirements

[r8.85] Personnel shall have adequate training for the role and job.

8.4 System security controls of the CA and personalization systems

[r8.90] The I-CA/I-CP shall ensure that the systems are secure and correctly operated, with minimal risk of failure.

In particular:

a) the integrity of systems and information shall be protected against viruses, malicious and unauthorized software;

b) damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures;

[r8.95] The Certification Authority System and Personalization system shall provide sufficient system security controls for enforcing the separation of roles described in this Policy or the relevant PS.

[r8.100] The security controls shall provide access control and traceability down to an individual level on all transactions and functions affecting the use of I-CA's private issuing keys.

[r8.105] System security controls imposed on computer systems used by Service Agencies depend on the role assigned to the agency. Agencies that undertake CAA/PA roles, load certificates onto cards, or initialize such cards, shall meet the requirements imposed upon I-CA/I-CPs.

8.4.1 Specific computer security technical requirements

[r8.110] Initialization of the sub-system operating I-CA's private certification keys shall require co-operation of at least two operators, both of which are securely authenticated by the system.

8.4.2 Computer security rating

[r8.115] The CA and personalization systems do not require formal rating as long as they fulfill all requirements in this section.

8.4.3 System development controls

[r8.120] The I-CA/I-CP shall use trustworthy systems and products that are protected against modification.

[r8.125] An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the I-CA/I-CP or on behalf of the I-CA/I-CP to ensure that security is built into IT systems.

[r8.130] Change control procedures shall exist for releases, modifications and emergency software fixes for any operational software.

8.4.4 Security management controls

[r8.135] The system roles (section 8.3.1) shall be implemented and enforced.

8.4.5 Network security controls

[r8.140] Controls (e.g., firewalls) shall be implemented to protect the I-CA/I-CP's internal network domains from external network domains accessible by third parties.

[r8.145] Sensitive data shall be protected when exchanged over networks which are not secure.

8.5 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.

8.5.1 Types of event recorded

[r8.150] The security audit functions related to the I-CA/I-CP computer/system shall log, for audit purposes:

- The creation of I-CA accounts (privileged or not).
- 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.
- Time and date and other descriptive information about all backups.

8.5.2 Frequency of processing audit log

[r8.155] The log shall be processed regularly and analyzed against malicious behavior. Log procedures will be described in the PS.

8.5.3 Retention period for audit log

[r8.160] Audit log shall be retained for at least **2** years.

8.5.4 Protection of audit log

[r8.165] Integrity of the audit logs shall be appropriately protected. All entries shall be individually time stamped.

[r8.170] Audit logs shall be verified and consolidated at least monthly. At least dual control is required.

8.5.5 Audit log backup procedures

[r8.180] The audit log shall be stored in a way that makes it possible to examine the log during its retention period.

[r8.185] The audit log shall be protected from unauthorized access.

8.6 Record archiving

8.6.1 Types of event recorded by the CIA

[r8.190] The records shall include all relevant evidence in the I-CIA's possession including, but not limited to:

- Certificate requests.
- Signed registration agreements from user's applications for certificates and cards, including the identity of the person responsible for accepting the application.
- Contractual agreements regarding certificates and associated cards.
- Currently and previously implemented Policy documents.

8.6.2 Types of event recorded by the CA/CP

[r8.195] The records shall include all relevant evidence in the I-CA/I-CP's possession including, but not limited to:

- Contents of issued certificates (I-CA).
- Audit journals including records of annual auditing of I-CA/I-CP's compliance with its PS.
- Currently and previously implemented certificate Policy documents and their related PSs.

[r8.200] Records of all digitally signed electronic requests made by I-CA/I-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.

8.6.3 Retention period for archive

[r8.205] Archives shall be retained and protected against modification or destruction for a period as specified in the PS.

8.6.4 Procedures to obtain and verify archive information

[r8.210] The I-CA/I-CP shall act in compliance with requirements regarding confidentiality as stated in section 2.4.

[r8.215] Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.

[r8.220] I-CA/I-CP shall make available on request, produced documentation of the I-CA/I-CP's compliance with the applicable PS according to section 10.5.

[r8.225] Subject to statute, a reasonable handling fee may be charged to cover the cost of record retrieval.

[r8.230] The I-CA/I-CP shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the I-CA/I-CP's operations are interrupted, suspended or terminated.

[r8.235] In the event that I-CA/I-CP services are to be interrupted, suspended or terminated, the I-CA/I-CP shall ensure the continued availability of the archive. All requests for access to archived information will be sent to the I-CA/I-CP or to the entity identified by the I-CA/I-CP prior to terminating its service.

8.7 CA/CP continuity planning

[r8.240] I-CA/I-CP shall have a business continuity plan (BCP) which do not depend 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.

[r8.241] Backups shall be performed at least once per week.

8.7.1 Member State keys compromise

Member State keys compromise is dealt with in section 5.

8.7.2 Other disaster recovery

[r8.245] I-CA/I-CP and subcontractors shall have routines established to prevent and minimize the effects of system disasters. These routines include secure and remote backup data storage.

8.8 Physical security control of the CA and personalization systems

[r8.250] Physical security controls shall be implemented to control access to the I-CA or I-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).

[r8.255] The Member state keys for signing certificates shall be kept physically and logically protected as described in the PS.

[r8.260] The I-CA/I-CP's facility shall also have a place to store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information. Backups shall be kept both for data recovery and for the archival of important information.

[r8.261] Backup media shall also be stored at a site different from where the I-CA/I-CP system resides, to permit restoration in the event of a natural disaster to the primary facility.

8.8.1 Physical access

[r8.270] Access to the physical area housing the I-CA keys and the means for their usage, shall be limited to the persons which have been individually appointed the right to enter the area.

[r8.275] Access may be controlled through the use of an access control list to the room housing the systems. Anyone not on the access control list shall be escorted by a person on the list. If an access control list is not feasible for a particular site, it may be acceptable to make sure that the CA and personalization related material is locked in a secure room or storage area when it is not being used.

9 CA or CP Termination

9.1 Final termination - MSA responsibility

Final termination of I-CA or I-CP is regarded as the situation where all service associated with a logical entity is terminated permanently. I-CA/I-CP termination implies either that a Member State withdraws from the Tachograph system or termination of the entire Tachograph system, since this cannot function without CAs, or equivalent authorities.

[r9.05] The I-MSA will ensure that the tasks outlined below are carried out.

[r9.10] Before the I-CA/I-CP terminates its services the following procedures has to be completed as a minimum:

- Inform all users and parties with whom the I-CA/I-CP has agreements or other form of established relations.
- Make publicly available information of its termination at least **3** month prior to termination.
- The I-CA/I-CP will terminate all authorization of subcontractors to act on behalf of the I-CA/I-CP in the process of issuing certificates.
- The I-CA/I-CP shall perform necessary undertakings to transfer obligation for maintaining event log archives for the remaining period of their life cycle.

9.2 Transfer of CA or CP responsibility

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

[r9.15] The I-MSA will ensure that orderly transfer of responsibilities and assets is carried out.

[r9.20] The old I-CA shall transfer all root keys to the new I-CA in the manner decided by the I-MSA .

[r9.25] The old I-CA shall destroy any copies of keys that are not transferred.

10 Audit

[r10.05] The I-MSA is responsible for ensuring that audits of the I-CA and I-CP take place.

10.1 Frequency of entity compliance audit

[r10.10] The I-CA/I-CP operating under this RSM-CPA Policy will be audited within 12 months of the start of the operations covered by this policy; the next audit may be performed within 24 months in case of absence of non –conformity evidence.

10.2 Topics covered by audit

[r10.15] The audit will cover the I-CA/I-CP´s practices.

[r10.20] The audit will cover the I-CA/I-CP´s compliance with this I-MSA Policy.

[r10.25] The audit will also consider the operations of any Service Agencies.

10.3 Who should do the audit

[r10.30] The I-MSA may consult an external certification or accreditation organization for approval of the I-CA/I-CP PS. Otherwise the I-MSA will undertake the auditing.

10.4 Actions taken as a result of deficiency

[r10.35] If irregularities are found in the audit the I-MSA will take appropriate action depending on severity.

10.5 Communication of results

[r10.40] Results of the audits on a security status level will be reported in English language to the ERCA. The evaluation will define corrective actions, including an implementation schedule.

11 Italian Tachograph MSA Policy change procedures

11.1 Items that may change without notification

[r11.05] The only changes to this specification not needing any notification are:

- Editorial or typographical corrections;
- Changes to the contact details.

11.2 Changes with notification

11.2.1 Notice

[r11.10] Any item in this certificate Policy may be changed with **90** days notice.

[r11.15] Changes to items which, in the judgment of the Policy responsible organization (the I-MSA), will not materially impact a substantial majority of the users or relying parties using this Policy may be changed with **30** days notice.

11.2.2 Comment period

[r11.20] Impacted users may file comments with the Policy administration organization within **15** days of original notice.

11.2.3 Whom to inform

[r11.25] Information about changes to this Policy will be sent to:

- ERCA
- I-CA and I-CP including Service Agencies
- I-CIA
- MSAs / CPAs eventually supported if a cooperation administrative arrangement between countries is in place (section 2.1.2)

11.2.4 Period for final change notice

[r11.30] If the proposed change is modified as a result of comments, notice of the modified proposed change will be given at least **30** days prior to the change taking effect.

11.3 Changes requiring a new Italian Tachograph MSA Policy approval

[r11.35] If a Policy change is determined by the I-MSA organization to have a material impact on a significant number of users of the Policy, the I-MSA will submit the revised I-MSA Policy to the Commission for approval.

12 Conformity to the ERCA Policy

The following table provides a rationale addressing each requirement as formulated in ERCA Policy – Section 5.3

Item	Reference ERCA Policy	Requirement	Reference MSA Policy
1	5.3.1	The MSA policy shall identify the entities in charge of operations.	§0.1
2	5.3.2	The Member State 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 [9]; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10]; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; 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.	§ 5.2 [r5.20] [r5.55] [r5.115]
3	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.	§5.2.1 [r5.30] §8.8 [r8.250, [r8.275]
4	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.	§5.2.2 [r5.45]
5	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 (see Section 4.2.5).	§5.2.1 [r5.40]
6	5.3.6	The MSA shall submit CA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.	§5.2 [r5.16]
7	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.	§5.3 [r5.95]
8	5.3.8	The MSA shall recognize the ERCA public key in the distribution format described in Annex B.	§5 [r5.06]

13 References

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. (provisional), property of 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)

[ERCA Policy] Digital Tachograph System European Root Policy, Version 2.1; JRC Technical Note No. JRC 53429, published at http://dtc.jrc.ec.europa.eu/

[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)

[CSG] Common Security Guideline, Card Issuing Project (provisional), property of the Commission

14 Glossary/Definitions and abbreviations

14.1 Glossary/Definitions

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

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

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

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

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

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual CA Policy. The CPS is in this I-MSA Policy replaced by a Practice Statement, because it has a broader view and connects to keys, certificates and equipment.
Equipment: In the Tachograph system the following equipment exists: Tachograph cards, VU (vehicle units) and Motion Sensors.
Key sharing: the method by which the CA of country A uses its national root keys to issue certificates upon Country B certification requests.
Manufacturer/Equipment manufacturer: Manufacturers of Tachograph equipment. In this Policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.
Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.
Practice Statement (PS). A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.
Private key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages. Also called Secret key.
Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.
Service Agency: An entity that undertakes to tasks on behalf of an CA, 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 will be uniquely identifiable entities.

In this document:
Signed: Where this Policy requires a signature, the requirement is met by a secure and verifiable digital signature.
Written: Where this Policy requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for the parties concerned.

14.2 List of abbreviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/ Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority

CC	Common Criteria
CP	Card Personalizing organization
CPA	Competent Party Authority
CPS	Certification Practice Statement
ERCA	European Root CA
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
KG	Key Generation
MS	Member State
MSA	Member State Authority
CA	Member State Certification Authority
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