Digital Tachograph System

Romanian CA Policy

Version 1.7

Revision 02.05.2007

INDEX

1 Introduction

This document is the **Romanian** National Certification Authority policy for the Digital Tachograph System. This National Certification Authority Policy (**NCA policy**) is in accordance with:

- COUNCIL REGULATION (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/84 and (EEC) No 3821/85
- Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport
- the "Guideline and Template National Certification Authority policy" – Version 1.0
- the "Common Security Guidelines" – Version 1.0
- Digital Tachograph System European Root Policy, Version 2.0; European Commission Special Publication I.04.131; published at http://dtc.jrc.it

1.1 Responsible organization

Responsible for this NCA policy is the Ministry of Transports, Constructions and Tourism (MTCT) as Member State Authority (**MSA**), further referred to as **RO-A**[1].

The appointed Card Issuing Authority (**CIA**) is the Romanian Road Transport Authority – ARR, further referred to as **RO-CIA**[2]**.**

The appointed Certification Authority (**CA**) is the Romanian Road Transport Authority - ARR, further referred to as **RO-CA**[3]**.**

The appointed Card Personalizing organization (**CP**) is the Romanian Road Transport Authority - ARR, further referred to as **RO-CP**[4].

The Romanian Road Transport Authority - ARR may subcontract parts of its processes as RO-CA or RO-CP to subcontractors, called Service Agencies. The use of Service Agencies in no way diminishes its overall responsibilities as RO-CA and RO-CP.

The appointed service agency for RO-CA and RO-CP is:

SC CERTSIGN SRL
Calea Serban Voda Nr. 133
Central Business Park
Corp C, et. 2
Sector 4, Bucharest
Romania

[1] **RO-A** - Romanian Authority
[2] **RO-CIA** - Romanian Card Issuing Authority
[3] **RO-CA** - Romanian Certification Authority
[4] **RO-CP** - Romanian Card Personalizing organization

1.2 Approval

This NCA policy is approved for the European Commission by the Digital Tachograph Root Certification Authority at … …… 2007.

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)

1.3 Availability and contact details

The NCA policy is publicly available at www.arr.ro .
Questions concerning this NCA policy should be addressed to:

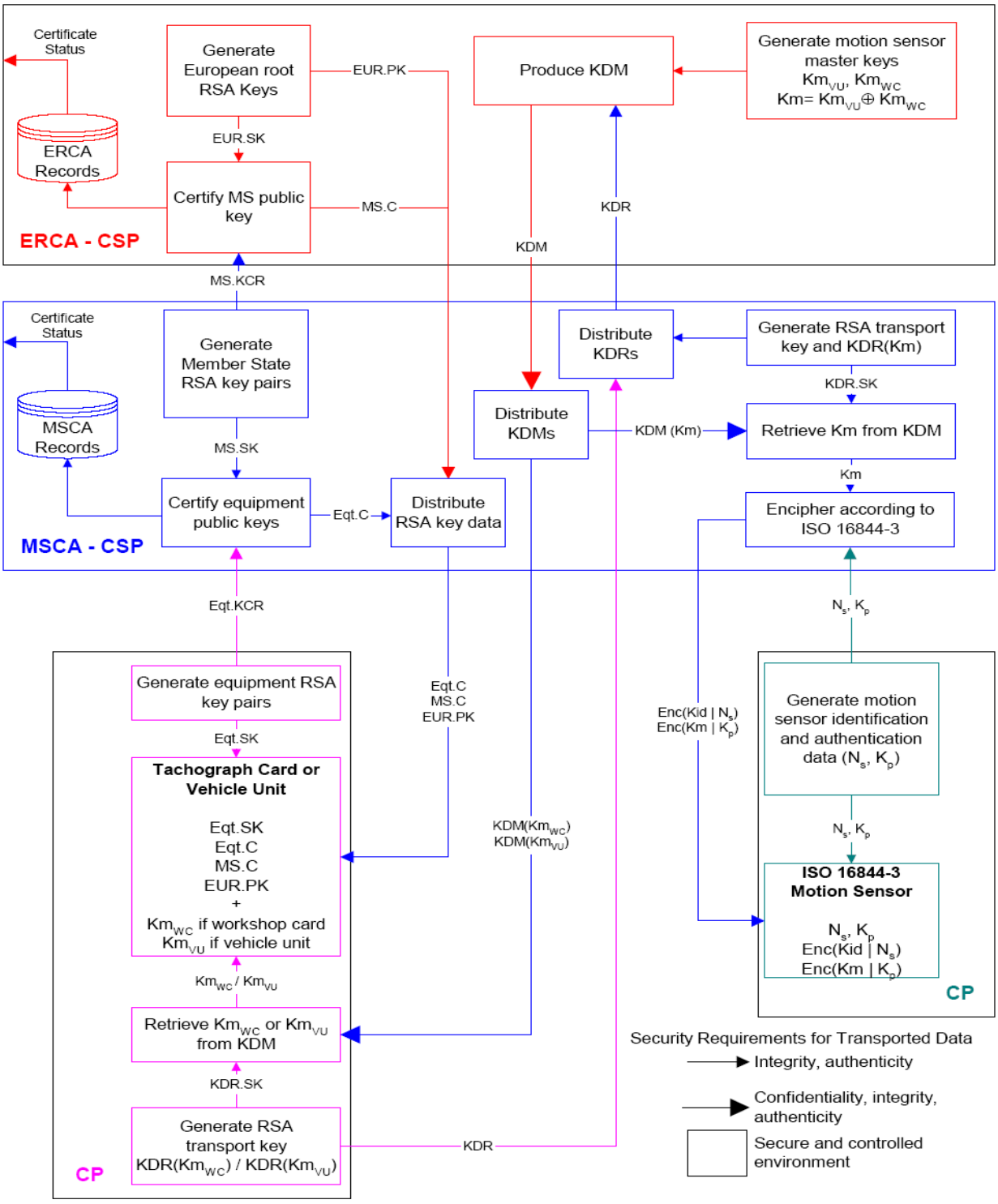
Romanian Road Transport Authority – ARR
No.38, Dinicu Golescu Avenue, Sector 1
Bucharest
Romania

2 Scope and applicability

[r1] The NCA policy is valid for the Tachograph system only.

[r2] The keys and certificates issued by the RO-CA are only for use within the Tachograph system.

[r3] The cards issued by the system are only for use within the Tachograph system.
The scope of the NCA policy within the Tachograph system is shown in the figure below.



3 General provisions

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

3.1 Obligations

This section contains provisions relating to the respective obligations of:

- RO-A and RO-CIA
- RO-CA and Service Agency (if any)
- RO-CP and Service Agency (if any)
- Users (Cardholders, VU manufacturers and Motion Sensor manufacturers)

3.1.1 RO-A and RO-CIA obligations

With regard to this NCA policy, the RO-A and RO-CIA have the following obligations.

[r4] The RO-A shall:

a) Maintain the NCA policy
b) Appoint an RO-CA and a RO-CP
c) Audit the appointed RO-CA and RO-CP including Service Agencies
d) Approve the RO-CA/RO-CP PS
e) inform the appointed parties about this policy
f) let this policy be approved by the **Commission**

[r5] The RO-CIA shall:

a) Ensure that correct and relevant user information from the application process is input to the RO-CA and RO-CP
b) inform the **users** of the requirements in this policy connected to the use of the system, i.e the Cardholders, the VU manufacturers and the Motion Sensor manufacturers

3.1.2 RO-CA obligations

[r6] The appointed RO-CA shall:

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

[r7] The RO-CA shall ensure that all requirements on RO-CA, as detailed in this policy, are implemented.

[r8] The RO-CA has the responsibility for conformance with the procedures prescribed in this policy, even when the RO-CA functionality is undertaken by subcontractors, Service Agencies. The RO-CA is responsible for ensuring that any Service Agency provides all its services consistent with its Practice Statement (PS) and the NCA policy.

3.1.3 RO-CP obligations

[r9] The appointed RO-CP (card personalization organization) has to:

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

[r10] The RO-CP shall ensure that all requirements on it, as detailed in this policy, are implemented.

[r11] The RO-CP has the responsibility for conformance with the procedures prescribed in this policy, even when the RO-CP functionality is undertaken by subcontractors, Service Agencies.

3.1.4 Service Agency obligations

[r12] Service Agencies (if applicable) have obligations towards the RO-CA or RO-CP and the users according to contractual agreements.

3.1.5 Cardholder obligations

[r13] The RO-CIA shall oblige, through agreement (see 5.1.2), the user (or user's organization) to fulfill the following obligations:

a) accurate and complete information is submitted to the RO-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 (Regulation14.4.a);
f) a user may have only one valid driver card (Regulation14.4.a);
g) a user may only under very special, and duly justified, circumstances have both a workshop card and a hauling company card (Annex 1B VI:1), or both a workshop card and a driver card, or several workshop cards
h) the user shall not use a damaged or expired card (Regulation14.4.a);
i) the user shall notify the RO-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 (Regulation15.1); or
   - the certificate content is, or becomes, inaccurate.

3.1.6 VU manufacturers' obligations (role as personalization organization)

Not applicable in Romania for the time being or in the foreseeable future.

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

Not applicable in Romania for the time being or in the foreseeable future.

3.2 Liability

The RO-CA and RO-CP do not carry liability towards end users, only towards the RO-A and RO-CIA. Any liability issues towards end users are the responsibility of the RO-A/RO-CIA.

[r16] Tachograph cards, keys and certificates are only for use within the Tachograph system, any other certificates present on Tachograph cards are in violation of this policy, and hence neither the RO-A, the RO-CIA, the RO-CA nor the RO-CP carries any liability in respect to any such.

3.2.1 RO-A and RO-CIA liability towards users and relying parties

[r17] The RO-A and RO-CIA are liable for damages resulting from failures to fulfill their obligations only if they have acted negligently. If the RO-A or RO-CIA has acted according to this NCA policy, and any other governing document, it shall not be considered to have been negligent.

3.2.2 RO-CA and RO-CP liability towards the RO-A and RO-CIA

[r18] The RO-CP and RO-CA are liable for damages resulting from failures to fulfill these obligations only if they have acted negligently. If the organization has acted according to this NCA policy and the corresponding PS or any other governing document, it shall not be considered to have been negligent.

3.3 Interpretation and enforcement

3.3.1 Governing law

All matters related to the implementation and enforcement on the Digital Tachograph System in Romania will be resolved according to the Romanian national legislation in force.

3.4 Confidentiality

Confidentiality is restricted according to the provisions of Law no. 677 / 21 November 2001 on the protection of individuals with regard to the processing of personal data and on the movement of such data.

3.4.1 Types of information to be kept confidential

[r19] Any personal or corporate information held by the RO-CA, the RO-CP or Service Agencies that is not appearing on issued cards or certificates is considered confidential, and shall not be released without the prior consent of the user, nor (where applicable) without prior consent of the user's employer or representative, unless required otherwise by law.

[r20] All private and secret keys used and handled within the RO-CA/RO-CP operation under this NCA policy are to be kept confidential.

[r23] Audit logs and records shall not be made available as a whole, except as required by law.

3.4.2 Types of information not considered confidential

[r24] Certificates are not considered confidential.

[r25] 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)

[r26] The RO-CA and RO-CP shall have statements of the practices and procedures used to address all the requirements identified in the NCA policy, Practice Statements (PS). The RO-A shall approve the PS. In particular:

a) The PS shall identify the obligations of all external organizations supporting the RO-CA and RO-CP services including the applicable policies and practices.
b) The Practice statement shall be made available to the RO-A, to users of the Tachograph system, and to relying parties (e.g. control bodies). However, the RO-CA/RO-CP is not generally required to make all the details of its practices public and available for the users.
c) The management of the RO-CA/RO-CP has responsibility for ensuring that the PS is properly implemented
d) The RO-CA/RO-CP shall define a review process for the PS.
e) The RO-CA/RO-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 RO-A approval.

5 Equipment management

The equipment in the Tachograph system is defined as:
- Tachograph cards
- Vehicle units
- Motion Sensors

The equipment is handled and managed by several roles:
- RO-CIA (registration, renewal, etc.)
- RO-CA (certificates, keys)
- RO-CP (visual and electronic personalization, distribution, deactivation)
- VU manufacturers and Motion Sensor manufacturers

The following functions are carried out by the RO-A:
- Quality control (type approval)

The following functions are carried out by the RO-CIA:
- Applications for cards
- Application approval registration
- Equipment registration and data storage (DB)

The following functions are carried out by the RO-CA and RO-CP:
- Quality control (sample tests)
- Key insertion
- Personalization of cards
- Distribution

The functions carried out by the VU manufacturers are out of the scope of this Policy.
The functions carried out by Motion Sensor manufacturers are out of the scope of this Policy.

5.1 Tachograph cards

5.1.1 Quality control – RO-CA/RO-CP function

[r27] The RO-CA/RO-CP shall ensure that only type approved cards according to the Regulation are personalized in the Tachograph system. See also 5.1.7.5

5.1.2 Application for card – handled by the RO-CIA

[r28] The RO-CIA shall inform the user of the terms and conditions regarding use of the card. This information shall be available in a readily understandable language.

[Practice] It is recommended that the information is available in at least both the national language(s) of the member state and in English.

[r29] The user shall, by applying for a card, and accepting delivery of the card, accept the terms and conditions.

5.1.2.1 User application

[r30] Applicants for a Tachograph card shall deliver an application in a form to be determined by the RO-A or RO-CIA. As a minimum, the application shall include the data needed to ensure the correct identification of the user.

The following information is required for issuing a card. Unless gathered from other sources, it should be included in the application:

- Full name
- Date and place of birth
- Place of residence
- Personal National Number (*CNP – Cod numeric personal*)
- Postal address
- Photo (unless a valid filed photo is used) (Optional except for driver cards)
- Preferred language

Driver card specific:

- Driving license number

Workshop card specific:

[r31] Workshop cards shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

- full name (including surname and given names) of the user;
- date and place of birth, reference to a nationally recognized identity document, or other attributes of the user which may be used to, as far as possible, distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organizational entity;

Control body card specific:

[r32] Control body certificates shall be issued only to physical persons associated with legal persons, and who can provide the following evidence:

- full name (including surname and given names) of the user;
- date and place of birth, reference to a nationally recognized identity document, or other attributes of the user which may be used to, as far as possible, distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organizational entity;

Hauling company card specific:

[r33] Hauling company certificates shall be issued to individual representatives of companies owning or holding vehicles fitted with digital Tachograph and who can provide evidence of:

- full name (including surname and given names) of the user;
- date and place of birth, reference to a nationally recognized identity document, or other attributes of the user which may be used to, as far as possible, distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organizational entity;
- any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;
- the user's association with the legal person or other organizational entity.

5.1.2.2 Agreement

[r34] The applicant shall, by making an application for a card and accepting delivery of the card, make an agreement with the RO-CIA, stating as a minimum the following:

- the user agrees to the terms and conditions regarding use and handling of the Tachograph card

- the user agrees to, and certifies, that from the time of card acceptance and throughout the operational period of the card, until RO-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 RO-CIA relevant for the information in the card is true;
    - the card is being conscientiously used in consistence with usage restrictions for the card

5.1.2.3 RO-CIA terms of approval - Driver card specific
[r35] A Driver card shall only be issued to individuals having permanent residence in the country of application.

[r36] The RO-CIA shall ensure that the applicant does not have a valid Driver card issued in another Member State.

[r37] The RO-CIA shall ensure that the applicant for a Driver card has a valid driving license of appropriate class.

5.1.3 Card renewal – handled by the RO-CIA

[r38] Workshop cards shall be valid for no more than **one** year from issuance (Regulation 12.1).

[r39] Driver cards shall be valid no more than **five** years from issuance (Regulation 14.4.a).

[r40] Company cards shall be valid no more than **five** years from issuance.

[r41] Control cards shall be valid no more than **two** years from issuance.

[r42] The RO-CIA shall establish routines to remind the user of pending expiration.

[r43] An application for renewal shall follow section 5.1.2

5.1.3.1 Driver cards
[r44] The user shall apply for a renewal card at least **15** days prior to card expiration. (Regulation article 15.1)

[r45] If the user complies with the above rule, the RO-CIA shall issue a new driver card before the current card expires. (Regulation article 14.4.a)

5.1.3.2 Workshop cards
[r46] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r47] The RO-CIA shall issue a renewal card within **5** working days of receiving a complete application. (Regulation article 12.1)

5.1.3.3 Company cards
[r48] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r49] If the user complies with the above rule, the RO-CIA shall issue a new company card before the current card expires.

5.1.3.4 Control cards

[r50] The user shall apply for a renewal card at least **15** days prior to card expiration.

[r51] The RO-CIA shall issue a renewal card within **5** working days of receiving a complete application.

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

[r52] A user who changes country of residence may request to have his/her driver card exchanged. If the current card is valid, the user shall only show proof of residence in order to have the application granted.

[r53] The RO-CIA shall upon delivery of the new card take possession of the previous card and send it to the RO-A of origin. (Regulation article 14.4.c)

[r54] Card exchange due to changed country of residence shall otherwise follow the rules for new card issuing.

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

[r55] If a card has been lost or stolen, the user shall report this to the local Police and receive a copy of the report. Loss of card may be reported by the user, or by the Police upon receiving a found card. The Police shall without delay notify the issuing RO-CIA of the report.

[r56] Stolen and lost card shall be put on a blacklist available to authorities in all Member States.

[r57] Damaged and malfunctioning cards shall be delivered to the issuing RO-CIA, visually and electronically cancelled, and put on a blacklist.

[r58] If the card is lost, stolen, damaged or malfunctioning, the user shall apply for a replacement card within **7** days. (Regulation article 15.1)

[r59] Provided the user follows the above requirements, the RO-CIA shall issue a replacement card with new keys and certificate within 5 working days from receiving a complete application. (Regulation article 14.4.a)

[r60] The replacement card shall inherit the time of validity from the original card. (Regulation Annex 1B: VII). If the replaced card has less than six months remaining validity, the RO-CIA may issue a renewal card instead of a replacement card.

5.1.6 Application approval registration – handled by the RO-CIA

[r61] The RO-CIA shall register approved applications in a database. This data is made available for the RO-CA/RO-CP, which uses the information as input to the certificate generation and card personalization.

5.1.7 Card personalization – handled by the RO-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 RO-A.

5.1.7.1 Visual personalization

[r62] Cards shall be visually personalized according to Regulation Annex 1B, section IV.

5.1.7.2 User data entry

[r63] 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.

5.1.7.3 Key entry
[r64] 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 management, 7.2.

5.1.7.4 Certificate entry
[r65] The user certificate shall be inserted in the card before distribution to the user.

5.1.7.5 Quality Control
[r66] 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.

5.1.7.6 Cancellation (destruction) of non-distributed cards
[r67] 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).

[r68] All destroyed cards shall be registered in a cancellation database.

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

[r69] The RO-CP is responsible for keeping track of which card and card number is given to which user. Data shall be transferred from the RO-CP to the RO-CIA register.

5.1.9 Card distribution to the user – handled by the RO-CP or RO-CIA

[r70]

a) The personalization shall be scheduled so as to minimize the time that the personalized card require safe-keeping before delivery to the user. Storage over night requires secure safe-keeping. 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 immediately transferred to the place where they are to be delivered or distributed to the user, i.e. a controlled area.
c) Personalized cards shall always be kept separated from non-personalized cards.
d) The Tachograph card shall be distributed in a manner so as to minimize the risk of loss.
e) At the point of delivery of the card to the user, evidence of the user's identity (e.g. name) shall be checked against a physical person.
f) The user shall present valid means of identification
g) The reception of the card shall be acknowledged by the user's signature.

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

This section applies only to Workshop cards.
[r71] 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)

[r72] PIN codes shall consist of at least **4** digits (Regulation Annex 1B, App 10: Vehicle Units: 4.1.2).

5.1.10.1 PIN generation

[r73] PIN codes shall be generated in a secure system, securely transferred to workshop cards, and direct-printed to PIN-envelopes. PIN codes shall never be stored on a computer system in a manner that allows connection between PIN and user. The PIN generation system shall meet the requirements of ITSEC E3, CC EAL4 or equivalent security criteria.

5.1.10.2 PIN distribution
[r74] PIN codes may be distributed by regular mail.

[r75] PIN codes shall not be distributed in connection with the corresponding cards.

5.1.11 Card deactivation – handled by RO-A/RO-CIA and RO-CP

[r76] It shall be possible to permanently deactivate a card and any keys residing thereon. A decision of deactivation shall be taken by the RO-A or RO-CIA, the actual operation should be carried out by the RO-CP or a Service Agency.

[r77] Deactivation of cards shall take place in equipment suitable for the operation and it shall be verified that card functions and keys are destroyed. The card shall also be visually cancelled.

[r78] Deactivation of cards shall be registered in the card database and the card number shall be put on the blacklist.

5.2 Vehicle Units and Motion Sensors

Not applicable in Romania for the time being or in the foreseeable future.

6 Root keys and transport keys management: European Root key, Member State keys, Motion Sensor keys, transport keys

This section contains provisions for the management of

- European Root key - the ERCA public key (EUR.PK)
- Romanian keys, i.e. the Romanian signing key pair(s) (MS.SK, MS.PK)
- the Motion Sensor keys (Km_{WC})
- the transport keys (for communication between the ERCA and the RO-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 **Romanian keys** are the Romanian signing keys and may also be called Romanian 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 RO-CA receives the Motion Sensor keys from the ERCA, stores them and distributes them to manufacturers.

The **transport keys** are the asymmetric keys used for securely exchanging information between the ERCA and the RO-CA.

If the RO-CA has need for other cryptographic keys than the above, these shall not be considered part of the Tachograph system, and are not dealt within this policy.

The RO-CA ensures within its domain the confidentiality and integrity of all non-public keys generated, used and/or stored with it and effectively prevents any misuse of these keys. For this purpose, it has to employ suitable technical systems, which fulfill one of the following requirements:

- FIPS 140-2 (or 140-1) level 3 or higher [FIPS],
- CEN Workshop Agreement 14176-2 [CEN],
- certification according to EAL 4 or higher in accordance with ISO 15408 [CC] to level E3 or higher [ITSEC] based on a protection profile or security instructions (“Security Targets”), which encompasses the requirements of this NCA Policy – based on a comprehensive risk analysis – as well as structural and non-technical security measures,
- security criteria, which provide an equivalent level of security.

In the same way, it has to be proved that these systems are operated in an adequately secured operating environment at the RO-CA. No copies of non-public keys exist outside the secured environment

The RO-CA will sign equipment certificates exclusively within the same device used to store the Member State Private Keys.

6.1 ERCA public key

[r98] The RO-CA shall keep the ERCA public key (EUR.PK) in such a way as to maintain its integrity and availability at all times. If the EUR.PK is stored in the RO-CP, the same rule applies.

[r99] The RO-CP shall ensure that EUR.PK is inserted in all tachograph cards and vehicle units within their authority.

6.2 Romanian keys

The Romanian keys are the RO-CA signing key pair(s), which is used to sign all equipment certificates. The key pair consists of a public key (MS.PK) and a private, or secret, key (MS.SK). The RO-CA public key is certified by the ERCA, but is always generated by the RO-CA itself.

[r100] The Romanian private keys must not be used for any other purposes than signing Tachograph equipment certificates and for production of the ERCA key certification request (KCR).

6.2.1 Member State keys generation

[r101] 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. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

[r102] The key generation device should be stand-alone.

[r103] The actual device used and requirements met shall be stated in the RO-CA PS.

[r104] RO-CA key-pair generation shall require the active participation of three separate individuals. At least one of these shall have a role of CAA/PA (certification authority / personalization administrator), the others may have other trusted roles (see section 9.3.1 for role descriptions).

[r105] Keys shall be generated using the RSA algorithm with a key length of modulus n=1024 bits (Regulation Annex 1B, app 11:2.1/3.2).

[r106] The RO-CA shall have at least two (2) and maximum five (5) Romanian key pairs with associated signing certificates to ensure continuity, since the ERCA cannot issue replacement Member State certificates rapidly.

6.2.2 Romanian keys period of validity

[r107] Each RO-CA private key usage period is **2** years from the date of issuance of the corresponding public key's certificate, and shall not be used after its validity period for any purpose.

[r108] The corresponding public key shall have no end of validity.

6.2.3 Romanian private key storage

[r109] 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. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

[r110] For access to the RO-CA private signing keys, dual control is required. This means that no single person shall possess the means required to access the environment where the private key is

stored. It does not mean that signing of equipment certificates must be performed under dual control.

6.2.4 Romanian private key backup

[r111] The Romanian 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 RO-CA PS.

6.2.5 Member State private key escrow

[r112] The Member State private signing keys shall not be escrowed.

6.2.6 Member State keys compromise

[r113] A written instruction shall exist, included in the RO-CA PS, which states the measures to be taken by users and security responsible persons at the RO-CA and/or Service Agencies if the Member State private keys has become exposed, or is otherwise considered or suspected to be compromised.

[r114] In such case the RO-CA shall as a minimum:
− Inform without delay the RO-A, the ERCA and all other MSCAs.

6.2.7 Member State keys end of life

[r115] The RO-CA shall have routines to ensure that it always has a valid, certified Member State signing key pair.

[r116] Upon termination of the usage period of a Member State signing key pair, the public key shall be archived, and the private key has to be destroyed by the RO-CA in such a manner that no feature its use, misuse or recovering is possible.

6.3 Motion Sensor keys

[r117] The RO-CA shall request motion sensor key KmWC from the ERCA (Regulation Annex 1B, app 11:3.1.3). The RO-CA shall not handle with motion sensor master key Km or vehicle unit motion sensor key KmVU.

[r120] The RO-CA shall forward only the workshop key to the RO-CP for insertion into Workshop cards. The RO-CA, using suitable measures, ensures that the key Km_{WC} is passed on only to the intended receiver and secures their forwarding using suitable measures.

[r121] The RO-CP shall undertake the RO-CA's task to ensure that the workshop key KmWC is inserted into all issued Workshop cards (Regulation Annex 1B, app 11:3.1.3).

[r122] The RO-CA and/or RO-CP shall, during storage, use and distribution, protect the motion sensor 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. This shall be to a security

target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other nontechnical security measures.

6.4 Transport keys

[r123] For secure data communication, RO-CP shall issue special, asymmetric, transport keys. The RO-CP shall, during generation, storage, use and distribution, 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. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other nontechnical security measures.

6.5 Key Certification Requests and Motion Sensor Key Distribution Request

All key transport between RO-CA and ERCA uses means, media and protocols defined by ERCA Root Policy. MSA will appoint an authorized person to carry the media that contains the messages between RO-CA and ERCA

[r123.1] The RO-CA submits their public keys (MS.PK) for certification by the ERCA using the key certification request (KCR) protocol described in Annex A of the Digital Tachograph System European Root Policy [ERCA].

[r123.2] The RO-CA recognizes the ERCA public key (EUR.PK) in the distribution format described in Annex B of the Digital Tachograph System European Root Policy [ERCA].

[r123.3] The RO-CA requests motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D of the Digital Tachograph System European Root Policy [ERCA].

[r123.4] The RO-CA uses the physical media for key and certificate transport described in Annex C of the Digital Tachograph System European Root Policy [ERCA].

[r123.5] The RO-CA and RO-CP ensures 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 RO-CA and RO-CP.

[r123.6] RO-CA ensures that private keys will remain in HSM and will not be transported during key certification operations.

[r123.7] RO-CP ensures that transport private keys will remain in HSM and will not be transported during symmetric key distribution operations.

7 Equipment keys (asymmetric)

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

- Tachograph cards
- Vehicle Units (Not applicable for Romania for the time being or in the foreseeable future)

The symmetric Motion Sensor keys are not handled here.

7.1 General aspects RO-CP / RO-CA incl. Service Agencies and VU manufacturers

[r124] Equipment (Card and VU) initialization, key loading and personalization shall be performed in a physically secure and controlled environment.
Entry to this area shall be strictly regulated, controllable at the individual level, and requiring a minimum of two persons to be present to operate the system. A log shall be kept of the entries and the actions in the system.

[r125] No sensitive information contained in the key generation systems may leave the system in a way that violates this policy.

[r126] Tachograph cards: No sensitive information in the card personalization system may leave the system in a way that violates this policy.

[r127] VU/Motion Sensor: No sensitive information in the VU personalization system may leave the system in a way that violates this policy.

[r128] **Organizations (Subcontractors, Service Agencies)** that perform key generation and card personalization on behalf of more than one Member State shall do this in a clearly separate process for each of these. A log shall be kept of each individual process and the relevant RO-A shall have access to this on request.

[r129] **VU manufacturers** that perform VU personalization shall do this in a process clearly separated from the VU production. A log shall be kept of the personalization and the relevant RO-A shall have access to this on request.

[r130] **RO-CA/RO-CP/Service Agencies/VU manufacturers:** The log of the personalization system shall contain a reference to the order, and list the corresponding equipment numbers and certificates. The relevant RO-A shall have access to the logs on request.

7.2 Equipment key generation

[r131] Equipment keys may be generated either by the equipment manufacturer or by the RO-CP (Annex 1B, Appendix 11:3.1.1)

[r132] RO-CP shall make sure that equipment keys are generated in a secure manner and that the equipment private key is kept secret.

[r133] 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. This shall be to a security

target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other nontechnical security measures.

[r134] Keys shall be generated using the RSA algorithm having a key length of modulus *n* 1024 bits. (Annex 1B, Appendix 11:2.1/3.2)

[r135] The generation procedure and storage of the private key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been inserted in the device.

[r136] 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. (This is presumably done by making sure that the key generation system is random at its nature and therefore the probability of generating non-unique keys is insignificant.)

7.2.1.1 Batch key generation
[r137] Cryptographic key generation may be performed by batch processing in advance of certificate request, or in direct connection with certificate request.

[r138] Batch processing must be performed in stand-alone equipment meeting the security requirements stated above. Key integrity has to be protected until certificate issuing is performed.

7.2.2 Equipment key validity

7.2.2.1 Keys on cards

[r139] Usage of an equipment private key in connection with certificates issued under this policy shall never exceed the end of validity of the certificate.

7.2.2.2 Vehicle units

[r140] Not applicable in Romania for the time being or in the foreseeable future.

7.2.3 Equipment private key protection and storage - Cards

[r141] The RO-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.

[r142] Copies of the private key are not to be kept anywhere except in the tachograph card, unless required during key generation and device personalization.

[r143] In no case may the card private key be exposed or stored outside the card.

7.2.4 Equipment private key protection and storage – VUs

Not applicable in Romania for the time being or in the foreseeable future.

7.2.5 Equipment private key escrow and archival

[r147] Equipment private keys shall be neither escrowed nor archived.

7.2.6 Equipment public key archival

[r148] All certified public keys shall be archived by the certifying RO-CA. Information about certified public keys can be stored by RO-CP as well.

7.2.7 Equipment keys end of life

[r149] Upon termination of use of a Tachograph card, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

[r150] Upon termination of use of a Vehicle Unit, the public key shall be archived, and the private key shall be:

- destroyed such that the private key cannot be retrieved; or
- retained in a manner such that it is protected against being put back into use.

8 Equipment certificate management

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

8.1 Data input

8.1.1 Tachograph cards

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

[r151] The RO-CP shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique. The RO-CA shall verify the uniqueness of the CHR within its domain.

[r151.1] The certificate request process shall ensure that the RO-CP has possession of the private key associated with the public key presented for certification. At this time the private key shall not leave the secured environment of key generation.

8.1.2 Vehicle units

Not applicable in Romania for the time being or in the foreseeable future.

8.2 Tachograph card certificates

8.2.1 Driver certificates

[r154] Driver certificates are issued only to successful applicants for a Driver card.

8.2.2 Workshop certificates

[r155] Workshop certificates are issued only to successful applicants for a Workshop card.

8.2.3 Control body certificates

[r156] Control body certificates are issued only to successful applicants for a Control body card.

8.2.4 Hauling company certificates

[r157] Hauling company certificates are issued only to successful applicants for a Hauling Company card.

8.3 Vehicle unit certificates

Not applicable in Romania for the time being or in the foreseeable future.

8.4 Equipment certificate time of validity

[r160] Certificates shall not be valid longer than the corresponding equipment (section 5):

- Driver certificates shall not be valid more than **5** years (Regulation 14.4.a).
- Workshop certificates shall not be valid for more than **1** year (Regulation 12.1).
- Control body certificates shall not be valid more than **2** years.
- Hauling company certificates shall not be valid more than **5** years.

8.5 Equipment certificate issuing

[r161] The RO-CA shall ensure that it issues certificates so that their authenticity and integrity is maintained. Certificate contents are defined by Regulation Annex 1B, appendix 11.

8.6 Equipment certificate renewal and update

See Equipment management (section 5). Since certificates and cards have the same time of validity, they are dealt with together. VU certificates have either no end of, or a very long time of validity, it is assumed that the lifetime of the equipment is shorter than that of the certificate.

8.7 Dissemination of equipment certificates and information

[r162] The RO-CA shall export all certificate data to the RO-CIA register so that certificates, equipment and users are connected.

[r163] The RO-CIA shall ensure that certificates are made available as necessary to users and relying parties.

[r164] The RO-CIA shall ensure that all terms and conditions, as well as relevant parts of the RO-CA PS, and other relevant information, are made readily available to all users, relying parties and other relevant groups.

[r164.1] The RO-CA shall maintain and make certificate status information available.

8.8 Equipment certificate use

[r165] The Tachograph certificates are only for use within the Tachograph system.

8.9 Equipment certificate revocation

[r166] Certificates are not revoked (rather than revoking certificates, non-valid Tachograph equipment is put on a "black list" which may be checked at roadside controls).

9 RO-CA and RO-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.

9.1 Information security management of the RO-CA and RO-CP

[r167] The RO-CA/RO-CP shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

[r168] The RO-CA/RO-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 RO-CA/RO-CP and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the RO-CA/RO-CP. The RO-CA/RO-CP shall retain responsibility for the disclosure of relevant practices of all parties.

[r169] The information security infrastructure necessary to manage the security within the RO-CA/RO-CP shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the RO-A.

[r170] The RO-CA/RO-CP shall adopt a security management system equivalent to ISO 17799 [ISO 17799]. Formal certification is not required.

9.2 Asset classification and management of the RO-CA/RO-CP

[r171] The RO-CA/RO-CP shall ensure that its assets and information receive an appropriate level of protection. In particular:

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

9.3 Personnel security controls of the RO-CA/RO-CP

9.3.1 Trusted Roles

[r172] An RO-CA/RO-CP, supporting this NCA policy, should recognize at least three distinct roles, as outlined below. 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 RO-CA/RO-CP PS.

[r173] To ensure that one person acting alone cannot circumvent safeguards, responsibilities in RO-CA/RO-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.

[r174] The recommended roles are:
a) Certification Authority Administrator or Personalization Administrator (CAA/PA)
b) System Administrator (SA)
c) Information System Security Officer (ISSO)

[r175] The CAA/PA role includes:

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

[r176] 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
a) 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.

[r177] 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 RO-CA/RO-CP's records.
f) Participating in Member State key generation

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

9.3.2 Separation of roles

[r178] For a RO-CA/RO-CP, different individuals shall fill each of the three roles described above and **at least one individual** shall be appointed per task.

9.3.3 Identification and Authentication for Each Role

[r179] 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

[r180] The CAA/PA (Certification Authority/ Personalization Administrator), which involves creating and managing certificate and key information, is a critical position. The individual assuming the CAA/PA role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

[r181] All RO-CA/RO-CP personnel in sensitive positions, including, at least, all CAA/PA and ISSO (Information System Security Officer) positions, shall:

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

[r182] The RO-CA/RO-CP organizations shall ensure that they will all the time have personnel which has been checked for their qualification, rank, absence of a criminal record, absence of credit risks. These requirements should be stated in the applicable PS.

9.3.5 Training requirements

[r183] Personnel shall have adequate training for the role and job.

9.4 System security controls of the CA and personalization systems

[r184] The RO-CA/RO-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;

[r185] The Certification Authority System (CAS) and Personalization system shall provide sufficient system security controls for enforcing the separation of roles described in this policy or the relevant PS.

[r186] The security controls shall provide access control and traceability down to an individual level on all transactions and functions affecting the use of RO-CA's private issuing keys.

[r187] System security controls imposed on computer systems used by Service Agencies depend on the role assigned to the agency. Agencies that undertake CAA/PA (certification authority/personalization administrator) roles, load certificates onto cards, or initialize such cards, shall meet the requirements imposed upon RO-CA/CPs.

9.4.1 Specific computer security technical requirements

[r188] Initialization of the system operating RO-CA's private certification keys shall require co-operation of at least two operators, both of which are securely authenticated by the system.

9.4.2 Computer security rating

[r189] The CA and personalization systems do not require formal rating as long as they fulfill all requirements in this section.

9.4.3 System development controls

[r190] The RO-CA/RO-CP shall use trustworthy systems and products that are protected against modification.

[r191] An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the RO-CA/RO-CP or on behalf of the RO-CA/RO-CP to ensure that security is built into IT systems.

[r192] Change control procedures shall exist for releases, modifications and emergency software fixes for any operational software.

9.4.4 Security management controls

[r193] The system roles (section 9.3.1) shall be implemented and enforced.

9.4.5 Network security controls

[r194] Controls (e.g., firewalls) shall be implemented to protect the RO-CA/RO-CP's internal network domains from external network domains accessible by third parties.

[r195] Sensitive data shall be protected when exchanged over networks which are not secure.

9.5 Security audit procedures

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

9.5.1 Types of event recorded

[r196] The security audit functions related to the RO-CA/RO-CP computer/system shall log, for audit purposes:

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

9.5.2 Frequency of processing audit log

[r197] The log shall be processed regularly and analyzed against malicious behavior. Log procedures shall be described in the PS.

9.5.3 Retention period for audit log

[r198] Audit log shall be retained for at least **7** years.

9.5.4 Protection of audit log

[r199] Audit logs shall be appropriately integrity protected. All entries shall be individually time stamped (system time is sufficient).

[r200] Audit logs shall be verified and consolidated at least monthly. At least two people in SA or ISSO roles (see section 9.3.1) shall be present for such verification and consolidation.

9.5.5 Audit log backup procedures

[r201] Two copies of the consolidated log shall be made and stored in separate physically secured locations.

[r202] The audit log shall be stored in a way that makes it possible to examine the log during its retention period.

[r203] The audit log shall be protected from unauthorized access.

9.5.6 Audit collection system (internal vs. external)

[r204] Only internal audit collection system is required.

9.6 Record archiving

9.6.1 Types of event recorded by the RO-CIA

[r205] The records shall include all relevant evidence in the RO-CIA's possession including, but not limited to:

a) Certificate requests and all related messages exchanged with the RO-CA/RO-CP, users, and the directory.
b) Signed registration agreements from user's applications for certificates and cards, including the identity of the person responsible for accepting the application.
c) Signed acceptance of the delivery of cards.
d) Contractual agreements regarding certificates and associated cards.
e) Certificate renewals and all messages exchanged with the user.
f) Revocation requests and all recorded messages exchanged with the originator of the request and/or the user.
g) Currently and previously implemented policy documents

9.6.2 Types of event recorded by the RO-CA/RO-CP

[r206] The records shall include all relevant evidence in the RO-CA/RO-CP's possession including, but not limited to:

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

[r207] Records of all digitally signed electronic requests made by RO-CA/RO-CP or Service Agency personnel (CAA/PA) shall include the identity of the administrator responsible for each request together with all information required for non-repudiation checking of the request for as long as the record is retained.

9.6.3 Retention period for archive

[r208] Archives shall 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

[r209] The RO-CA/RO-CP shall act in compliance with requirements regarding confidentiality as stated in section 3.4.

[r210] Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognized representatives.

[r211] RO-CA/RO-CP shall make available on request, produced documentation of the RO-CA/RO-CP's compliance with the applicable PS according to section 11.5.

[r212] Subject to statute, a reasonable handling fee may be charged to cover the cost of record retrieval.

[r213] The RO-CA/RO-CP shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the RO-CA/RO-CP's operations are interrupted, suspended or terminated.

[r214] In the event that RO-CA/RO-CP services are to be interrupted, suspended or terminated, the RO-CA/RO-CP shall send notification to all customer organizations to ensure the continued availability of the archive. All requests for access to archived information shall be sent to the RO-CA/RO-CP or to the entity identified by the RO-CA/RO-CP prior to terminating its service.

9.7 RO-CA/RO-CP continuity planning

[r215] RO-CA/RO-CP shall have a business continuity plan (BCP). 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

9.7.1 Member State keys compromise

Member State keys compromise is dealt with in section 6.

9.7.2 Other disaster recovery

[r216] RO-CA/RO-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, functioning data restoration procedures etc., to be detailed in the BCP.

9.8 Physical security control of the CA and personalization systems

[r217] Physical security controls shall be implemented to control access to the RO-CA or RO-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).

[r218] The Member state keys for signing certificates shall be kept physically and logically protected as described in the PS.

[r219] The RO-CA/RO-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. Backup

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

[r220] A security check of the facility housing the RO-CA/RO-CP's central equipment shall be made at least once every **24** hours. If it is a continuously attended facility, this may be a visual check once per shift to ensure that the systems and any associated cryptographic devices/cards are securely stored if not in use, that the physical security systems (e.g., door locks and alarms) are functioning properly, and that there have been no attempts at forceful entry or unauthorized access.

9.8.1 Physical access

[r221] Access to the physical area housing the Member state keys and the means for their usage, shall require simultaneously presence of at least **2** persons which have been individually appointed the right to enter the area.

[r222] Access to other RO-CA/RO-CP facilities shall be limited to those personnel performing one of the roles described in section 9.3.1. 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.

10 RO-CA or RO-CP Termination

10.1 Final termination - RO-A responsibility

Final termination of an RO-CA or RO-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 RO-CA service is passed over from an old Member State key pair to new Member State key pair or ERCA key.

[r223] The RO-A shall ensure that the tasks outlined below are carried out. Note: RO-CA/RO-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.

[r224] Before the RO-CA/RO-CP terminates its services the following procedures has to be completed as a minimum:

a) Inform all users and parties with whom the RO-CA/RO-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 RO-CA/RO-CP shall terminate all authorization of subcontractors to act on behalf of the RO-CA/RO-CP in the process of issuing certificates.
d) The RO-CA/RO-CP shall perform necessary undertakings to transfer obligation for maintaining record archives for the remaining period of their life cycle.

10.2 Transfer of RO-CA or RO-CP responsibility

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

[r225] The RO-A shall ensure that orderly transfer of responsibilities and assets is carried out.

[r226] The old RO-CA shall transfer all root keys to the new RO-CA in the manner decided by the RO-A.

[r227] The old RO-CA shall destroy any copies of keys that are not transferred.

11 Audit

[r228] The RO-A is responsible for ensuring that audits of the RO-CA and RO-CP take place.

11.1 Frequency of entity compliance audit

[r229] An RO-CA/RO-CP operating under this NCA policy shall be audited at least annually for conformance with the policy.

11.2 Topics covered by audit

[r230] The audit shall cover the RO-CA/RO-CP´s practices (according to their PSs).

[r231] The audit shall cover the RO-CA/RO-CP´s compliance with this NCA policy.

[r231.1] The audit shall cover the requirements defined in ERCA-CP §5.3 [ERCA]

[r232] The audit shall also consider the operations of any Service Agencies.

11.3 Who should do the audit

[r233] The RO-A may consult an external certification or accreditation organization for approval of the RO-CA/RO-CP PS in order to increase relying parties' trust in the implementation. Otherwise the RO-A shall undertake the auditing.

11.4 Actions taken as a result of deficiency

[r234] If irregularities are found in the audit the RO-A shall take appropriate action depending on severity.

11.5 Communication of results

[r235] Results of the audits on a security status level shall be available upon request. Actual audit reports shall not be available except on need-to-know basis.
[r235.1] The RO-A includes the results of the audit in a report that defines corrective actions including an implementation schedule, required to fulfill the RO-A obligations. The report will be provided, in English, to the ERCA.

12 NCA policy change procedures

12.1 Items that may change without notification

[r236] The only changes that may be made to this specification without notification are

a) Editorial or typographical corrections
b) Changes to the contact details

12.2 Changes with notification

12.2.1 Notice

[r237] Any item in this certificate policy may be changed with **90** days notice.

[r238] Changes to items which, in the judgment of the policy responsible organization (the RO-A), **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

[r239] Impacted users may file comments with the policy administration organization within **15** days of original notice.

12.2.3 Whom to inform

[r240] Information about changes to this policy shall be sent to:

- The European Commission
- ERCA
- RO-CA and RO-CP including Service Agencies
- All other MSAs
- Affected VU Manufacturers and Motion Sensor Manufacturers

12.2.4 Period for final change notice

[r241] 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 NCA policy approval

[r242] If a policy change is determined by the RO-A organization to have a material impact on a significant number of users of the policy, the RO-A shall submit the revised NCA policy to the **ERCA** for approval.

13 References

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. - owned by the European Commission.

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

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

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

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

[ISO 17799] BS ISO/IEC 17799: 2005. Information technology -- Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project. – owed by the European Commission

[ERCA] Digital Tachograph System European Root Policy – Version 2.0.

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 NCA 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.

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 RO-CA, as a subcontractor.

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

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

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
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
MSCA Member State CA
PIN Personal Identification Number
PKI Public Key Infrastructure
RSA A specific Public key algorithm
SA System Administrator
PS Practice Statement
VU Vehicle Unit
VUP VU Personalizing organization

15 Correspondence table with the ERCA Policy

The requirements for the Romanian CA Policy are formulated in the ERCA Policy § 5.3. The table below provides the rationale between the requirements as formulated in the ERCA Policy [ERCA] and the requirements in the Romanian CA Policy.

Item	Reference ERCA Policy	Requirement	Reference RO-MSA Policy
1	§ 5.3.1	The MSA Policy shall identify the entities in charge of operations.	§1.3 Responsible organization
2	§ 5.3.2	The MSCA key pairs for equipment key certification and for motion sensor key distribution shall be generated and stored within a device which either: • is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [10]; • is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [11]; • is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [12]; to level E3 or higher in ITSEC [13]; or equivalent security criteria. These evaluations shall be to a protection profile or security target, • is demonstrated to provide an equivalent level of security.	§6.2.1 Member State keys generation §6.3 Motion Sensor Keys §6.4 Transport keys §6.5 Key Certification Requests and Motion Sensor Key Distribution Request
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.	§6 Root keys and transport keys management: European Root key, Member State keys, Motion Sensor keys, transport keys [paragraph 8] §6.2.1 Member State keys generation [r104]
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.	§6.2.2 Romanian keys period of validity
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	§6.2.1 Member State keys generation [r106]

6	§ 5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.	§6.5 Key Certification Requests and Motion Sensor Key Distribution Requests [r123.1]
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.	§6.5 Key Certification Requests and Motion Sensor Key Distribution Requests [r123.3]
8	§ 5.3.8	The MSA shall recognise the ERCA public key in the distribution format described in Annex B	§6.5 Key Certification Requests and Motion Sensor Key Distribution Requests [r123.2]
9	§ 5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C	§6.5 Key Certification Requests and Motion Sensor Key Distribution Requests [r123.4]
10	§ 5.3.10	The MSA 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 MSCA.	§6.5 Key Certification Requests and Motion Sensor Key Distribution Requests [r123.5]
11	§ 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.	§6.2.7 Member State keys end of life [r116]
12	§ 5.3.12	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 • 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; The last two of these requirements on generation shall be met by generating equipment keys within a device which either:	§5.1.1 Quality control – RO-CA/RO-CP function[r27] §7.1 General aspects RO-CP / RO-CA incl. Service Agencies and VU manufacturers [r124] to [r126] §7.2 Equipment key generation

		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.	
13	§ 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.	§3.4.1 Types of information to be kept confidential [r20] §6.2.1 Member State keys generation §6.2.3 Romanian private key storage §6.4 Transport keys §7.2 Equipment key generation
14	§ 5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	§6.2.3 Romanian private key storage §6.4 Transport keys §7.2 Equipment key generation §7.2.3 Equipment private key protection and storage – Cards
15	§ 5.3.15	The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.	§6.2.1 Member State keys generation [r106] §6.2.4 Romanian private key backup [r111]
16	§ 5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	§6.5 Key Certification Requests and Motion Sensor Key Distribution Request [r123.6] §7.2.3 Equipment private key protection and storage – Cards [r143]

17	§ 5.3.17	Key escrow is strictly forbidden	§6.2.5 Member State private key escrow [r112] §7.2.5 Equipment private key escrow and archival [r147]
18	§ 5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	§6.3 Motion Sensor keys [r120], [r122]
19	§ 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 [7].	Not applicable
20	§ 5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	Not applicable
21	§ 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 [r120]
22	§ 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
23	§ 5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	§6.3 Motion Sensor keys [r122]
24	§ 5.3.24	The MSA shall ensure that its motion sensor key copies are 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 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.	§6.3 Motion Sensor keys [r122]
25	§ 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
26	§ 5.3.26	The MSA shall ensure availability of its equipment public key certification service.	§6.2.1 Member State keys generation [r106]
27	§ 5.3.27	The MSA shall only use the Member State Private Keys for:	§6.2 Romanian keys [r100]

		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 [6]; 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).	
28	§ 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).	§6.2.3 Romanian private key storage [r109]
29	§ 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) [6].	§7.2 Equipment key generation [r136] §8.1.1 Tachograph cards [r151]
30	§ 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.	§8.1.1 Tachograph cards [r151.1]
31	§ 5.3.31	The MSA shall maintain and make certificate status information available	§8.7 Dissemination of equipment certificates and information [r164.1] §8.9 Equipment certificate revocation [r166]
32	§ 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 [r160]
33	§ 5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	§8.4 Equipment certificate time of validity [r160]
34	§ 5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	Not applicable
35	§ 5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	§5.1.2.1 User application [r30] to [r33] §5.1.9 Card distribution to the user – handled by the RO-CP or RO-CIA [r70]
36	§ 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 Member State keys compromise [r113], [r114]

37	§ 5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	§6.2.1 Member State keys generation [r106] §9.7 RO-CA/RO-CP continuity planning [r215]
38	§ 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 security management of the RO-CA and RO-CP [r170]
39	§ 5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	§9.3 Personnel security controls of the RO-CA/RO-CP
40	§ 5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	§9.6.1 Types of event recorded by the RO-CIA [r205] §9.6.2 Types of event recorded by the RO-CA/RO-CP [r206]
41	§ 5.3.41	The MSA shall include provisions for MSCA termination in the MSA Policy.	§10 RO-CA or RO-CP Termination
42	§ 5.3.42	The MSA Policy shall include change procedures.	§12 NCA policy change procedures
43	§ 5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	§11.2 Topics covered by audit [r230] to [r232]
44	§ 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 [r229]
45	§ 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 ERCA.	§11.5 Communication of results [r235.1]
46	§ 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 [r235.1]