Council of the
European Union

Brussels, 14 March 2019
(OR. en)

7510/19
ADD 3

TRANS 199
DELACT 68

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2019) 1789 final - Annex 3
Subject:	ANNEX to the Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

Delegations will find attached document C(2019) 1789 final - Annex 3.

Encl.: C(2019) 1789 final - Annex 3

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 3

ANNEX

to the

Commission Delegated Regulation

supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TABLE OF CONTENTS

ANNEX III

1. INTRODUCTION

1.1. Overview and scope of this policy

This certificate policy defines the European C-ITS trust model based on public key infrastructure (PKI) within the scope of the overall EU C-ITS security credential management system (EU CCMS). It defines requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. At its highest level, the PKI is composed of a set of root CAs 'enabled' as a result of the trust list manager (TLM) inserting their certificates in a European certificate trust list (ECTL), which is issued and published by the central entity TLM (see sections 1.2 and 1.3).

This policy is binding on all entities participating in the trusted C-ITS system in Europe. It helps in the assessment of the level of trust that can be established in the received information by any receiver of a message authenticated by an end-entity certificate of the PKI. To allow assessment of trust in the certificates provided by the EU CCMS, it sets out a binding set of requirements for the operation of the central entity TLM and the compilation and management of the ECTL. Consequently, this document governs the following aspects relating to the ECTL:

- identification and authentication of principals obtaining PKI roles for the TLM, including statements of the privileges allocated to each role;
- minimum requirements for local security practices for the TLM, including physical, personnel and procedural controls;
- minimum requirements for technical security practices for the TLM, including computer security, network security and cryptographic module engineering controls;
- minimum requirements for operational practices for the TLM, including registration of new root CA certificates, the temporary or permanent deregistration of existing included root CAs, and the publication and distribution of ECTL updates;
- an ECTL profile, including all mandatory and optional data fields in the ECTL, cryptographic algorithms to be used, the exact ECTL format and recommendations for processing the ECTL;
- ECTL certificate lifecycle management, including distribution of ECTL certificates, activation, expiration and revocation;
- management of the revocation of trust of root CAs where necessary.

Since the trustworthiness of the ECTL does not depend solely on the ECTL itself, but to a large extent also on the root CAs that compose the PKI and their sub-CAs, this policy also sets out minimum requirements, which are mandatory for all participating CA's (root CAs and sub-CAs). The requirement areas are the following:

- identification and authentication of principals obtaining PKI roles (e.g. security officer, privacy officer, security administrator, directory administrator and end-user), including a statement of duties, responsibilities, liabilities and privileges associated with each role;

- key management, including acceptable and mandatory certificate-signing and data-signing algorithms, and certificate validity periods;
- minimum requirements for local security practices, including physical, personnel and procedural controls;
- minimum requirements for technical security practices such as computer security, network security and cryptographic module engineering controls;
- minimum requirements for operational practices of the CA, EA, AA and end-entities, including aspects of registration, de-registration (i.e. de-listing), revocation, key-compromise, dismissal for cause, certificate update, audit practices and non-disclosure of privacy-related information;
- certificate and CRL profile, including formats, acceptable algorithms, mandatory and optional data fields and their valid value ranges, and how verifiers are expected to process certificates;
- regular monitoring, reporting, alerting and restoring duties of the C-ITS trust model entities in order to establish secure operation, including in cases of misbehaviour.

In addition to these minimum requirements, the entities running the root CAs and sub-CAs may decide their own additional requirements and set them out in the relevant certificate practice statements (CPSs), provided they do not contradict the requirements set out in the certificate policy. See section 1.5 for details on how CPSs are audited and published.

The CP also states the purposes for which the root CAs, sub-CAs and their issued certificates may be used. It sets out the liabilities assumed by:

- the TLM;
- each root CA whose certificates are listed in the ECTL;
- the root CA's sub-CAs (EA and AA);
- each member or organisation responsible for, or operating, one of the C-ITS trust model entities.

The CP also defines mandatory obligations applying to:

- the TLM;
- each root CA whose certificates are listed in the ECTL;
- each sub-CA certified by a root CA;
- all end-entities;
- each member organisation responsible for, or operating, one of the C-ITS trust model entities.

Finally, the CP sets out requirements as regards the documentation of limitations to liabilities and obligations in the CPS of each root CA whose certificates are listed in the ECTL.

This CP is in line with the certificate policy and certification practices framework adopted by the Internet Engineering Task Force (IETF) [3].

1.2. Definitions and acronyms

The definitions in [2], [3] and [4] apply.

AA	authorisation authority
AT	authorisation ticket
CA	certification authority
CP	certificate policy
CPA	C-ITS certificate policy authority
CPOC	C-ITS point of contact
CPS	certificate practice statement
CRL	certificate revocation list
EA	enrolment authority
EC	enrolment credential
ECIES	elliptic curve integrated encryption scheme
EE	end-entity (i.e. C-ITS station)
ECTL	European certificate trust list
EU CCMS	EU C-ITS security credential management system
GDPR	General Data Protection Regulation
HSM	Hardware security module
PKI	public key infrastructure
RA	registration authority
sub-CA	EA and AA
TLM	trust list manager

Glossary

applicant	The natural person or legal entity that applies for (or seeks renewal of) a certificate. Once the initial certificate is created (initialisation), the applicant is referred to as the subscriber. For certificates issued to end-entities, the subscriber (certificate applicant) is the entity that controls or operates/maintains the end-entity to which the certificate is issued, even if the end-entity is sending the actual certificate request.
authorisation authority	In this document, the term 'authorisation authority' (AA) refers not only to the specific function of the AA, but also to the legal and/or operational entity managing it.
certification authority	The root certification authority, enrolment authority and authorisation authority are cumulatively referred to as the certification authority (CA).
C-ITS trust model	The C-ITS trust model is responsible for establishing a relationship of trust between C-ITS stations. It is implemented through the use of a PKI composed of root CAs, the CPOC, TLM, EAs, AAs and a secure network.
crypto-agility	The capability of the C-ITS trust model entities to adapt the CP to changing environments or to new future requirements, e.g. by a change of cryptographic algorithms and key length over time
cryptographic module	A secure hardware-based element within which keys are generated and/or stored, random numbers are generated and data are signed or encrypted.
enrolment authority	In this document, the term 'enrolment authority' (EA) refers not only to the specific function of the EA, but also to the legal and/or operational entity managing it.
PKI participants	Entities of the C-ITS trust model, i.e. the TLM, root CAs, EAs, AAs and C-ITS stations.
re-keying	This subcomponent is used to describe certain elements relating to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key as described in [3].
repository	The repository used for storing the certificates and information on certificates provided by the entities of the C-ITS trust model, as defined in section 2.3.
root certification authority	In this document, the term 'root certification authority' (CA) refers not only to the specific function of the CA, but also to the legal and/or operational entity managing it.
subject	The natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber.
subscriber	A natural person or legal entity to which a certificate is issued and which is legally bound by a subscriber or terms of use agreement.
subscriber agreement	An agreement between the CA and the applicant/subscriber that specifies the rights and responsibilities of the parties.

1.3. PKI participants

1.3.1. Introduction

PKI participants play a role in the PKI defined by the present policy. Unless explicitly it is prohibited, a participant can assume multiple roles at the same time. It may be prohibited from assuming specific roles at the same time in order to avoid conflicts of interest or to ensure a segregation of duties.

Participants may also delegate parts of their role to other entities as part of a service contract. For example, when revocation status information is provided using CRLs, the CA is also the CRL issuer, but it may delegate the responsibility for issuing CRLs to a different entity.

PKI roles consist of:

- authoritative roles, i.e. each role is uniquely instantiated;
- operational roles, i.e. roles that can be instantiated in one or more entities.

For example, a root CA can be implemented by a commercial entity, a common interest group, a national organisation and/or a European organisation.

Figure 1 shows the C-ITS trust model architecture based on [2]. The architecture is described briefly here, but the main elements are described in more detail in sections 1.3.2 to 1.3.6.

The CPA appoints the TLM, which is therefore a trusted entity for all PKI participants. The CPA approves the root CA operation and confirms that the TLM can trust the root CA(s). The TLM issues the ECTL that provides all PKI participants with trust in the approved root CAs. The root CA issues certificates to the EA and AA, thus providing trust in their operation. The EA issues enrolment certificates to the sending and relaying C-ITS stations (as end-entities), thus providing trust in their operation. The AA issues ATs to the C-ITS stations on the basis of trust in the EA.

The receiving and relaying C-ITS station (as relaying party) can trust other C-ITS stations, since the ATs are issued by an AA that is trusted by a root CA, which is trusted by the TLM and the CPA.

Note that Figure 1 describes only the root CA level of the C-ITS trust model. Details of the lower layers are provided in the subsequent sections of this CP or the CPS of the specific root CAs.

Figure 2 provides an overview of the information flows between PKI participants. The green dots indicate flows that require machine-to-machine communications. The information flows in red have defined security requirements.

The C-ITS trust model is based on a multiple root CA architecture, where the root CA certificates are transmitted periodically (as set out below) to the central point of contact (CPOC) through a secure protocol (e.g. link certificates) defined by the CPOC.

A root CA can be operated by a governmental or a private organisation. The C-ITS trust model architecture contains at least one root CA (the EU root CA with the same level as the other root CAs). The EU root CA is delegated by all entities participating in the C-ITS trust model that do not want to set up their own root CA. The CPOC transmits the received root CA certificates to the TLM, which is responsible for

collecting and signing the list of root CA certificates and sending them back to the CPOC, which makes them publicly available to everybody (see below).

The trust relationships between the entities in the C-ITS trust model are described in the following figures, tables and sections.

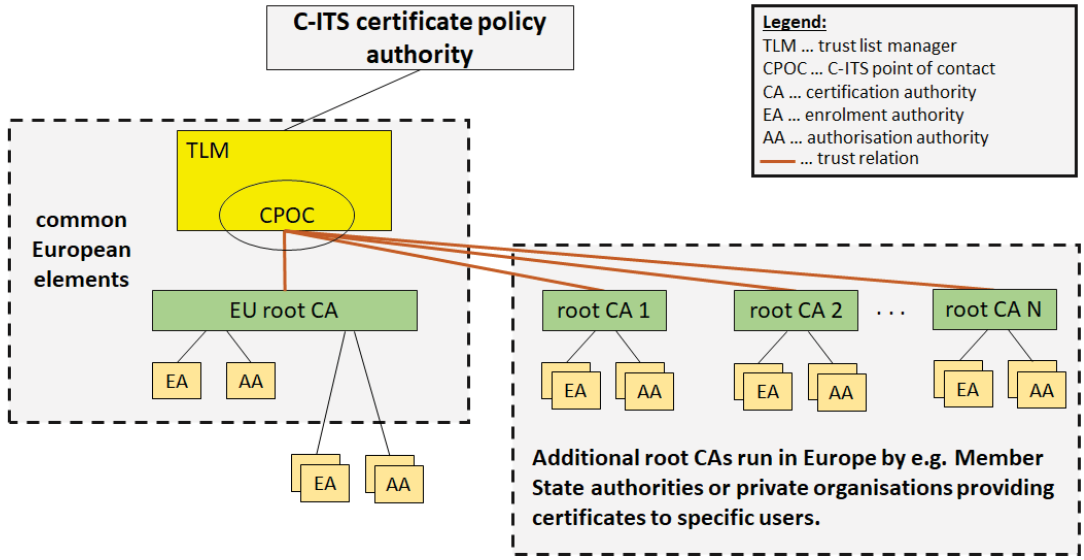

Figure 1: C-ITS trust model architecture

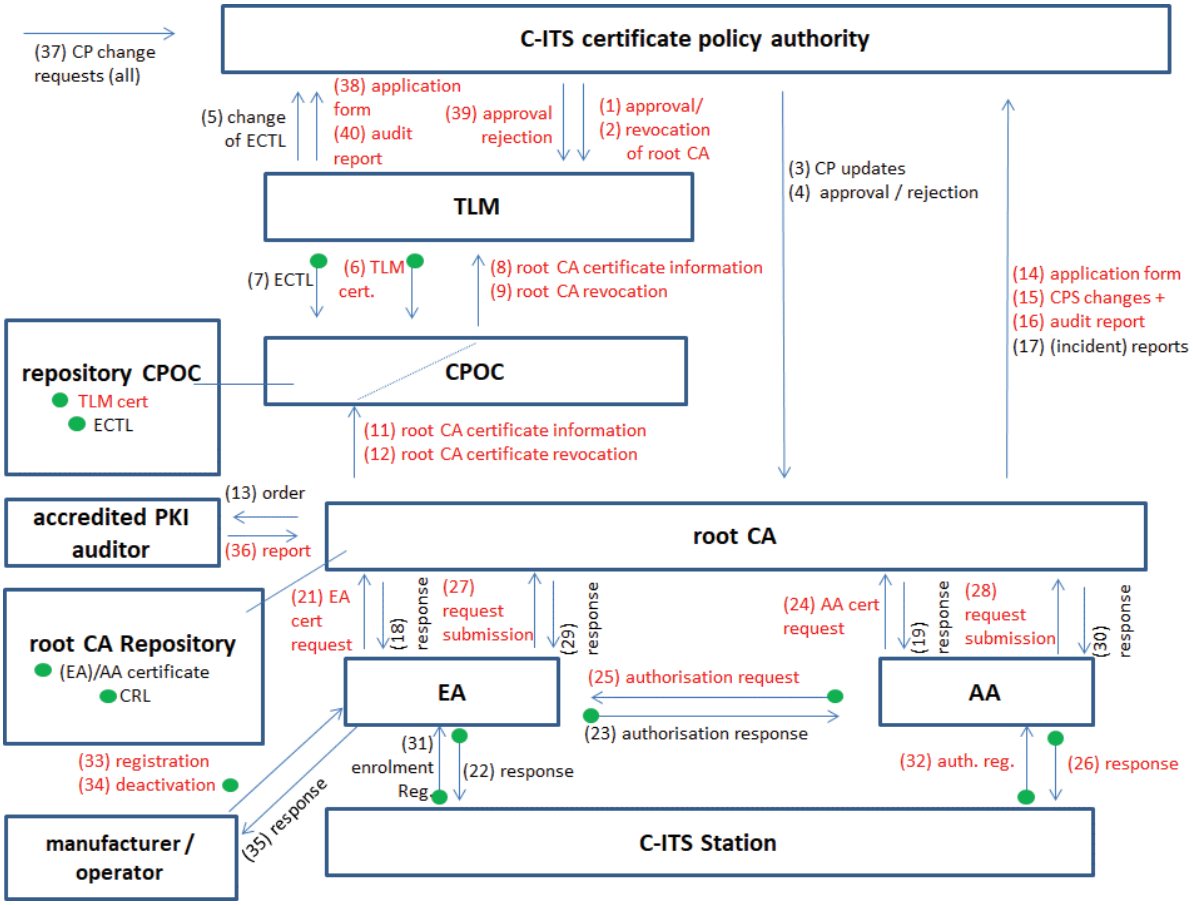

Figure 2: C-ITS Trust model information flows

Flow ID	From	To	Content	Reference
(1).	CPA	TLM	approval of root CA application	8
(2).	CPA	TLM	information on revocation of root CA	8.5
(3).	CPA	root CA	CP updates	1.5
(4).	CPA	root CA	approval/rejection of root CA application form or the CPS request changes or the audit process.	8.5, 8.6
(5).	TLM	CPA	notification of change of ECTL	4, 5.8.1
(6).	TLM	CPOC	TLM certificate	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	root CA certificate information	4.3.1.1
(9).	CPOC	TLM	root CA certificate revocation	7.3
(10).	CPOC	all end-entities	TLM certificate	4.4.2
(11).	root CA	CPOC	root CA certificate information	4.3.1.1
(12).	root CA	CPOC	root CA certificate revocation	7.3
(13).	root CA	auditor	audit order	8
(14).	root CA	CPA	root CA application form — initial request	4.1.2.1
(15).	root CA	CPA	root CA application form — CPS changes	1.5.1
(16).	root CA	CPA	root CA application form — audit report	8.6
(17).	root CA	CPA	root CA incident reports, including revocation of a sub-CA (EA, AA)	Annex III, 7.3.1
(18).	root CA	EA	EA certificate response	4.2.2.3
(19).	root CA	AA	AA certificate response	4.2.2.3
(20).	root CA	All	EA/AA certificate, CRL	4.4.2
(21).	EA	root CA	EA certificate request	4.2.2.3
(22).	EA	C-ITS station	enrolment credential response	4.3.1.4
(23).	EA	AA	authorisation response	4.2.2.5
(24).	AA	root CA	AA certificate request	4.2.2.3
(25).	AA	EA	authorisation request	4.2.2.5
(26).	AA	C-ITS station	authorisation ticket response	4.3.1.5
(27).	EA	root CA	request submission	4.1.2.3
(28).	AA	root CA	request submission	4.1.2.3
(29).	root CA	EA	response	4.12 and 4.2.1

(30).	root CA	AA	response	4.12 and 4.2.1
(31).	C-ITS station	EA	enrolment credential request	4.2.2.4
(32).	C-ITS station	AA	authorisation ticket request	4.2.2.5
(33).	manufacturer / operator	EA	registration	4.2.1.4
(34).	manufacturer / operator	EA	deactivation	7.3
(35).	EA	manufacturer / operator	response	4.2.1.4
(36).	auditor	root CA	report	8.1
(37).	all	CPA	CP change requests	1.5
(38).	TLM	CPA	application form	4.1.2.2
(39).	CPA	TLM	approval/rejection	4.1.2.2
(40).	TLM	CPA	audit report	4.1.2.2

Table 1: Detailed description of information flows in the C-ITS trust model

1.3.2. C-ITS certificate policy authority

(1) The C-ITS certificate policy authority (CPA) is composed of the representatives of public and private stakeholders (e.g. Member States, vehicle manufacturers, etc.) participating in the C-ITS trust model. It is responsible for two sub-roles:

(1) certificate policy management, including:

- approval of the present CP and future CP change requests;
- deciding on the review of CP change requests and recommendations submitted by other PKI participants or entities;
- deciding on the release of new CP versions;

(2) PKI authorisation management, including:

- defining, deciding and publishing the CPS approval and CA audit procedures (collectively referred to as 'CA approval procedures');
- authorising the CPOC to operate and report regularly;
- authorising the TLM to operate and report regularly;
- approval of the root CA's CPS, if it is in line with the common and valid CP;
- scrutiny of the audit reports from the accredited PKI auditor for all root CAs;
- notifying the TLM about the list of approved or non-approved root CAs and their certificates on the basis of received approval reports of the root CAs and regular operations reports.

(2) The CPA's authorised representative is responsible for authenticating the TLM's authorised representative and approving the TLM's enrolment process application form. The CPA is responsible for authorising the TLM to operate as mentioned in this section.

1.3.3. Trust list manager

(3) The TLM is a single entity appointed by the CPA.

(4) The TLM is responsible for:

- the operation of the ECTL in accordance with the common valid CP and regular activity reporting to the CPA for the overall secure operation of the C-ITS trust model;
- receiving root CA certificates from the CPOC;
- including/excluding root CA certificates in the ECTL upon notification by the CPA;
- signing the ECTL;
- the regular and timely transmission of the ECTL to the CPOC.

1.3.4. Accredited PKI auditor

(5) The accredited PKI auditor is responsible for:

- performing or organising audits of root CAs, TLM and sub-CAs;
- distributing the audit report (from an initial or periodic audit) to the CPA in line with the requirements in section 8 below. The audit report is to include recommendations from the accredited PKI auditor;
- notifying the entity managing the root CA of the successful or unsuccessful execution of an initial or periodic audit of the sub-CAs;
- assessing CPSs' compliance with this CP.

1.3.5. C-ITS point of contact (CPOC)

(6) The CPOC is a single entity appointed by the CPA. The CPA's authorised representative is responsible for authenticating the CPOC's authorised representative and approving the CPOC enrolment process application form. The CPA is responsible for authorising the CPOC to operate as set out in this section.

(7) The CPOC is responsible for:

- establishing and contributing to the secure communication exchange between all entities of the C-ITS trust model in an efficient and fast way;
- reviewing procedural change requests and recommendations submitted by other trust model participants (e.g. root CAs);
- transmitting root CA certificates to the TLM;
- publication of the common trust anchor (current public key and link certificate of the TLM);
- publication of the ECTL.

Complete details of the ECTL can be found in section 7.

1.3.6. Operational roles

(8) The following entities defined in [2] play an operational role, as defined in RFC 3647:

Functional element	PKI role ([3] and [4])	Detailed role ([2])
root certification authority	CA/RA (registration authority)	Provides EA and AA with proof that it may issue ECs or ATs
enrolment authority	subscriber to root CA / subject of EA certificate CA/RA	Authenticates a C-ITS station and grants it access to ITS communications
authorisation authority	subscriber to root CA / subject of AA certificate CA/RA	Provides a C-ITS station with authoritative proof that it may use specific ITS services
sending C-ITS station	subject of end-entity (EE) certificate (EC)	Acquires rights from EA to access ITS communications Negotiates rights from AA to invoke ITS services Sends single-hop and relayed broadcast messages
relaying (forwarding) C-ITS station	relaying party / subject of EE certificate	Receives broadcast message from sending C-ITS station and forwards them to receiving C-ITS station if required
receiving C-ITS station	relaying party	Receives broadcast messages from sending or relaying C-ITS station
manufacturer	subscriber to EA	Installs necessary information for security management in C-ITS station at production
operator	subscriber to EA / AA	Installs and updates necessary information for security management in C-ITS station during operation

Table 2: Operational roles

Note: in accordance with [4], different terms are used in this CP for the 'subscriber' which contracts with the CA for the issuance of certificates and the 'subject' to which the certificate applies. Subscribers are all entities that have a contractual relationship with a CA. Subjects are entities to which the certificate applies. EA/AAs are subscribers and subjects of the root CA and can request EA/AA certificates. C-ITS stations are subjects and can request end-entity certificates.

(9) Registration authorities:

The EA is to perform the role of a registration authority for end-entities. Only an authenticated and authorised subscriber can register new end-entities (C-ITS stations) in an EA. The relevant root CAs are to perform the role of registration authorities for EAs and AAs.

1.4. Certificate usage

1.4.1. Applicable domains of use

(10) Certificates issued under the present CP are intended to be used to validate digital signatures in the cooperative ITS communication context in accordance with the reference architecture of [2].

(11) The certificate profiles in [5] determine certificate uses for the TLM, root CAs, EAs, AAs and end-entities.

1.4.2. Limits of responsibility

(12) Certificates are not intended, nor authorised, for use in:

- circumstances that offend, breach or contravene any applicable law, regulation (e.g. GDPR), decree or government order;
- circumstances that breach, contravene or infringe the rights of others;
- breach of this CP or the relevant subscriber agreement;
- any circumstances where their use could lead directly to death, personal injury or severe environmental damage (e.g. through failure in the operation of nuclear facilities, aircraft navigation or communication, or weapons control systems);
- circumstances that contravene the overall objectives of greater road safety and more efficient road transport in Europe.

1.5. Certificate policy administration

1.5.1. Updating of CPSs of CAs listed in the ECTL

(13) Each root CA listed in the ECTL shall publish its own CPS, which must be in compliance with this policy. A root CA may add additional requirements, but shall ensure that all requirements of this CP are met at all times.

(14) Each root CA listed in the ECTL shall implement an appropriate change process for its CPS document. The key properties of the change process shall be documented in the public part of the CPS.

(15) The change process shall ensure that all changes to this CP are carefully analysed and, if necessary for compliance with the CP as amended, the CPS is updated within the timeframe laid down in the implementation step of the change process for the CP. In particular, the change process shall involve emergency change procedures that ensure timely implementation of security-relevant changes to the CP.

(16) The change process shall include appropriate measures to verify CP compliance for all changes to the CPS. Any changes to the CPS shall be clearly documented. Before a new version of a CPS is implemented, its compliance with the CP must be confirmed by an accredited PKI auditor.

(17) The root CA shall notify the CPA of any change made to the CPS with at least the following information:

- an exact description of the change;
- the rationale for the change;
- a report from the accredited PKI auditor confirming compliance with the CP;
- contact details of the person responsible for the CPS;
- planned timescale for implementation.

1.5.2. CPS approval procedures

(18) Before starting its operations, a prospective root CA shall present its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and to the CPA for approval (flow 15).

(19) A root CA shall present changes to its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and to the CPA for approval (flow 15) before those changes become effective.

(20) An EA/AA shall present its CPS or changes to its CPS to the root CA. The root CA may order a certificate of conformity from the national body or private entity responsible for approval of the EA/AA, as defined in sections 4.1.2 and 8.

(21) The accredited PKI auditor shall assess the CPS in accordance with section 8.

(22) The accredited PKI auditor shall communicate the results of the CPS assessment as part of the audit report, as set out in section 8.1. The CPS shall be accepted or rejected as part of the audit report acceptance referred to in sections 8.5 and 8.6.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Methods for the publication of certificates information

(23) Certificate information may be published pursuant to section 2.5:

- in a regular or periodic way; or
- in response to a request from one of the participating entities.

In each case, different degrees of urgency for publication and therefore time schedules apply, but entities must be ready for both types of arrangement.

(24) The regular publication of the certificate information makes it possible to determine a maximum deadline by which certificate information is updated for all nodes of the C-ITS network. The frequency of the publication of all certificate information is laid down in section 2.2.

(25) At the request of entities participating in the C-ITS network, any of the participants may start to publish certificate information at any time and, depending on its status, request a current set of certificate information so as to become a fully trusted node of the C-ITS network. The purpose of such publication is mainly to update entities on the overall current status of certificate information in the network and enable them to communicate on a trusted basis until the next regular publication of the information.

(26) A single root CA may also initiate the publication of certificate information at any point in time by sending an updated set of certificates to all 'subscribed members' of the C-ITS network that are regular recipients of such information. This supports the operation of the CAs and enables them to address members between the regular and scheduled dates for publishing the certificates.

(27) Section 2.5 sets out the mechanism and all procedures for publishing root CA certificates and the ECTL.

(28) The CPOC shall publish the root CA certificates (as included in the ECTL and intended for public consumption), the TLM certificate and the ECTL that it issues.

(29) Root CAs shall publish their EA/AA certificates and CRLs, and be able to support all three mechanisms referred to here for publishing them to their subscribed members and relying parties, taking all necessary steps to ensure secure transmission, as referred to in section 4.

2.2. Time or frequency of publication

(30) The requirements as to the publication schedule for certificates and CRLs must be determined in the light of the various limiting factors of the single C-ITS nodes, with the overall goal of operating a 'trusted network' and publishing updates as quickly as possible to all C-ITS stations involved.

- For the regular publication of updated certificate information (e.g. changes in the ECTL or CRL composition), a maximum period of three months is required for the safe operation of the C-ITS network.
- Root CAs shall publish their CA certificates and CRLs as soon as possible after issuance.
- For the publication of the CRL, the root CA repository shall be used.

In addition, the CPS for each CA shall specify the period of time within which a certificate will be published after the CA issues the certificate.

This section specifies only the time or frequency of the regular publication. Means of connectivity to update C-ITS stations with the ECTL and CRLs within a week of their publication (under normal operation conditions, e.g. with cellular coverage, vehicle in actual operation, etc.) shall be implemented in accordance with the requirements in this document.

2.3. Repositories

(31) The requirements regarding the structure of the repository for storing the certificates and what information is provided by the entities of the C-ITS network are as follows for the single entities:

- in general, each root CA should use a repository of its own currently active EA/AA certificate information and CRL to publish certificates for the other PKI participants (e.g. an LDAP-based directory service). The repository of each root CA shall support all required access controls (section 2.4) and transmission times (section 2.2) for every method of distribution of C-ITS-related information;
- the TLM's repository (which stores the ECTL and TLM certificates published by the CPOC, for example) should be based on a publication mechanism able to ensure the transmission times set out in section 2.2 for every method of distribution.

Requirements of AAs are not defined, but they must support the same security levels as the other entities and these must be declared in their CPS.

2.4. Access controls on repositories

(32) The requirements on access control to repositories of certificate information shall at least comply with the general standards of secure information handling

outlined in ISO/IEC 27001 and with the requirements in section 4. In addition, they shall reflect the process security needs to be established for the single process steps in the publication of certificate information.

- This includes the implementation of the repository for TLM certificates and the ECTL in the TLM/CPOC. Each CA or repository operator shall implement access controls in relation to all of the C-ITS entities and external parties for at least three different levels (e.g. public, restricted to C-ITS entities, root CA level) in order to prevent unauthorised entities from adding to, amending or deleting repository entries.
- The exact access control mechanisms of the single entity should be part of the respective CPS.
- For each root CA, the EA and AA repositories shall comply with the same requirements for access control procedures regardless of the place or contractual link to the service provider operating the repository.

As a starting point for the levels of access control, each root CA or repository operator should provide at least three different levels (e.g. public, restricted to C-ITS entities, root CA level).

2.5. Publication of certificate information

2.5.1. Publication of certificate information by the TLM

(33) The TLM in the European common C-ITS trust domain shall publish the following information via the CPOC:

- all currently valid TLM certificates for the next period of operation (current and link certificate if available);
- access point information for the CPOC repository to provide the signed list of root CA´s (ECTL);
- general information point for the ECTL and C-ITS deployment.

2.5.2. Publication of certificate information by CAs

(34) Root CAs in the European common C-ITS trust domain shall publish the following information:

- issued (currently valid) root CA certificates (current and correctly re-keyed certificates, including a link certificate) in the repository referred to in section 2.3;
- all valid EA, AA entities, with their operator ID and planned period of operation;
- issued CA certificates in the repositories referred to in section 2.3;
- the CRLs for all revoked CA certificates covering their subordinate EAs and AAs;
- information regarding the root CA’s point of access to the CRL and CA information.

All certificate information shall be categorised in accordance with three levels of confidentiality and documents for the general public must be publicly available without restrictions.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of name

3.1.1.1. Names for TLM, root CAs, EAs, AAs

(35) The name in the TLM certificate shall consist of a single subject_name attribute with the reserved value 'EU_TLM'.

(36) The name for root CAs shall consist of a single subject_name attribute with a value allocated by the CPA. The uniqueness of names is the sole responsibility of the CPA and the TLM shall maintain the registry of root CA names upon notification by the CPA (approval, revocation/removal of a root CA). Subject names in certificates are limited to 32 bytes. Each root CA proposes its name to the CPA in the application form (flow 14). The CPA is responsible for checking name uniqueness. If the name is not unique, the application form is rejected (flow 4).

(37) The name in each EA/AA certificate may consist of a single subject_name attribute with a value generated by the issuer of the certificate. The uniqueness of names is the sole responsibility of the issuing root CA.

(38) The EA and AA certificates shall not use a name greater than 32 bytes, because subject_name in certificates are limited to 32 bytes.

(39) ATs shall not contain a name.

3.1.1.2. Names for end-entities

(40) Each C-ITS station shall be assigned two kinds of unique identifier:

- a canonical ID that is stored at the initial registration of the C-ITS station under the responsibility of the manufacturer. This shall contain a substring identifying the manufacturer or operator so that this identifier can be unique;
- a subject_name, which may be part of the C-ITS station's EC, under the responsibility of the EA.

3.1.1.3. Identification of certificates

(41) Certificates following the format of [5] shall be identified by computing a HashedId8 value as defined in [5].

3.1.2. Need for names to be meaningful

No stipulation.

3.1.3. Anonymity and pseudonymity of end-entities

(42) The AA shall ensure that the pseudonymity of a C-ITS station is established by providing the C-ITS station with ATs that do not contain any names or information that may link the subject to its real identity.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

(43) Names for the TLM, root CAs, EAs, AAs and canonical IDs for C-ITS stations shall be unique.

(44) The TLM shall ensure in the registration process of a given root CA in the ECTL that its certificate identifier (HashedId8) is unique. The root CA shall ensure in the issuance process that the certificate identifier (HashedId8) of each subordinate CA is unique.

(45) The HashedId8 of an EC shall be unique within the issuing CA. The HashedId8 of an AT does not have to be unique.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

(46) The root CA shall prove that it rightfully holds the private key corresponding to the public key in the self-signed certificate. The CPOC shall check this proof.

(47) The EA/AA shall prove that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The root CA shall check this proof.

(48) Possession of a new private key (for re-keying) shall be proven by the signing of the request with the new private key (inner signature) followed by the generation of an outer signature over the signed request with the current valid private key (to guarantee the authenticity of the request). The applicant shall submit the signed certificate request to the issuing CA via a secure communication. The issuing CA shall verify that the applicant's digital signature on the request message was created using the private key corresponding to the public key attached to the certificate request. The root CA shall specify which certificate request and responses it supports in its CPS.

3.2.2. Authentication of organisation identity

3.2.2.1. Authentication of root CAs' organisation identity

(49) In an application form to the CPA (i.e. flow 14), the root CA shall provide the identity of the organisation and registration information, composed of:

- organisation name;
- postal address;
- e-mail address;
- the name of a physical contact person in the organisation;
- telephone number;
- digital fingerprint (i.e. SHA 256 hashvalue) of the root CA's certificate in printed form;
- cryptographic information (i.e. cryptographic algorithms, key lengths) in the root CA certificate;
- all permissions that the root CA is allowed to use and to pass to the sub-CAs.

(50) The CPA shall check the identity of the organisation and other registration information provided by the certificate applicant for the insertion of a root CA certificate in the ECTL.

(51) The CPA shall collect either direct evidence, or an attestation from an appropriate and authorised source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to which a certificate is issued. Submitted evidence may be in the form of paper or electronic documentation.

(52) The subject's identity shall be verified at the time of registration by appropriate means and in accordance with the present certificate policy.

(53) At each certificate application, evidence shall be provided of:

- the full name of the organisational entity (private organisation, government entity or non-commercial entity);
- nationally recognised registration or other attributes that may be used, as far as possible, to distinguish the organisational entity from others with the same name.

The rules above are based on TS 102 042 [4]: *The CA shall ensure that evidence of the subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorised sources, and that certificate requests are accurate, authorised and complete in accordance with the collected evidence or attestation.*

3.2.2.2. Authentication of TLM organisation identity

(54) The organisation operating the TLM shall provide evidence of the identification and accuracy of the name and associated data in order to enable appropriate verification at initial creation and re-keying of the TLM certificate.

(55) The subject's identity shall be verified at the time of certificate creation or re-keying by appropriate means and in accordance with the present CP.

(56) Organisation evidence shall be provided as specified in section 3.2.2.1.

3.2.2.3. Authentication of sub-CAs organisation identity

(57) The root CA shall check the identity of the organisation and other registration information provided by certificate applicants for sub-CA (EA/AA) certificates.

(58) At a minimum, the root CA shall:

- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
- use postal mail or a comparable procedure requiring the certificate applicant to confirm certain information about the organisation, that it has authorised the certificate application and that the person submitting the application on behalf of the applicant is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.

(59) Validation procedures for issuing CA certificates shall be documented in a CPS of the root CA.

3.2.2.4. Authentication of end-entities' subscriber organisation

(60) Before the subscriber of end-entities (manufacturer/operator) can register with a trusted EA to enable its end-entities for sending EC certificate requests, the EA shall:

- check the identity of the subscriber organisation and other registration information provided by the certificate applicant;
- check that the C-ITS station type (i.e. the concrete product based on brand, model and version of the C-ITS station) meets all compliance assessment criteria.

(61) At a minimum, the EA shall:

- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
- use postal mail or a comparable procedure to require the certificate applicant to confirm certain information about the organisation, that it has authorised the certificate application and that the person submitting the application on its behalf is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.

(62) Validation procedures for the registration of a C-ITS station by its subscriber shall be documented in a CPS of the EA.

3.2.3. Authentication of individual entity

3.2.3.1. Authentication of TLM/CA individual entity

(63) For the authentication of an individual entity (physical person) identified in association with a legal person or organisational entity (e.g. the subscriber), evidence shall be provided of:

- full name of the subject (including surname and given names, in line with the applicable law and national identification practices);
- date and place of birth, reference to a nationally recognised identity document or other attributes of the subscriber that may be used, as far as possible, to distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organisational entity (e.g. the subscriber);
- any relevant registration information (e.g. company registration) of the associated legal person or other organisational entity;
- evidence that the subject is associated with the legal person or other organisational entity.

Submitted evidence may be in the form of paper or electronic documentation.

(64) To verify his/her identity, the authorised representative of a root CA, EA, AA or subscriber shall provide documentation proving that he/she works for the organisation (certificate of authorisation). He/she shall also show an official ID.

(65) For the initial enrolment process (flow 31/32), a representative of the EA/AA shall provide the corresponding root CA with all necessary information (see section 4.1.2).

(66) The personnel at the root CA shall verify the identity of the certificate applicant representative and all associated documents, applying the requirements of 'trusted personnel' as set out in section 5.2.1. (The process of validating application information and generating the certificate by the root CA shall be carried out by 'trusted persons' at the root CA, under at least dual supervision, as they are sensitive operations within the meaning of section 5.2.2).

3.2.3.2. Authentication of C-ITS stations' subscriber identity

(67) Subscribers are represented by authorised end-users in the organisation who are registered at the issuing EA and AA. These end-users designated by organisations (manufacturers or operators) shall prove their identity and authenticity before:

- registering the EE at its corresponding EA, including its canonical public key, canonical ID (unique identifier) and the permissions in accordance with the EE;
- registering at the AA and securing proof of a subscriber agreement that can be sent to the EA.

3.2.3.3. Authentication of C-ITS stations' identity

(68) EE subjects of ECs shall authenticate themselves when requesting ECs (flow 31) by using their canonical private key for the initial authentication. The EA shall check the authentication using the canonical public key corresponding to the EE. The canonical public keys of the EEs are brought to the EA before the initial request is executed, by a secure channel between the C-ITS station manufacturer or operator and the EA (flow 33).

(69) EE subjects of ATs shall authenticate themselves when requesting ATs (flow 32) by using their unique enrolment private key. The AA shall forward the signature to the EA (flow 25) for validation; the EA shall validate it and confirm the result to the AA (flow 23).

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of authority

3.2.5.1. Validation of TLM, root CA, EA, AA

(70) Every organisation shall identify in the CPS at least one representative (e.g. a security officer) responsible for requesting new certificates and renewals. The naming rules in section 3.2.3 shall apply.

3.2.5.2. Validation of C-ITS station subscribers

(71) At least one physical person responsible for registering C-ITS stations at an EA (e.g. security officer) shall be known to and approved by the EA (see section 3.2.3).

3.2.5.3. Validation of C-ITS stations

(72) A C-ITS station's subscriber may register C-ITS stations at a specific EA (flow 33) as long as it is authenticated at that EA.

Where the C-ITS station is registered at an EA with a unique canonical ID and a canonical public key, it may request an EC using a request signed with the canonical private key related to the previously registered canonical public key.

3.2.6. Criteria for interoperation

(73) For communication between C-ITS stations and EAs (or AAs), the C-ITS station shall be able to establish secure communication with EAs (or AAs), i.e. to implement authentication, confidentiality and integrity functions, as specified in [1]. Other protocols may be used, provided that [1] is implemented. The EA and AA shall support this secure communication.

(74) The EA and AA shall support certificate requests and responses that comply with [1], which provides for a secure AT request/response protocol supporting the anonymity of the requester *vis-à-vis* the AA and separation of duties between the AA and the EA. Other protocols may be used, provided that [1] is implemented. To prevent disclosure of C-ITS stations' long-term identity, communication between a mobile C-ITS station and an EA shall be confidential (e.g. communication data shall be encrypted end-to-end).

(75) The AA shall submit an authorisation validation request (flow 25) for each authorisation request it receives from an EE certificate subject. The EA shall validate this request with respect to:

- the status of the EE at the EA;
- the validity of the signature;
- the requested ITS Application IDs (ITS-AID) and permissions;
- the status of service provision of the AA to the subscriber.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key requests

3.3.1.1. TLM certificates

(76) The TLM generates a key pair and two certificates: one self-signed and one link certificate as referred to in section 7.

3.3.1.2. Root CA certificates

Not applicable.

3.3.1.3. EA/AA certificate renewal or re-keying

(77) Prior to the expiry of an EA/AA certificate, the EA/AA shall request a new certificate (flow 21/flow 24) to maintain continuity of certificate usage. The EA/AA shall generate a new key pair to replace the expiring key pair and sign the re-key request containing the new public key with the current valid private

key ('re-keying'). The EA or AA generates a new key pair and signs the request with the new private key (inner signature) to prove possession of the new private key. The whole request is signed (oversigned) with the current valid private key (outer signature) to ensure the integrity and authenticity of the request. If an encryption and decryption key pair is used, possession of private decryption keys shall be proven (for detailed description of re-keying, see section 4.7.3.3).

(78) The identification and authentication method for routine re-keying is the same as that for the initial issuance of an initial root CA certificate validation, as set out in section 3.2.2.

3.3.1.4. End-entities' enrolment credentials

(79) Prior to the expiry of an existing EC, the EE shall request a new certificate (flow 31) to maintain continuity of certificate usage. The EE shall generate a new key pair to replace the expiring key pair and request a new certificate containing the new public key; the request shall be signed with the current valid EC private key.

(80) The EE may sign the request with the newly created private key (inner signature) to prove possession of the new private key. The whole request is then signed (oversigned) with the current valid private key (outer signature) and encrypted to the receiving EA as specified in [1], to ensure the confidentiality, integrity and authenticity of the request. Other protocols may be used, provided that [1] is implemented.

3.3.1.5. End-entities' authorisation tickets

(81) The certificate re-key for ATs is based on the same process as the initial authorisation, as defined in [1]. Other protocols may be used, provided that [1] is implemented.

3.3.2. Identification and authentication for re-key requests after revocation

3.3.2.1. CA certificates

(82) The authentication of a CA organisation for root CA, EA and AA certificate re-keying after revocation is handled in the same way as the initial issuance of a CA certificate, as set out in section 3.2.2.

3.3.2.2. End-entities' enrolment credentials

(83) The authentication of an EE for EC certificate re-keying after revocation is handled in the same way as the initial issuance of an EE certificate, as set out in section 3.2.2.

3.3.2.3. End-entities' authorisation requests

Not applicable, since ATs are not revoked.

3.4. Identification and authentication for revocation request

3.4.1. Root CA/EA/AA certificates

(84) Requests to delete a root CA certificate from the ECTL shall be authenticated by the root CA to the TLM (flows 12 and 9). Requests to revoke an EA/AA certificate shall be authenticated by the relevant root CA and sub-CA itself.

(85) Acceptable procedures for authenticating a subscriber's revocation requests include:

- a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked;
- communication with the subscriber providing reasonable assurances that the person or organisation requesting revocation is in fact the subscriber. Depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.2. C-ITS station enrolment credentials

(86) The C-ITS station subscriber may revoke the EC of a previously registered C-ITS station at an EA (flow 34). The requesting subscriber shall create a request for revocation of a given C-ITS station or list of C-ITS stations. The EA shall authenticate the revocation request before processing it and confirm the revocation of the C-ITS stations and their ECs.

(87) The EA may revoke the EC of a C-ITS station in accordance with section 7.3.

3.4.3. C-ITS station authorisation tickets

(88) As ATs are not revoked, their validity shall be limited to a specific period. The range of acceptable validity periods in this certificate policy is specified in section 7.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate application

(89) This section sets out the requirements for an initial application for certificate issuance.

(90) The term 'certificate application' refers to the following processes:

- registration and setup of a trust relation between the TLM and the CPA;
- registration and setup of a trust relation between the root CA and the CPA and TLM, including the insertion of the first root CA certificate in the ECTL;
- registration and setup of a trust relation between the EA/AA and the root CA, including the issuance of a new EA/AA certificate;
- registration of the C-ITS station at the EA by the manufacturer/operator;
- C-ITS station's request for EC/AT.

4.1.1. Who can submit a certificate application

4.1.1.1. Root CAs

(91) Root CAs generate their own key pairs and issue their root certificate by themselves. A root CA can submit a certificate application through its designated representative (flow 14).

4.1.1.2. *TLM*

(92) The TLM generates its own key pairs and issues its certificate by itself. The initial creation of the TLM certificate shall be processed by a TLM organisation representative under the control of the CPA.

4.1.1.3. EA and AA

(93) An authorised representative of the EA or AA may submit the sub-CA (EA and/or AA) certificate request application to the authorised representative of the relevant root CA (flow 27/28).

4.1.1.4. C-ITS station

(94) Subscribers shall register each C-ITS station at the EA in accordance with section 3.2.5.3.

(95) Each C-ITS station registered at the EA may send EC requests (flow 31).

(96) Each C-ITS station may send AT requests (flow 32) without requesting any subscriber interaction. Before requesting an AT, a C-ITS station shall have an EC.

4.1.2. Enrolment process and responsibilities

(97) Permissions for root-CAs and sub-CAs issuing certificates for special (governmental) purposes (i.e.special mobile and fixed C-ITS stations) may be granted only by the Member States in which the organisations are located.

4.1.2.1. Root CAs

(98) After being audited (flow 13 and 36, section 8), root CAs may apply for insertion of their certificate(s) in the ECTL at the CPA (flow 14). The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA by the root CA's authorised representative and that contains at least the information referred to in sections 3.2.2.1, 3.2.3 and 3.2.5.1.

(99) The root CA's application form shall be signed by its authorised representative.

(100) In addition to the application form, the root CA's authorised representative shall provide a copy of the root CA's CPS (flow 15) and its audit report to the CPA for approval (flow 16). In cases of positive approval, the CPA generates and sends a certificate of conformity to the CPOC/TLM and the corresponding root CA.

(101) The root CAs authorised representative shall then bring its application form (containing the fingerprint of the self-signed certificate), the official ID and a proof of authorisation to the CPOC/TLM. The self-signed certificate shall be delivered electronically to the CPOC/TLM. The CPOC/TLM shall verify all documents and the self-signed certificate.

(102) In cases of positive verifications, the TLM shall add the root CA's certificate to the ECTL based on the notification from the CPA (flows 1 and 2). The detailed process is described in the CPS of the TLM.

(103) An additional procedure to get an approval of the CPS and audit report of a root CA at a national body of specific countries should be possible.

4.1.2.2. *TLM*

(104) After being audited, the TLM may enrol with the CPA. The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA (flow 38) by the TLM's authorised representative and contains at least the information referred to in sections 3.2.2.2 and 3.2.3.

(105) The TLM's application form shall be signed by its authorised representative.

(106) First, the TLM generates its self-signed certificate and transmits it securely to the CPA. The TLM then brings its application form (containing the fingerprint of the self-signed certificate), a copy of its CPS, an official ID, a proof of authorisation and its audit report to the CPA (flow 40). The CPA shall check all the documents and the self-signed certificate. In cases of positive verification of all documents, the self-signed certificate and the fingerprint, the CPA shall confirm the enrolment process by sending its approval to the TLM and the CPOC (flow 39). The CPA shall store the application information sent by the TLM. The TLM certificate is then issued via the CPOC.

4.1.2.3. EA and AA

(107) During the enrolment process, the EA/AA shall bring the relevant documents (e.g. the CPS and the audit report) to the corresponding root CA for approval (flow 27/28). In cases of positive checks of the documents, the root CA sends an approval to the corresponding root sub-CAs (flow 29/30). The sub-CA (EA or AA) shall then transmit its signed request electronically, and physically deliver its application form (in accordance with section 3.2.2.1), proof of authorisation and ID document to the corresponding root CA. The root CA verifies the request and the received documents (application form containing the fingerprint, which is the SHA 256 hashvalue of the sub-CA request, proof of authorisation and ID Document). If all checks lead to a positive result, the root CA issues the corresponding sub-CA certificate. Detailed information how an initial request is done is described in its specific CPS.

(108) In addition to the sub-CA application form, the sub-CA's authorised representative shall attach a copy of the CPS to the root CA.

(109) Information shall be given to an accredited PKI auditor for auditing in accordance with section 8.

(110) If a sub-CA is owned by an entity different than the entity that owns a root CA, before issuing a sub-CA certificate request, the sub-CA's entity shall sign a contract regarding the root CA service.

4.1.2.4. C-ITS station

(111) The initial registration of end-entities subjects (C-ITS stations) shall be carried out by the responsible subscriber (manufacturer /operator) with the EA (flows 33 and 35) after successful authentication of the subscriber organisation and one of its representatives in line with sections 3.2.2.4 and 3.2.5.2.

(112) A C-ITS station may generate an EC key pair (see section 6.1) and create a signed EC request in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(113) During the registration of a normal C-ITS station (as opposed to a special mobile or fixed C-ITS station), the EA must verify that the permissions in the

initial request are not for governmental use. Permissions for governmental use are defined by the corresponding Member States. The detailed procedure for the registration and response of the EA to the manufacturer/operator (flows 33 and 35) shall be set out in the corresponding CPS of the EA.

(114) A C-ITS station shall be enrolled at an EA (section 3.2.5.3) by sending its initial EC request in accordance with [1].

(115) Upon initial registration by an authenticated subscriber representative, the EA approves which ATs the end-entity subject (i.e. the C-ITS station) may obtain. Furthermore, each end-entity is assigned a trust assurance level, which is related to the certification of the end-entity in accordance with one of the protection profiles listed in section 6.1.5.2.

(116) Regular vehicles shall have only one C-ITS station that is registered at one EA. Special-purpose vehicles (such as police cars and other special-purpose vehicles with specific rights) may be registered at an additional EA or have one additional C-ITS station for authorisations within the scope of the special purpose. Vehicles to which such an exemption applies shall be defined by the Member States responsible. Permissions for special mobile and fixed C-ITS stations shall be granted only by the Member States responsible. The CPS of root CAs or sub-CAs issuing certificates for such vehicles in those Member States shall determine how the certificate process applies to such vehicles.

(117) Where the subscriber is in the process of migrating a C-ITS station from one EA to another EA, the C-ITS station may be registered at two (similar) EAs.

(118) A C-ITS station generates an AT key pair (see section 6.1) and creates an AT request in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(119) C-ITS stations send an authorisation request to the AA's URL (flows 32 and 26) by sending at least the required information referred to in section 3.2.3.3). The AA and EA validate the authorisation for each request in accordance with sections 3.2.6 and 4.2.2.5.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

4.2.1.1. Identification and authentication of root CAs

(120) The CPA's authorised representative is responsible for authenticating the root CA's authorised representative and approving its enrolment process in accordance with section 3.

4.2.1.2. Identification and authentication of the TLM

(121) The CPA's authorised representative is responsible for authenticating the TLM's authorised representative and approving its enrolment process application form in accordance with section 3.

4.2.1.3. Identification and authentication of EA and AA

(122) The corresponding root CA is responsible for authenticating the EA/AA's authorised representative and approving its enrolment process application form in accordance with section 3.

(123) The root CA shall confirm its positive validation of the application form to the EA/AA. The EA/AA may then send a certificate request to the root CA (flow 21/24), which shall issue certificates to the corresponding EA/AA (flow 18/19).

4.2.1.4. Identification and authentication of EE subscriber

(124) Before a C-ITS station can request an EC certificate, the EE subscriber shall securely transmit the C-ITS station identifier information to the EA (flow 33). The EA shall verify the request and in cases of positive verification register the C-ITS station information in its database and confirm this to the EE subscriber (flow 35). This operation is done only once by the manufacturer or operator for each C-ITS station. Once a C-ITS station is registered by an EA, it may request a single EC certificate it needs (flow 31) at a time. The EA authenticates and verifies that the information in the EC certificate request is valid for a C-ITS station.

4.2.1.5. Authorisation tickets

(125) During authorisation requests (flow 32), in accordance with [1], the AA must authenticate the EA from which the C-ITS station received its EC. Other protocols may be used, provided that [1] is implemented. If the AA is not able to authenticate the EA, the request is rejected (flow 26). As a requirement, AA shall possess the EA certificate to authenticate the EA and verify its response (flows 25 and 23, section 3.2.5.3).

(126) The EA authenticates the C-ITS station requesting an AT by verifying its EC (flows 25 and 23).

4.2.2. Approval or rejection of certificate applications

4.2.2.1. Approval or rejection of root CA certificates

(127) The TLM inserts/deletes the root CA certificates into the ECTL in accordance with the approval of the CPA (flow 1/2).

(128) The TLM should verify the signature, information and encoding of root CA certificates after receiving an approval by the CPA (flow 1). After positive validation and the CPA's approval, the TLM shall put the corresponding root certificate on the ECTL and notify the CPA (flow 5).

4.2.2.2. *Approval or rejection of TLM certificate*

(129) The CPA is responsible for approving or rejecting TLM certificates.

4.2.2.3. *Approval or rejection of EA and AA certificates*

(130) The root CA verifies sub-CA certificate requests (flow 21/24) and the relevant reports (issued by the accredited PKI auditor) on receiving them (flow 36, section 8) from the corresponding sub-CA of the root CA. If the check of the request leads to a positive result, the corresponding root CA issues a certificate to the requesting EA/AA (flow 18/19); otherwise, the request is rejected and no certificate shall be issued to the EA/AA.

4.2.2.4. Approval or rejection of EC

(131) The EA shall verify and validate EC requests in accordance with sections 3.2.3.2 and 3.2.5.3.

(132) If the certificate request in accordance with [1] is correct and valid, the EA shall generate the requested certificate.

(133) Where the certificate request is invalid, the EA refuses it and sends a response setting out the reason for refusal in accordance with [1]. If a C-ITS station still wants an EC, it shall make a new certificate request. Other protocols may be used, provided that [1] is implemented.

4.2.2.5. Approval or rejection of AT

(134) The certificate request is checked by the EA. The AA shall establish communication with EA to validate the request (flow 25). The EA shall authenticate the requesting C-ITS station and validate whether it is entitled to receive the requested AT following the CP (e.g. by checking the revocation status and validate certificate time/region validity, permissions, assurance level, etc.). The EA shall return a validation response (flow 23) and, if the response is positive, the AA shall generate the requested certificate and transmit it to the C-ITS station. If the AT request is not correct or the EA validation response is negative, the AA refuses the request. If a C-ITS station still requires an AT, it shall make a new authorisation request.

4.2.3. Time to process the certificate application

4.2.3.1. Root CA certificate application

(135) The time to process the identification and authentication process of a certificate application is during working day and shall be subject to a maximum time limit laid down in the root CA's CPS.

4.2.3.2. *TLM certificate application*

(136) The processing of the TLM certificate application shall be subject to a maximum time limit laid down in the TLM's CPS.

4.2.3.3. *EA and AA certificate application*

(137) The time to process the identification and authentication process of a certificate application is during working day in accordance with the agreement and contract between the Member State/private organisation root CA and the sub-CA. The time to process sub-CA certificate applications shall be subject to a maximum time limit laid down in the sub-CA's CPS.

4.2.3.4. *EC application*

(138) The processing of EC applications shall be subject to a maximum time limit laid down in the EA's CPS.

4.2.3.5. *AT application*

(139) The processing of AT applications shall be subject to a maximum time limit laid down in the AA's CPS.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

4.3.1.1. Root CA certificate issuance

(140) Root CAs issue their own self-signed root CA certificates, link certificates, sub-CA certificates and CRLs.

(141) After CPA approval (flow 4), the root CA sends its certificate to the TLM through the CPOC to be added to the ECTL (flows 11 and 8) (see

section 4.1.2.1). The TLM checks whether the CPA has approved the certificate (flow 1).

4.3.1.2. *TLM certificate issuance*

(142) The TLM issues its own self-signed TLM and link certificate and sends it to the CPOC (flow 6).

4.3.1.3. EA and AA certificate issuance

(143) The sub-CAs generate a signed certificate request and transmit it to the corresponding root CA (flows 21 and 24). The root CA verifies the request and issues a certificate to the requesting sub-CA in accordance with [5] as soon as possible, as laid down in the CPS for usual operational practices, but not later than five working days after the request has been received.

(144) The root CA shall update the repository containing the certificates of the sub-CAs.

4.3.1.4. EC issuance

(145) The C-ITS station shall send an EC request to the EA in accordance with [1]. The EA shall authenticate and verify that the information in the certificate request is valid for a C-ITS station. Other protocols may be used, provided that [1] is implemented.

(146) In cases of positive validation, the EA shall issue a certificate in accordance with the C-ITS station registration (see 4.2.1.4) and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(147) If there is no registration, the EA shall generate an error code and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(148) EC requests and EC responses shall be encrypted to ensure confidentiality and signed to ensure authentication and integrity.

4.3.1.5. AT issuance

(149) The C-ITS station shall send an AT request message to the AA, in accordance with [1]. The AA shall send an AT validation request in accordance with [1] to the EA. The EA shall send an AT validation response to the AA. In cases of a positive response, the AA shall generate an AT and send it to the C-ITS station using an AT response message in accordance with [1]. In cases of a negative response, the AA shall generate an error code and send it to the C-ITS station using an AT response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(150) AT requests and AT responses shall be encrypted (only needed for mobile C-ITS stations) to ensure confidentiality and signed to ensure authentication and integrity.

4.3.2. CA's notification to subscriber of issuance of certificates.

Not applicable.

4.4. Certificate acceptance

4.4.1. Conducting certificate acceptance

4.4.1.1. *Root CA*

Not applicable.

4.4.1.2. *TLM*

Not applicable.

4.4.1.3. EA and AA

(151) The EA/AA shall verify the certificate type, the signature and the information in the received certificate. The EA/AA shall discard all EA/AA certificates that are not correctly verified and issue a new request.

4.4.1.4. C-ITS station

(152) The C-ITS station shall verify the EC/AT response received from the EA/AA against its original request, including the signature and the certificate chain. It shall discard all EC/AT responses that are not correctly verified. In such cases, it should send a new EC/AT request.

4.4.2. Publication of the certificate

(153) TLM certificates and their link certificates shall be made available to all participants through the CPOC.

(154) Root CA certificates are published by the CPOC via the ECTL, which is signed by the TLM.

(155) Sub-CAs' (EAs' and AAs') certificates are published by the root CA.

(156) ECs and ATs are not published.

4.4.3. Notification of certificate issuance

There are no notifications of issuance.

4.5. Key pair and certificate usage

*4.5.1. **Private key and certificate usage***

4.5.1.1. Private key and certificate usage for TLM

(157) The TLM shall use its private keys to sign its own (TLM and link) certificates and the ECTL.

(158) The TLM certificate shall be used by PKI participants to verify the ECTL and authenticate the TLM.

4.5.1.2. Private key and certificates usage for root CAs

(159) Root CAs shall use their private keys to sign their own certificates, CRL, link certificates and the EA/AA certificates.

(160) Root CA certificates shall be used by PKI participants to verify the associated AA and EA certificates, link certificates and the CRLs.

4.5.1.3. Private key and certificate usage for EAs and AAs

(161) EAs shall use their private keys to sign ECs and for enrolment request decryption.

(162) EA certificates shall be used to verify the signature of the associated ECs and for EC and AT request encryption by EEs as defined in [1].

(163) AAs shall use their private keys to sign ATs and for AT request decryption.

(164) AA certificates shall be used by EEs to verify associated ATs and for AT request encryption as defined in [1].

4.5.1.4. Private key and certificate usage for end-entity

(165) EEs shall use the private key corresponding to a valid EC to sign a new enrolment request as defined in [1]. The new private key shall be used to build the inner signature in the request to prove possession of the private key corresponding to the new EC public key.

(166) EEs shall use the private key corresponding to a valid EC to sign an authorisation request as defined in [1]. The private key corresponding to the new AT should be used to build the inner signature in the request to prove possession of the private key corresponding to the new AT public key.

(167) EE shall use the private key corresponding to an appropriate AT to sign C-ITS messages as defined in [5].

4.5.2. ***Relying party public key and certificate usage***

(168) Relying parties use the trusted certification path and associated public keys for the purposes referred to in the certificates and to authenticate the trusted common identity of ECs and ATs.

(169) Root CA, EA and AA certificates, ECs and ATs shall not be used without a preliminary check by a relying party.

4.6. Certificate renewal

Not allowed.

4.7. Certificate re-key

4.7.1. Circumstances for certificate re-key

(170) Certificate re-key shall be processed when a certificate reaches the end of its lifetime or a private key reaches the end of operational use, but the trust relation with the CA still exists. A new key pair and the corresponding certificate shall be generated and issued in all cases.

4.7.2. Who may request re-key

4.7.2.1. *Root CA*

(171) The root CA does not request re-key. The re-keying process is an internal process for the root CA, because its certificate is self-signed. The root CA shall re-key either with link certificates or new issuance (see section 4.3.1.1).

4.7.2.2. *TLM*

(172) The TLM does not request re-key. The re-keying process is internal for the TLM, because the TLM certificate is self-signed.

4.7.2.3. EA and AA

(173) The sub-CA's certificate request has to be submitted in due time in order to be sure to have a new sub-CA certificate and operational sub-CA key pair before

expiry of the current private sub-CA key. The date of submission must also take account of the time required for approval.

4.7.2.4. C-ITS station

Not applicable.

4.7.3. Re-keying process

4.7.3.1. TLM certificate

(174) The TLM decides to re-key on the basis of the requirements in sections 6.1 and 7.2. The detailed process is set out in its CPS.

(175) The TLM shall execute the re-keying process in due time in order to allow for the distribution of the new TLM certificate and link certificate to all participants before the current TLM certificate expires.

(176) The TLM shall use link certificates for re-keying and to guarantee the trust relation of the new self-signed certificate. The newly generated TLM and link certificate is transferred to the CPOC.

4.7.3.2. Root CA certificate

(177) The root CA decides to re-key on the basis of the requirements of sections 6.1.5 and 7.2. The detailed process should be defined in its CPS.

(178) The root CA shall execute the re-keying process in due time (before the root CA certificate expires) in order to allow for insertion of the new certificate in the ECTL before the root CA certificate becomes valid (see section 5.6.2). The re-keying process shall be carried out either via link certificates or like an initial request.

4.7.3.3. EA and AA certificates

(179) The EA or AA shall request a new certificate as follows:

Step	Indication	Re-keying request
1	**Key-pair generation**	The sub-CAs (EAs and AAs) shall generate new key pairs in accordance with section 6.1.
2	**Generation of certificate request and inner signature**	The sub-CA generates a certificate request out of the newly generated public key considering the naming scheme (subject_info) of section 3, the signature algorithm, the Service Specific Permissions (SSP) and optional additional parameter, and generates the inner signature with the corresponding new private key. If an encryption key is required, the sub-CA must also prove possession of the corresponding private decryption key.
3	**Generate outer signature**	The whole request shall be signed with the current valid private key to guarantee the authenticity of the signed request.
4	**Send request to root CA**	The signed request shall be submitted to the corresponding root CA.
5	**Verification of request**	The corresponding root CA shall verify the integrity and authenticity of the request. First, it shall check the outer signature. If the verification is positive, it shall check the inner signature. Where there is proof of possession of the private decryption key, it shall also check this proof.
6	**Accept or reject request**	If all checks lead to a positive result, the root CA accepts the request; otherwise, it rejects it.

7	**Generate and issue certificate**	The root CA generates a new certificate and distributes it to the requesting sub-CA.
8	**Send response**	The sub-CA shall send a status message (as to whether or not the certificate was received) to the root CA.

Table 3: Re-keying process for EAs and AAs

(180) During automatic re-keying for sub-CAs, the root CA shall ensure that the requestor is indeed in possession of its private key. Appropriate protocols for proof of possession of private decryption keys shall be applied, for instance as defined in RFC 4210 and 4211. For private signature keys, the inner signature should be used.

4.7.3.4. C-ITS station certificates

Not applicable for AT.

4.8. Certificate modification

Not allowed.

4.9. Certificate revocation and suspension

See section 7

4.10. Certificate status services

4.10.1. Operational characteristics

Not applicable

4.10.2. Service availability

Not applicable

4.10.3. Optional features

Not applicable

4.11. End of subscription

Not applicable

4.12. Key escrow and recovery

4.12.1. Subscriber

4.12.1.1. Which key pair can be escrowed

Not applicable.

4.12.1.2. Who can submit a recovery application

Not applicable.

4.12.1.3. Recovery process and responsibilities

Not applicable.

4.12.1.4. Identification and authentication

Not applicable.

4.12.1.5. Approval or rejection of recovery applications

Not applicable.

4.12.1.6. KEA and KRA actions during key pair recovery

Not applicable.

4.12.1.7. KEA and KRA availability

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

(181) The PKI is composed of the root CA, the EA/AA, the CPOC and the TLM, including their ICT components (e.g. networks and servers).

(182) In this section, the entity responsible for an element of the PKI is identified by the element itself. In other words, the sentence 'the CA is responsible for executing the audit' is equivalent to 'the entity or personnel managing the CA is responsible for executing …'.

(183) The term 'C-ITS trust model elements' includes the root CA, the TLM, the EA/AA, the CPOC and the secure network.

5.1. Physical controls

(184) All C-ITS trust model operations shall be conducted in a physically protected environment that deters, prevents and detects unauthorised use of, access to or disclosure of sensitive information and systems. C-ITS trust model elements shall use physical security controls in compliance with ISO 27001 and ISO 27005.

(185) The entities managing the C-ITS trust model elements shall describe the physical, procedural and personnel security controls in their CPS. In particular, the CPS shall cover information about the site location and construction of the buildings and their physical security controls guaranteeing controlled access to all rooms used in the facility of the C-ITS trust model entities.

5.1.1. Site location and construction

5.1.1.1. Root CA, CPOC, TLM

(186) The location and construction of the facility housing the root CA, CPOC and TLM equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house high-value and sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components' physical areas.

(187) The root CA, CPOC and TLM shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the root CA equipment is installed, so as to guarantee that:

- it is isolated from networks outside the trust model;
- it is separated into a series of (at least two) progressively more secure physical perimeters;
- sensitive data (HSM, key pair backup, activation data, etc.) are stored in a dedicated safe located in a dedicated physical area under multiple access control.

(188) The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

- perimeter alarms, closed-circuit television, reinforced walls and motion detectors;
- two-factor authentication (e.g. smartcard and PIN) for every person and badge to enter and leave the root CA facilities and safe physical secured area.

(189) The root CA, CPOC and TLM use authorised personnel to continually monitor the facility housing equipment on a 7x24x365 basis. The operational environment (e.g. physical facility) shall never be left unattended. The personnel of the operational environment shall never have access to the secure areas of root CAs or sub-CAs unless authorised.

5.1.1.2. *EA/AA*

(190) The same provisions of section 5.1.1.1 apply.

5.1.2. Physical access

5.1.2.1. Root CA, CPOC, TLM

(191) Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall always be protected from unauthorised access. The physical security mechanisms for equipment shall at least:

- monitor, either manually or electronically, for unauthorised intrusion at all times;
- ensure that no unauthorised access to the hardware and activation data is permitted;
- ensure that all removable media and paper containing sensitive plain-text information are stored in a secure container;
- ensure that any individual entering secure areas who is non-authorised on a permanent basis shall not be left without supervision by an authorised employee of the root CA, CPOC and TLM facilities;
- ensure that an access log is maintained and inspected periodically;
- provide at least two layers of progressively increasing security, e.g. at perimeter, building and operational room level;

- require two trusted-role physical access controls for the cryptographic HSM and activation data.

(192) A security check of the facility housing equipment shall be carried out if it is to be left unattended. At a minimum, the check shall verify that:

- the equipment is in a state that is appropriate for the current mode of operation;
- for off-line components, all equipment is shut down;
- any security containers (tamper-proof envelope, safe, etc.) are properly secured;
- physical security systems (e.g. door locks, vent covers, electricity) are functioning properly;
- the area is secured against unauthorised access.

(193) Removable cryptographic modules shall be deactivated prior to storage. When not in use, such modules and the activation data used to access or enable them shall be placed in a safe. Activation data shall either be memorised or recorded and stored in a manner commensurate with the security afforded to the cryptographic module. They shall not be stored with the cryptographic module, so as to avoid only one person having access to the private key.

(194) A person or group of trusted roles shall be made explicitly responsible for making such checks. Where a group of people is responsible, a log shall be maintained that identifies the person performing each check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and confirms that all necessary physical protection mechanisms are in place and activated.

5.1.2.2. *EA/AA*

(195) The same provisions of section 5.1.2.1 apply.

5.1.3. Power and air conditioning

(196) Secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be equipped with reliable access to electric power to ensure operation with no or minor failures. Primary and back-up installations are required in the event of external power failure and smooth shutdown of the C-ITS trust model equipment in the event of a lack of power. C-ITS trust model facilities shall be equipped with heating/ventilation/air-conditioning systems to maintain the temperature and relative humidity of the C-ITS trust model equipment within operational range. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.4. Water exposures

(197) Secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) should be protected in a way that minimises impact from water exposure. For this reason, water and soil pipes shall be avoided. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.5. Fire prevention and protection

(198) To prevent damaging exposure to flame or smoke, the secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be constructed and equipped accordingly and procedures shall be implemented to address fire-related threats. Media storage should be protected against fire in appropriate containers.

(199) C-ITS trust model elements shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorised use of, access to or disclosure of such media. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.6. Media management

(200) Media used in the C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) are securely handled to protect them from damage, theft and unauthorised access. Media management procedures are implemented to protect against obsolescence and deterioration of media in the period for which records have to be retained.

(201) Sensitive data shall be protected against being accessed as a result of re-used storage objects (e.g. deleted files), which may make the sensitive data accessible to unauthorised users.

(202) An inventory of all information assets shall be maintained and requirements set out for the protection of those assets that are consistent with the risk analysis. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.7. Waste disposal

(203) C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall implement procedures for the secure and irreversible disposal of waste (paper, media or any other waste) to prevent the unauthorised use of, access to or disclosure of waste containing confidential/private information. All media used for the storage of sensitive information, such as keys, activation data or files, shall be destroyed before being released for disposal. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.8. Off-site backup

5.1.8.1. Root CA, CPOC and TLM

(204) Full back-ups of root CA, CPOC and TLM components, sufficient to recover from system failure, are made offline after root CA, CPOC and TLM deployment and after each new key-pair generation. Back-up copies of essential business information (key pair and CRL) and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of the business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery). The back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

(205) Backup data are subject to the same access requirements as the operational data. Backup data shall be encrypted and stored offsite. In the event of complete loss of data, the information required for putting the root CA, CPOC and TLM back into operation shall be completely recovered from the backup data.

(206) Private root CA, CPOC and TLM key material shall not be backed up using standard backup mechanisms, but using the backup function of the cryptographic module.

5.1.8.2. *EA/AA*

(207) The processes described in the section 5.1.8.1 apply to this section.

5.2. Procedural controls

This section describes requirements for roles, duties and identification of personnel.

5.2.1. Trusted roles

(208) Employees, contractors and consultants who are assigned to trusted roles shall be considered 'trusted persons'. Persons seeking to become trusted persons for obtaining a trusted position shall meet the screening requirements of this certificate policy.

(209) Trusted persons have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in certificate applications;
- the acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests;
- the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

(210) Trusted roles include, but are not limited to:

- customer service;
- system administration;
- designated engineering;
- executives charged with the management of infrastructural trustworthiness.

(211) The CA shall provide clear descriptions of all trusted roles in its CPS.

5.2.2. Number of persons required per task

(212) C-ITS trust model elements shall establish, maintain and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that multiple trusted persons are required to perform sensitive tasks. The C-ITS trust model elements (TLM, CPOC, root CA, EA and AA) should comply with [4] and with the requirements in the following paragraphs.

(213) Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and the

management of CA cryptographic hardware (HSM) and its associated key material, must require the authorisation of multiple trusted persons.

(214) These internal control procedures shall be designed to ensure that at least two trusted persons are required to have physical or logical access to the device. Restrictions on access to CA cryptographic hardware must be strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3. Identification and authentication for each role

(215) All persons assigned a role, as described in this CP, are identified and authenticated so as to guarantee that the role enables them to perform their PKI duties.

(216) C-ITS trust model elements shall verify and confirm the identity and authorisation of all personnel seeking to become trusted persons before they are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on CA systems.

(217) The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4. Roles requiring separation of duties

(218) Roles requiring separation of duties include (but are not limited to):

- the acceptance, rejection and revocation of requests, and other processing of CA certificate applications;
- the generation, issuing and destruction of a CA certificate.

(219) Segregation of duties may be enforced using PKI equipment, procedures or both. No individual shall be assigned more than one identity unless approved by the root CA.

(220) The part of the root CA and CA concerned with certificate generation and revocation management shall be independent of other organisations for its decisions relating to the establishing, provisioning, maintaining and suspending of services in line with the applicable certificate policies. In particular, its senior executive, senior staff and staff in trusted roles shall be free from any commercial, financial and other pressures that might adversely influence trust in the services it provides.

(221) The EA and AA that serve mobile C-ITS stations shall be separate operational entities, with separate IT infrastructure and IT management teams. In accordance with the GDPR, the EA and AA shall not exchange any personal data, except for the authorisation of AT requests. They shall transfer data relating to the approval of AT requests only using the authorisation validation protocol of [1] over a dedicated secure interface. Other protocols may be used, provided that [1] is implemented.

(222) The logfiles stored by the EA and AA may be used solely for the purpose of revoking misbehaving ECs based on ATs in intercepted malicious CAM/DENM messages. After a CAM/DENM message has been identified as malicious, the AA will look up the AT's verification key in its issuance logs and submit a revocation request to the EA containing the encrypted signature under the EC private key that was used during the issuance of the AT. All logfiles must be adequately protected against access by unauthorised parties and may not be shared with other entities or authorities.

Note: At the time of drafting this version of the CP, the design of the misbehaving function is not defined. It is planned to potentially design the misbehaving function in future revisions of the policy.

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements

(223) C-ITS trust model elements employ a sufficient number of personnel with the expert knowledge, experience and qualifications necessary for the job functions and services offered. PKI personnel fulfil those requirements through formal training and credentials, actual experience or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and privileges, and position sensitivity is determined on the basis of duties and access levels, background screening, and employee training and awareness.

5.3.2. Background check procedures

(224) C-ITS trust model elements shall conduct background checks on personnel seeking to become trusted persons. Background checks shall be repeated for personnel holding trusted positions at least every five years.

(225) The factors revealed in a background check that may be considered grounds for rejecting candidates for trusted positions or for taking action against an existing trusted person include (but are not limited to) the following:

- misrepresentations made by the candidate or trusted person;
- highly unfavourable or unreliable professional references;
- certain criminal convictions;
- indications of a lack of financial responsibility.

(226) Reports containing such information shall be evaluated by human resources personnel, who shall take reasonable action in the light of the type, magnitude and frequency of the behaviour uncovered by the background check. Such action may include measures up to and including cancelling offers of employment made to candidates for trusted positions or terminating the employment of existing trusted persons. The use of information revealed in a background check as a basis for such action shall be subject to applicable law.

(227) Background investigation of persons seeking to become a trusted person includes but is not limited to:

- confirmation of previous employment;

- a check of professional references covering their employment over a period of at least five years;
- a confirmation of the highest or most relevant educational degree obtained;
- a search of criminal records.

5.3.3. Training requirements

(228) C-ITS trust model elements shall provide their personnel with the requisite training to fulfil their responsibilities relating to CA operations competently and satisfactorily.

(229) Training programmes shall be reviewed periodically and their training shall address matters that are relevant to functions performed by their personnel.

(230) Training programmes shall address matters that are relevant to the particular environment of the trainee, including:

- security principles and mechanisms of the C-ITS trust model elements;
- hardware and software versions in use
- all duties the person is expected to perform, and internal and external reporting processes and sequences;
- PKI business processes and workflows;
- incident and compromise reporting and handling;
- disaster recovery and business continuity procedures;
- sufficient IT knowledge.

5.3.4. Retraining frequency and requirements

(231) The persons assigned to trusted roles are required to refresh the knowledge they have gained from training on an ongoing basis using a training environment. Training must be repeated whenever deemed necessary and at least every two years.

(232) C-ITS trust model elements shall provide their staff with refresher training and updates to the extent and with the frequency required to ensure that they maintain the required level of proficiency to fulfil their job responsibilities competently and satisfactorily.

(233) Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan and the execution of that plan shall be documented.

5.3.5. Job rotation frequency and sequence

(234) No stipulation as long as the technical skills, experience and access rights are ensured. The administrators of the C-ITS trust model elements shall ensure that changes in staff do not affect the security of the system.

5.3.6. Sanctions for unauthorised actions

(235) Each C-ITS trust model elements must develop a formal disciplinary process to ensure that unauthorised actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges must be withdrawn.

5.3.7. Independent contractor requirements

(236) C-ITS trust model elements may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and on condition that the entity trusts the contractors or consultants to the same extent as if they were employees and that they fulfil the requirements applicable to employees.

(237) Otherwise, independent contractors and consultants shall have access to C-ITS PKI secure facilities only if escorted and directly supervised by trusted persons.

5.3.8. Documentation supplied to personnel

(238) C-ITS trust model elements shall provide their personnel with requisite training and access to the documentation they need to fulfil their job responsibilities competently and satisfactorily.

5.4. Audit logging procedures

(239) This section sets out requirements as regards the types of event to be recorded and the management of audit logs.

5.4.1. Types of event to be recorded and reported by each CA

(240) A CA representative shall regularly review the CA logs, events and procedures.

(241) C-ITS trust model elements shall record the following types of audit event (if applicable):

- physical facility access – access by physical persons to the facilities will be recorded by storing the access requests through smartcards. An event will be created every time a record is created;
- trusted roles management – any change in the definition and level of access of the different roles will be recorded, including modification of the attributes of the roles. An event will be created every time a record is created;
- logical access – an event will be generated when an entity (e.g. a program) has access to sensitive areas (i.e. networks and servers);
- backup management – an event is created every time a backup is completed, either successfully or unsuccessfully;
- log management – logs will be stored. An event is created when the log size exceeds a specific size;
- data from the authentication process for subscribers and C-ITS trust model elements – events will be generated for every authentication request by subscribers and C-ITS trust model elements;
- acceptance and rejection of certificate requests, including certificate creation and renewal – an event will be generated periodically with a list of accepted and rejected certificate requests in the previous seven days;
- manufacturer registration – an event will be created when a manufacturer is registered;
- C-ITS station registration – an event will be created when a C-ITS station is registered;

- HSM management – an event will be created when an HSM security breach is recorded;
- IT and network management, as they pertain to the PKI systems – an event will be created when a PKI server is shut down or restarted;
- security management (successful and unsuccessful PKI system access attempts, PKI and security system actions performed, security profile changes, system crashes, hardware failures and other anomalies, firewall and router activities; and entries to and exits from the PKI facilities);
- event-related data will be stored for at least five years unless additional national rules apply.

(242) In accordance with the GDPR, the audit logs shall not permit access to privacy-related data concerning C-ITS station private vehicles.

(243) Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

(244) Each event related to certificate life-cycle is logged in such a way that it can be attributed to the person that performed it. All data relating to a personal identity are encrypted and protected against non-authorised access.

(245) At a minimum, each audit record includes the following (recorded automatically or manually for each auditable event):

- type of event (as from the list above);
- trusted date and time the event occurred;
- result of the event – success or failure where appropriate;
- identity of the entity and/or operator that caused the event if applicable;
- identity of the entity for which the event is addressed.

5.4.2. Frequency of processing log

(246) Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the CA systems and in addition periodically every year.

(247) Audit-log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit-log summary. Audit-log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries and an investigation of any alerts or irregularities in the logs. Action taken on the basis of audit-log reviews shall be documented.

(248) The audit log is archived at least weekly. An administrator shall archive it manually if the free disk space for audit log is below the expected amount of audit-log data produced that week.

5.4.3. Retention period for audit log

(249) Log records relating to certificate life-cycles are kept for at least five years after the corresponding certificate expires.

5.4.4. Protection of audit log

(250) The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Internal audit logs may be accessed only by administrators; certificate life-cycle related audit logs may also be accessed by users with the appropriate authorisation via a web page with user login. Access has to be granted with multi-user (at least two-user) and at least two-level authentication. It must be technically ensured that users cannot access their own log files.

(251) Each log entries shall be signed using key material from HSM.

(252) Event logs containing information that can lead to personal identification, such as a private vehicle, are encrypted in such a way that only authorised persons can read them.

(253) Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the period for which the logs have to be held.

(254) Event logs are protected in such a way as to remain readable for the duration of their storage period.

5.4.5. Audit log backup procedures

(255) Audit logs and summaries are backed up via enterprise backup mechanisms, under the control of authorised trusted roles, separated from their component source generation. Audit-log backups are protected with the same level of trust that applies to the original logs.

5.4.6. Audit collection system (internal or external)

(256) The equipment of the C-ITS trust model elements shall activate the audit processes at system startup and deactivate them only at system shutdown. If audit processes are not available, the C-ITS trust model element shall suspend its operation.

(257) At the end of each operating period and at the re-keying of certificates, the collective status of equipment should be reported to the operations manager and operation governing body of the respective PKI element.

5.4.7. Notification to event-causing subject

(258) Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.8. Vulnerability assessment

(259) The role in charge of conducting audit and roles in charge of realising PKI system operation in the C-ITS trust model elements explain all significant events in an audit-log summary. Such reviews involve verifying that the log has not been tampered with and that there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken as a result of these reviews is documented.

(260) C-ITS trust model elements shall:

- implement organisational and/or technical detection and prevention controls under the control of the C-ITS trust model elements to protect PKI systems against viruses and malicious software;
- document and follow a vulnerability correction process that addresses the identification, review, response and remediation of vulnerabilities;
- undergo or perform a vulnerability scan:
  - after any system or network changes determined by the C-ITS trust model elements as significant for PKI components; and
  - at least once a month, on public and private IP addresses identified by the CA, CPOC as the PKI's systems,
- undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications determined by the C-ITS trust model elements as significant for CA's PKI component;
- for online systems, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable vulnerability or penetration test;
- track and remediate vulnerabilities in line with enterprise cybersecurity policies and risk mitigation methodology.

5.5. Record archiving

5.5.1. Types of record archived

(261) C-ITS trust model elements shall archive records detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following PKI events records shall be archived (if applicable):

- physical facility access log of C-ITS trust model elements (minimum one year);
- trusted roles management log for C-ITS trust model elements (minimum 10 years);
- IT access log for C-ITS trust model elements (minimum five years);
- CA key creation, use and destruction log (minimum five years) (not for TLM and CPOC);
- certificate creation, use and destruction log (minimum two years);
- CPA request log (minimum two years);
- activation data management log for C-ITS trust model elements (minimum five years);
- IT and network log for C-ITS trust model elements (minimum five years);

- PKI documentation for C-ITS trust model elements (minimum five years);
- security incident and audit report for C-ITS trust model elements (minimum 10 years);
- system equipment, software and configuration (minimum five years).

(262) The C-ITS trust model elements shall retain the following documentation relating to certificate requests and the verification thereof, and all TLM, root CAs and CA certificates and CRL thereof, for at least seven years after any certificate based on that documentation ceases to be valid:

- PKI audit documentation kept by C-ITS trust model elements;
- CPS documents kept by C-ITS trust model elements;
- contract between CPA and other entities kept by C-ITS trust model elements;
- certificates (or other revocation information) kept by CA and TLM;
- certificate request records in root CA system (not applicable to the TLM);
- other data or applications sufficient to verify archive contents;
- all work related to or from the C-ITS trust model elements and compliance auditors.

(263) The CA entity shall retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years after any certificate based on that documentation ceases to be valid.

5.5.2. Retention period for archive

(264) Without prejudice to regulations requiring a longer archival period, C-ITS trust model elements shall keep all records for at least five years after the corresponding certificate has expired.

5.5.3. Protection of archive

(265) C-ITS trust model elements shall store the archive of records in a safe, secure storage facility separate from the CA equipment, with physical and procedural security controls equivalent to or better than those of the PKI.

(266) The archive shall be protected against unauthorised viewing, modification, deletion or other tampering by storage in a trustworthy system.

(267) The media holding the archive data and the applications required to process them shall be maintained to ensure that they can be accessed for the period set in this CP.

5.5.4. System archive and storage

(268) C-ITS trust model elements shall incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an offsite secure facility.

5.5.5. Requirements for time-stamping of records

(269) C-ITS trust model elements managing a revocation database shall ensure that the records contain information as to the time and date when revocation records are created. The integrity of such information will be implemented with cryptographic-based solutions.

5.5.6. Archive collection system (internal or external)

(270) The archive collection system is internal.

5.5.7. Procedures to obtain and verify archive information

(271) All C-ITS trust model elements shall allow only authorised trusted persons to access the archive. Root CAs and CAs shall describe the procedures for creating, verifying, packaging, transmitting and storing archive information in the CPS.

(272) Root CA and CA equipment shall verify the integrity of the information before it is restored.

5.6. Key changeover for C-ITS trust model elements

(273) The following elements of the C-ITS trust model have specific requirements for their key changeover: TLM, root CA and EA/AA certificates.

*5.6.1. **TLM***

(274) The TLM shall delete its private key on expiry of the corresponding certificate. It shall generate a new key pair and corresponding TLM certificate before deactivation of the current valid private key. It shall take care that the new (link) certificate is inserted in the ECTL in time to be distributed to all C-ITS stations before it becomes valid. The link certificate and the new self-signed certificate are transferred to the CPOC.

5.6.2. Root CA

(275) The root CA shall deactivate and delete the current private key (including backup keys), so that it will not issue EA/AA certificates with a validity that extends beyond the validity of the root CA certificate.

(276) The root CA shall generate a new key pair and corresponding root CA and link certificate before deactivation of the current private key (including backup keys) and send it to the TLM for insertion into the ECTL. The validity period of the new root CA certificate shall start at the planned deactivation of the current private key. The root CA shall take care that the new certificate is inserted in the ECTL in time to be distributed to all C-ITS stations before it becomes valid.

(277) The root CA shall activate the new private key when the corresponding root CA certificate becomes valid.

5.6.3. EA/AA certificate

(278) The EA/AA shall deactivate the current private key so that it will not issue ECs/ATs with a validity that extends beyond the validity of the EA/AA certificate.

(279) The EA/AA shall generate a new key pair and request a corresponding EA/AA certificate before deactivation of the current private key. The validity period of

the new EA/AA certificate shall start at the planned deactivation of the current private key. The EA/AA shall take care that the new certificate can be published in time to be distributed to all C-ITS stations before it becomes valid.

(280) The EA/AA shall activate the new private key when the corresponding EA/AA certificate becomes valid.

5.6.4. Auditor

No provisions.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling

(281) C-ITS trust model elements shall monitor their equipment on an ongoing basis, so as to detect potential hacking attempts or other forms of compromise. In such an event, they shall investigate in order to determine nature and degree of damage.

(282) If the personnel responsible for the management of the root CA or TLM detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and the degree of damage. In the event of the private key being compromised, the root CA certificate shall be revoked. The IT security experts of the CPA shall assess the scope of potential damage in order to determine whether the PKI needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI has been compromised. In addition, the CPA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the CPA business continuity plan.

(283) Incident, compromise and business continuity are covered in the CPS, which may also rely on other enterprise resources and plans for its implementation.

(284) If the personnel responsible for the management of the EA/AA/CPOC detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and degree of damage. The personnel responsible for the management of the CA or the CPOC entity shall assess the scope of potential damage in order to determine whether the PKI component needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI component has been compromised. In addition, the sub-CA entity determines which services are to be maintained and how, in accordance with the sub-CA entity business continuity plan. In the event of a PKI component being compromised, the CA entity shall alert its own root CA and the TLM through the CPOC.

(285) Incident, compromise and business continuity are covered in the CPS of the root CA or the TLM or other relevant documents in the case of the CPOC, which may also rely on other enterprise resources and plans for their implementation.

(286) The root CA and CA shall alert, with precise information on the consequences of the incident, each Member State representative and root CA with which they have an agreement in the C-ITS context, in order to allow them to activate their own incident management plan.

5.7.2. Corruption of computing resources, software and/or data

(287) If a disaster is discovered that prevents the proper operation of a C-ITS trust model element, that element shall suspend its operation and investigate whether the private key has been compromised (except CPOC). Defective hardware shall be replaced as quickly as possible and the procedures described in sections 5.7.3 and 5.7.4 shall apply.

(288) The corruption of computing resources, software and/or data shall be reported to the root CA within 24 hours for the highest levels of risk. All other events must be included in the periodic report of the root CA, EAs and AAs.

5.7.3. Entity private key compromise procedures

(289) If the private key of a root CA is compromised, lost, destroyed or suspected of being compromised, the root CA shall:

- suspend its operation;
- start the disaster recovery and migration plan;
- revoke its root CA certificate;
- investigate the 'key issue' that generated the compromise and notify the CPA, which will revoke the root-CA certificate through the TLM (see section 7);
- alert all subscribers with which it has an agreement.

(290) If an EA/AA's key is compromised, lost, destroyed or suspected of being compromised, the EA/AA shall:

- suspend its operation;
- revoke its own certificate;
- investigate the 'key issue' and notify the root CA;
- alert subscribers with which an agreement exists.

(291) If a C-ITS station EC or AT key is compromised, lost, destroyed or suspected of being compromised, the EA/AA to which the C-ITS station is subscribed shall:

- revoke the EC of the affected ITS;
- investigate the 'key issue' and notify the root CA;
- alert subscribers with which it has an agreement.

(292) Where any of the algorithms or associated parameters used by the root CA and/or CA or C-ITS stations becomes insufficient for its remaining intended usage, the CPA (with a recommendation from cryptographic experts) shall inform the root CA entity with which it has an agreement and change the algorithms used. (For details, see section 6 and the CPSs of the root CA and sub-CA).

5.7.4. Business continuity capabilities after a disaster

(293) The C-ITS trust model elements operating secure facilities for CA operations shall develop, test, maintain and implement a disaster recovery plan designed

to mitigate the effects of any natural or man-made disaster. Such plans address the restoration of information systems services and key business functions.

(294) After an incident of a certain risk level, the compromised CA must be re-audited by an accredited PKI auditor (see section 8).

(295) Where the compromised CA is unable to operate any longer (e.g. following a severe incident), a migration plan must be drawn up for the transfer of its functions to another root CA. At least the EU root CA shall be available to support the migration plan. The compromised CA shall cease its functions.

(296) The root CAs shall include the disaster recovery plan and the migration plan in the CPS.

5.8. Termination and transfer

*5.8.1. **TLM***

(297) The TLM shall not terminate its operation, but an entity managing the TLM may take over another entity.

(298) In the event of the managing entity changing:

- it shall request the CPA's approval for a change of TLM management from the old entity to the new entity;
- the CPA shall approve the change of TLM management;
- all audit logs and archived records shall be transferred from the old management entity to the new entity.

5.8.2. Root CA

(299) The root CA shall not terminate/start its operation without establishing a migration plan (set out in the relevant CPS) that guarantees ongoing operation for all subscribers.

(300) In the event of the termination of the root CA service, the root CA shall:

- notify the CPA;
- notify the TLM so that it can delete the root CA certificate from the ECTL;
- revoke the corresponding root CA by issuing a CRL containing itself;
- alert root CAs with which it has an agreement for the renewal of EA/AA certificates;
- destroy the root CA private key;
- communicate last revocation status information (CRL signed by root CA) to the relying party, indicating clearly that it is the latest revocation information;
- archive all audit logs and other records prior to termination of the PKI;
- transfer archived records to an appropriate authority.

(301) The TLM shall delete the corresponding root CA certificate from the ECTL.

5.8.3. ***EA/AA***

(302) In the event of the termination of the EA/AA service, the EA/AA entity provides notice prior to the termination. An EA or AA shall not terminate/start its operation without establishing a migration plan (set out in the relevant CPS) that guarantees ongoing operation for all subscribers. The EA/AA shall:

- inform the root CA by registered letter;
- destroy the CA private key;
- transfer its database to the entity appointed by the root CA;
- stop issuing certificates;
- during the transfer of its database and until the database is fully operational in a new entity, maintain capability to authorise requests from the responsible privacy authority;
- where a sub-CA has been compromised, the root CA shall revoke the sub-CA and issue a new CRL with a list of revoked sub-CAs;
- archive all audit logs and other records prior to terminating the PKI;
- transfer archived records to an entity designated by the root CA.

(303) In the event of termination of the CA's services, the CA shall be responsible for keeping all relevant records regarding the needs of CA and PKI components.

6. TECHNICAL SECURITY CONTROLS

6.1. Key-pair generation and installation

6.1.1. TLM, root CA, EA, AA

(304) The key-pair generation process shall fulfil the following requirements:

- each participant shall be able to generate its own key pairs in accordance with sections 6.1.4 and 6.1.5;
- the process of deriving symmetric encryption keys and a MAC key for certificate requests (ECIES) shall be carried out in line with [1] and [5];
- the key-generation process shall use the algorithms and key lengths described in sections 6.1.4.1 and 6.1.4.2;
- the key-pair generation process shall be subject to the requirements of 'secure storing of private keys' (see section 6.1.5);
- the root CAs and their subscribers (sub-CAs) shall ensure that the integrity and authenticity of their public keys and any associated parameters are maintained during distribution to sub-CA registered entities.

6.1.2. EE — mobile C-ITS station

(305) Each mobile C-ITS station shall generate its own key pairs in accordance with sections 6.1.4 and 6.1.5.

(306) The process of deriving symmetric encryption keys and a MAC key for certificate requests (ECIES) shall be carried out in accordance with [1] and [5].

(307) The key-generation processes shall use the algorithms and key lengths described in sections 6.1.4.1 and 6.1.4.2.

(308) The key-pair generation processes shall be subject to the requirements of 'secure storing of private keys' (see section 6.1.5).

6.1.3. EE — fixed C-ITS station

(309) Each fixed C-ITS station shall generate its own key pair in accordance with sections 6.1.4 and 6.1.5.

(310) The key-generation processes shall use the algorithms and key lengths described in section 6.1.4.1 and 6.1.4.2.

(311) The key-pair generation processes shall be subject to the requirements of 'secure storing of private keys' (see section 6.1.5).

6.1.4. Cryptographic requirements

(312) All PKI participants shall satisfy the cryptographic requirements set out in the following paragraphs as regards signature algorithm, key length, random number generator and link certificates.

6.1.4.1. *Algorithm and key length - signature algorithms*

(313) All PKI participants (TLM, root CA, EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key for signing operations with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 4.

(314) All PKI participants that must check the integrity of the ECTL, certificates and/or signed messages in accordance with their role, as defined in section 1.3.6, shall support the corresponding algorithms listed in Table 5 for verification. In particular, C-ITS stations shall be able to check the integrity of the ECTL.

	TLM	root CA	EA	AA	C-ITS station
ECDSA_nistP256_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
X indicates mandatory support					

Table 4: Generating key pairs and use of private key for signing operations

	TLM	root CA	EA	AA	C-ITS station
ECDSA_nistP256_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
X indicates mandatory support					

Table 5: Verification overview

(315) If the CPA so decides on the basis of newly found cryptographic weaknesses, all C-ITS stations shall be able to switch to one of the two algorithms (ECDSA_nistP256_with_SHA 256 or ECDSA_brainpoolP256_with_SHA 256) as soon as possible. The actual algorithm(s) that is/are used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

6.1.4.2. *Algorithm and key length - encryption algorithms for enrolment and authorisation*

(316) All PKI participants (EA, AA and C-ITS stations) shall be able to use public keys to encrypt enrolment and authorisation requests/responses with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 6. The actual algorithm(s) that is/are used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

(317) The named algorithms in Table 6 indicate the key length and hash algorithm length and shall be implemented in accordance with [5].

	TLM	root CA	EA	AA	C-ITS station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indicates mandatory support					

Table 6: Use of public keys for encryption of enrolment and authorisation requests/responses

(318) All PKI participants (EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key to decrypt enrolment and authorisation requests/responses with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 7:

	TLM	root CA	EA	AA	C-ITS station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indicates mandatory support					

Table 7: Generate key pairs and use of private key for the decryption of enrolment and authorisation requests/responses

6.1.4.3. *Crypto-agility*

(319) Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. The CPA shall monitor the need for such changes in the light of actual vulnerabilities and state-of-the-art cryptography. It will draft, approve and publish an update of this certificate policy if it decides that the cryptographic algorithms should be updated. Where a new issue of this CP signals a change of algorithm and/or key length, the CPA will adopt a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported.

(320) In order to enable and facilitate the transfer to new algorithms and/or key lengths, it is recommended that all PKI participants implement hardware and/or software that is capable of a changeover of key lengths and algorithms.

(321) Changes of root and TLM certificates shall be supported and executed with the help of link certificates (see section 4.6) that are used to cover the transition period between the old and new root certificates (‘migration of the trust model’).

6.1.5. Secure storing of private keys

This section describes the requirements for the secure storage and generation of key pairs and random numbers for CAs and end-entities. These requirements are defined for cryptographic modules and described in the following sub-sections.

6.1.5.1. *Root CA, sub-CA and TLM level*

(322) A cryptographic module shall be used for:

- generating, using, administering and storing private keys;
- generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification);
- creating backups of private keys in accordance with section 6.1.6;
- deletion of private keys.

The cryptographic module shall be certified with one of the following protection profiles (PPs), with assurance level EAL-4 or higher:

- PPs for HSMs:
  - CEN EN 419 221-2: Protection profiles for TSP cryptographic modules – Part 2: Cryptographic module for CSP signing operations with backup;
  - CEN EN 419 221-4: Protection profiles for TSP cryptographic modules – Part 4: Cryptographic module for CSP signing operations without backup;
  - CEN EN 419 221-5: Protection profiles for TSP cryptographic modules – Part 5: Cryptographic module for trust services;
- PPs for smartcards:
  - CEN EN 419 211-2: Protection profiles for secure signature creation device – Part 2: Device with key generation;
  - CEN EN 419 211-3: Protection profiles for secure signature creation device — Part 3: Device with key import.

Manual access to the cryptographic module shall require two-factor authentication from the administrator. In addition, this shall require the involvement of two authorised persons.

The implementation of a cryptographic module shall ensure that keys are not accessible outside the cryptographic module. The cryptographic module shall include an access control mechanism to prevent unauthorised use of private keys.

6.1.5.2. *End-entity*

(323) A cryptographic module for EEs shall be used for:

- generating, using, administering and storing private keys;
- generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification);
- secure deletion of a private key.

(324) The cryptographic module shall be protected against unauthorised removal, replacement and modification. All PPs and related documents applicable for the security certification of the cryptographic module shall be evaluated, validated and certified in accordance with ISO 15408, applying the Mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS), or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity framework.

(325) Given the importance of maintaining the highest possible security level, security certificates for the cryptographic module shall be issued under the common criteria certification scheme (ISO 15408) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS Agreement, or issued by a conformity assessment body accredited by a

national cybersecurity certification authority of a Member State. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

Note: the link between the cryptographic module and the C-ITS station shall be protected.

6.1.6. Backup of private keys

(326) The generation, storage and use of backups of private keys shall fulfil the requirements of at least the security level required for the original keys.

(327) Backups of private keys shall be made by root CAs, EAs and AAs.

(328) Backups of private keys shall not be made for ECs and ATs.

6.1.7. Destruction of private keys

(329) The root CAs, EAs, AAs, and mobile and fixed C-ITS stations shall destroy their private key and any corresponding backups, if a new key pair and corresponding certificate has been generated and successfully installed, and the overlap time (if any — CA only) has passed. The private key shall be destroyed using the mechanism offered by the cryptographic module used for the key storage or as described in the corresponding PP as referred to in section 6.1.5.2.

6.2. Activation data

(330) Activation data refer to authentication factors required to operate cryptographic modules to prevent unauthorised access. The usage of the activation data of a CA's cryptographic device shall require action by two authorised persons.

6.3. Computer security controls

(331) The CAs' computer security controls shall be designed in accordance with the high security level by adhering to the requirements of ISO/IEC 27002.

6.4. Life-cycle technical controls

(332) The CA's technical controls shall cover the whole life-cycle of the CA. In particular, this includes the requirements of section 6.1.4.3 ('Crypto-agility').

6.5. Network security controls

(333) The networks of the CAs (root CA, EA and AA) shall be hardened against attacks in line with the requirements and implementation guidance of ISO/IEC 27001 and ISO/IEC 27002.

(334) The availability of the CA's networks shall be designed in the light of the estimated traffic.

7. CERTIFICATE PROFILES, CRL AND CTL

7.1. Certificate profile

(335) The certificate profiles defined in [5] shall be used for the TLM, root certificates, EA certificates, AA certificates, ATs and ECs. National governmental EAs may use other certificate profiles for ECs.

(336) Root CA, EA and AA certificates shall indicate the permissions for which these CAs (root CAs, EA and AA) are allowed to issue certificates.

(337) On the basis of [5]:

- each root CA shall use its own signing private key to issue CRLs;
- the TLM shall use its own signing private key to issue the ECTL.

7.2. Certificate validity

(338) All C-ITS certificate profiles shall include an issue and an expiry date, which represent the validity time of the certificate. At each PKI level, certificates shall be generated in good time before expiry.

(339) The validity time of CA and EC certificates shall include an overlap time. TLM and root CA certificates shall be issued and put on the ECTL a maximum of three months and at least one month before their validity starts based on the start time in the certificate. This preloading phase is required to safely distribute the certificates to all correspondent relying parties in accordance with section 2.2. This ensures that, from the beginning of the overlap time, all relying parties are already able to verify messages issued with a new certificate.

(340) At the beginning of the overlap time, the successive CA, EC and AT certificates shall be issued (if applicable), distributed to and installed by the correspondent relying parties. During the overlap time, the current certificate shall be used only for verification.

(341) As the validity periods listed in Table 8 must not exceed the validity period of the superior certificate, the following restrictions apply:

- maximumvalidity(Root CA) = privatekeyusage(Root CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);
- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

(342) The validity of (Root and TLM) link certificates starts at the corresponding private key usage and ends at the maximum validity time of the root CA or TLM.

(343) Table 8 shows the maximum validity time for C-ITS CA certificates (for AT validity periods, see section 7.2.1).

Entity	Max. private key usage period	Maximum validity time
Root CA	3 years	8 years
EA	2 years	5 years
AA	4 years	5 years
EC	3 years	3 years
TLM	3 years	4 years

Table 8: Validity periods of the certificates in the C-ITS trust model

7.2.1. Pseudonym certificates

(344) In this context, pseudonyms are implemented by ATs. As a consequence, this section refers to ATs rather than pseudonyms.

(345) The requirements set out in this section apply only to ATs of mobile C-ITS stations sending CAM and DENM messages, where the risk of location privacy is applicable. No specific requirements on AT certificates apply to ATs for fixed C-ITS stations and mobile C-ITS stations used for special functions where location privacy is not applicable (e.g. marked emergency and law-enforcement vehicles).

(346) The following definitions shall apply:

- 'validity period for ATs' – the period for which an AT is valid, i.e. the period between the AT's starting date and its expiry date;
- 'preloading period for ATs' – preloading is the possibility for C-ITS stations to obtain ATs before the validity period starts. The preloading period is the maximum allowed time period from the request of ATs to the latest end of validity date of any requested AT;
- 'usage period for ATs' – the period during which an AT is effectively used to sign CAM/DENM messages;
- 'maximum number of parallel ATs' – the number of ATs from which a C-ITS station can choose at any given time when signing a CAM/DENM message, i.e. the number of different ATs issued to one C-ITS station that are valid at the same time.

(347) The following requirements shall apply:

- the preloading period for ATs shall not exceed three months;
- the validity period for ATs shall not exceed one week;
- the maximum number of parallel ATs shall not exceed 100 per C-ITS station;
- the usage period of an AT depends on the AT change strategy and the amount of time that a vehicle is in operation, but is limited by the maximum number of parallel ATs and the validity period. More specifically, the average usage period for one C-ITS station is at least the operational time of the vehicle during one validity period divided by the maximum number of parallel ATs.

7.2.2. Authorisation tickets for fixed C-ITS stations

(348) The definitions in section 7.2.1 and the following requirements apply:

- the preloading period for ATs shall not exceed three months;
- the maximum number of parallel ATs shall not exceed two per C-ITS station.

7.3. Revocation of certificates

7.3.1. Revocation of CA, EA and AA certificates

Root CA, EA and AA certificates shall be revocable. Revoked certificates of root CAs, EAs and AAs shall be published on a CRL as soon as possible and without

undue delay. This CRL shall be signed by its corresponding root CA and use the profile described in section 7.4. For revocation of root CA certificates, the corresponding root CA issues a CRL containing itself. In addition, in cases of a security compromise, section 5.7.3 applies. In addition the TLM shall remove revoked root CAs from the trust list and issue a new trust list. Expired certificates shall be removed from the corresponding CRL and trust list.

(349) Certificates are revoked where:

- the root CAs have reason to believe or strongly suspect that the corresponding private key have been compromised;
- the root CAs have been notified that the contract with the subscriber has been terminated;
- information (such as name and associations between CA and subject) in the certificate is incorrect or has changed;
- a security incident takes place that affects the certificate owner;
- an audit (see section 8) leads to a negative result.

(350) Subscriber shall immediately notify the CA of a known or suspected compromise of their private key. It must be assured that only authenticated requests result in revoked certificates.

7.3.2. Revocation of enrolment credentials

(351) Revocation of ECs may be initiated by the C-ITS station subscriber (flow 34) and shall be implemented by an internal blacklist in a revocation database with a timestamp, which is generated and maintained by each EA. The blacklist is never published and shall be kept confidential and used only by the corresponding EA to verify the validity of the corresponding ECs in the context of requests for ATs and new ECs.

7.3.3. Revocation of authorisation tickets

(352) As ATs are not revoked by the corresponding CAs, they shall have a short lifetime and cannot be issued too far in advance of becoming valid. The permissible certificate life-cycle parameter values are set out in section 7.2.

7.4. Certificate revocation list

(353) The format and content of the CRL issued by root CAs shall be as laid down in [1].

7.5. European certificate trust list

(354) The format and content of the ECTL issued by the TLM shall be as laid down in [1].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Topics covered by audit and audit basis

(355) The purpose of a compliance audit is to verify that the TLM, root CAs, EAs and AAs operate in accordance with this CP. The TLM, root CAs, EAs and AAs shall select an independent acting and accredited PKI auditor to audit their CPS. The audit shall be combined with an ISO/IEC 27001 and ISO/IEC 27002 assessment.

(356) A compliance audit is ordered by a root CA (flow 13) for the root CA itself, and for a sub-CA by its subordinate EA/AA.

(357) A compliance audit for the TLM is ordered by the CPA (flow 38).

(358) When requested, an accredited PKI auditor shall perform a compliance audit on one of the following levels:

(1) conformity of the TLM's, root CA's, EA's or AA's CPS with this CP;

(2) conformity of the TLM's, root CA's, EA's or AA's intended practices with its CPS prior to operation;

(3) conformity of the TLM's, root CA's, EA's or AA's practices and operational activities with its CPS during operation.

(359) The audit shall cover all requirements of this CP to be fulfilled by the TLM, root CAs, EAs and AAs to be audited. It shall also cover the operation of the CA in the C-ITS PKI, including all processes mentioned in its CPS, the premises and responsible persons.

(360) The accredited PKI auditor shall provide a detailed report of the audit to the root CA (flow 36), EA, AA or CPA (flow 16 and 40), as applicable.

8.2. Frequency of the audits

(361) A root CA, TLM, EA or AA shall order a compliance audit of itself from an independent and accredited PKI auditor in the following cases:

- at its first setting-up (levels 1 and 2 compliance);
- at every change of the CP. The CPA shall define the CP change content and time-plan of deployment and determine the needs for audits (including the necessary compliance level) accordingly;
- at every change of its CPS (levels 1, 2 and 3 compliance). Since the managing entities of root CAs, the TLM and EAs/AAs decide what implementation changes follow the update of their CPS, they shall order a compliance audit before implementing those changes. In cases of only minor changes of the CPS (e.g. of an editorial nature), the managing entity may send the CPA a duly justified request for its approval to skip level 1, 2 or 3 compliance audits;
- regularly, and at least every three years during its operation (level 3 compliance).

8.3. Identity/qualifications of auditor

(362) The CA to be audited shall select an independently acting and accredited company/organisation ('auditing body') or accredited PKI auditors to audit it in accordance with this CP. The auditing body shall be accredited and certified by a member of European Accreditation[1].

8.4. Auditor's relationship to audited entity

(363) The accredited PKI auditor shall be independent of the audited entity.

[1] Members of the European Accreditation Body are listed at: http://www.european-accreditation.org/ea-members

8.5. Action taken as a result of deficiency

(364) Where an audit report finds the TLM to be non-compliant, the CPA shall order the TLM to take immediate preventive/corrective action.

(365) Where a root CA with a non-compliant audit report makes a new application, the CPA shall reject the application and send a corresponding rejection to the root CA (flow 4). In such cases, the root CA will be suspended. It must take corrective action, re-order the audit and make a new request for CPA approval. The root CA shall not be allowed to issue certificates during the suspension.

(366) In cases of a regular root CA audit or a change to a root CA's CPS, and depending on the nature of the non-compliance described in the audit report, the CPA may decide to revoke the root CA and communicate this decision to the TLM (flow 2), causing the deletion of the root CA certificate from the ECTL and insertion of the root CA on the CRL. The CPA shall send a corresponding rejection to the root CA (flow 4). The root CA must take corrective action, re-order a full audit (level 1 to 3) and make a new request for CPA approval. Alternatively, the CPA may decide not to revoke the root CA, but to give it a grace period in which the root CA shall take corrective action, re-order an audit and re-submit the audit report to the CPA. In this case, the root CA operation must be suspended and it is not allowed to issue certificates and CRLs.

(367) In case of an EA/AA audit, the root CA shall decide whether or not to accept the report. Depending on the audit result, the root CA shall decide whether to revoke the EA/AA certificate in accordance with rules in the root CA's CPS. The root CA shall at all times ensure the EA/AA's compliance with this CP.

8.6. Communication of results

(368) The root CA and the TLM shall send the audit report to the CPA (flow 16). The root CA and TLM shall store all audit reports they have ordered. The CPA shall send a corresponding approval or rejection (flow 4) to the root CA and TLM.

(369) The root CA shall send a certificate of conformity to the corresponding EA/AA.

9. OTHER PROVISIONS

9.1. Fees

(370) One principle of the implemented EU C-ITS trust model is that the root CAs together fully finance the regular recurrent costs of operation of the CPA and the central elements (TLM and CPOC) relating to the activities set out in this CP.

(371) The root CAs (including the EU root CA) are entitled to take fees from their sub-CAs.

(372) Throughout their period of operation, every participant of the C-ITS trust model shall have access to at least one root CA, EA and AA on a non-discriminatory basis.

(373) Each root CA is entitled to pass on the fees it pays for CPA and the central elements (TLM and CPOC) to the registered participants of the C-ITS trust model, including the enrolled and authorised C-ITS stations.

9.2. Financial responsibility

(374) The initial establishment of a root CA shall cover a period of at least three years of operation, in order for it to become a member of the EU C-ITS trust model. The CPS of a root CA operator shall also contain detailed provisions on root CA revocation or closure.

(375) Each root CA must demonstrate the financial viability of the legal entity implementing it for at least three years. This financial viability plan is part of the initial set of documents for enrolment and must be updated every three years and reported to the CPA.

(376) Each root CA must report the structure of charges applied to EAs/AAs and the enrolled and authorised C-ITS stations each year to the operations manager and the CPA to demonstrate its financial sustainability.

(377) All financial and legal responsible entities of the root CA, EA, AA and the central elements (CPOC and TLM) of the C-ITS trust model must cover their operational duties with adequate insurance levels to compensate for operational errors and financial recovery of their duties if one of the technical elements fails.

9.3. Confidentiality of business information

(378) The following shall be kept confidential and private:

- root CA, EA, AA application records, whether approved or rejected;
- root CA, EA, AA and TLM audit reports;
- root CAs', EAs', AAs', CPOCs' and TLM's disaster recovery plans;
- private keys of the elements of the C-ITS trust model (C-ITS stations, TLM, EA, AA, root CAs);
- any other information identified as confidential by the CPA, root CAs, EA, AA, TLM and CPOC.

9.4. Privacy plan

(379) The CPSs of the root CAs and the EAs/AAs shall set out the plan and the requirements for the treatment of personal information and privacy on the basis of the GDPR and other applicable legislative (e.g. national) frameworks.

10. REFERENCES

The following references are used in this Annex.

[1] ETSI TS 102 941 V1.2.1, Intelligent transport systems (ITS) – security, trust and privacy management.

[2] ETSI TS 102 940 V1.3.1, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management.

[3] Certificate policy and certification practices framework (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 Policy requirements for certification authorities issuing public key certificates.

[5] ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS) – security, security header and certificate formats.

[6] Calder, A. (2006). Information security based on ISO 27001/ISO 1779: a management guide. Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – information technology, security techniques, information security risk management. ISO.