European Commission

C-ITS Platform Phase II

Certificate Policy for Deployment and Operation of European **Cooperative Intelligent Transport Systems** (C-ITS)

RELEASE 1
JUNE 2017

Certificate Policy
for
Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

Release 1

June 2017

C-ITS Platform Phase II
chaired by the

Foreword

This document is a deliverable of the C-ITS Platform following the adoption of the European Commission's Communication COM 2016/766 on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" adopted on 30th of November 2016.

The C-ITS Strategy of the Commission announced that the Commission will work together with all relevant stakeholders in the C-ITS domain to steer the development of a common security and certificate policy and other accompanying documents needed for the deployment and operation of C-ITS in Europe. Concretely it was announced that guidance will be published in 2017.

Hence this document is an deliverable of the Platform for the deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) which was created and chaired by the European Commission services in November 2014 to pave the way towards deployment of C-ITS in Europe. Following intensive work in a broad consultation process steered by the Commission from early 2016 onwards this document delivers the guidelines on a common C-ITS certificate policy that has been agreed upon by all involved stakeholders.

Document History

Release	Changes	Editor	Date
1	First Release*	C-ITS Platform	June 2017

** This document is the first published version of the C-ITS Certificate Policy for deployment and operation of European C-ITS. Please note that other accompanying documents, namely for instance the "C-ITS Security Policy" are currently still being drafted within the C-ITS Platform and are hence not published yet. The finalisation of all documents will lay the foundation for deployment of secure and interoperable C-ITS services in Europe.*

All documents are by definition subject to future change and will hence be updated whenever required and consequently published as a new release. As soon as the described governance roles have been concretely setup in Europe in the future, the publishing of these documents will be taken over by the respective roles and entities defined in the documents.

Please note that this first release includes a few items that have been marked in yellow (marked with "TBD" – "to be defined") to indicate that these paragraphs or elements still need to be updated as soon as the lacking elements become available.

In case of remarks on this document, please contact: MOVE-JRC-C-ITS-POLICY-AUTHORITY@ec.europa.eu

Table of Contents

1. Introduction

1.1. Overview and Scope of this Policy

Cooperative Intelligent Transport Systems (C-ITS) use technologies that allow road vehicles to communicate with other vehicles, with roadside infrastructure as well as with other road users. The systems are also known as vehicle-to-vehicle communications (V2V), or vehicle-to-infrastructure communications (V2I). C-ITS can cover a very wide range of different services. Depending on the nature of the applications (e.g. information supply, awareness, assistance, warning to avoid an accident, traffic management), C-ITS can contribute to improving road safety by avoiding accidents and reducing their severity, to decreasing congestion, by optimising performance and available capacity of existing road transport infrastructure, to enhancing vehicle fleet management, by increasing travel time reliability and to reducing energy use and negative environmental impact. Further C-ITS are considered a first milestone towards higher levels of automation in road transport.

For many data communication scenarios, it is very important to verify the authenticity and integrity of the messages containing information such as position, velocity and heading. This authenticity and integrity allows to assess the trustworthiness of this sent information. At the same time the impact on privacy of road users should be minimized. To ensure those main objectives, a security architecture with support of a Public Key Infrastructure (PKI) using commonly changing pseudonym certificates, has been developed.

This certificate policy defines the European C-ITS Trust model based on Public Key Infrastructure. It defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. The PKI is composed at its highest level by a set of root CAs "enabled" by the Trust List Manager (TLM), i.e. whose certificates are inserted in an European Certificate Trust List (ECTL), which is defined and published by the central entity TLM (see sections 1.3 and 1.5).

This policy is binding to all entities participating in the trusted C-ITS system in Europe. The policy can therefore be used as guidance to assess which level of trust 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 certificates, this policy defines a binding set of requirements for the operation of the central entity TLM and the definition and management of the ECTL. Consequently, this document defines the following aspects related 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 the Local Security Practices for the TLM, including physical controls, personnel controls and procedural controls.
- Minimum requirements for the Technical Security Practices for the TLM, including computer security controls, network security controls and cryptographic module engineering controls.
- Minimum requirements for Operational Practices for the TLM including registration of new root CA certificates as well as temporary or permanent deregistration of existing included root CAs as well as publication and distribution of the ECTL updates.

- ECTL Profile, including all mandatory and optional data fields contained in the ECTL, used cryptographic algorithms, as well as the exact ECTL format and recommendations for processing of the ECTL.

- ECTL certificate lifecycle management, including distribution of ECTL certificates, activation, expiration and revocation.
- Management of the revocation of trust of root CAs when needed.

Since the trustworthiness of the ECTL does not solely depend 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 defines minimum requirements for certain aspects, which are mandatory for all participating CA´s to be implemented in the certificate practice statements of these CAs. In particular, these aspects are:

- 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 as well as certificate validity periods.

- Minimum requirements for Local Security Practices including physical controls, personnel controls and procedural controls.

- Minimum requirements for Technical Security Practices such as computer security controls, network security controls and cryptographic module engineering controls.

- Minimum requirements for Operational Practices of the CA, EA, AA and end-entities including topics 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 certificates are expected to be processed by verifiers.

- Regular monitoring reporting, alerting and restore duties of the C-ITS Trust model entities in order to establish a secure operation including cases of misbehaviour.

In addition to these minimum requirements the entities running the root CAs and Sub CAs can define their own additional requirements and define them in the respective CPS. See section 1.7 for details on how the CPS is audited and published. However, these additional requirements shall not contradict this present certificate policy.

Together with the Security policy, this document also describes the Certificate Policy Administration: duties, responsibilities and liabilities for procedures for development and maintenance of the CP document and the nature of changes that should lead to issuance of a new policy.

The Certificate Policy explicitly identifies the applicable European regulations to which the TLM shall conform, including data protection, privacy, access to information and lawful interception legislation. The

certificate policy also states the purposes on which the root CAs, sub CAs and their issued certificates are constrained to be used. The certificate policy defines liabilities to be taken 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 certificate policy also defines mandatory obligations to be taken by

- The TLM.
- Each root CA, whose certificates are listed in the ECTL.
- Each Sub CAs certified by root CAs.
- All End-Entities.
- Each member organisation responsible for or operating one of the C-ITS Trust model entities.

The certificate policy will finally put requirements on the documentation of limitations to liabilities and obligations in the Certificate Practice Statement of each CA contained on the ECTL.

This CP is conforming to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction [3]. Within this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [8].

1.2. Elements, which are out of scope of this certificate policy

Details of governance structure including the process to become member of the governance and the related obligations are out of the scope of this certificate policy. The test and validation procedures before distributing the ECTL to ITS-S is out of scope of this certificate policy. The test and validation procedures of C-ITS services/applications and their compliance assessment process is out of scope of this certificate policy.

1.3. Definitions and Acronyms

The definitions of [2], [3], [4] apply.

AA	Authorization Authority
AT	Authorization Ticket
CA	Certification Authority

C-ITS station	ITS station: functional entity specified by the ITS station (ITS-S) reference architecture. This CP distinguishes between mobile ITS-S (including vehicle ITS-S) and fixed ITS-S.
CP	Certificate Policy
CPOC	C-ITS Point of Contact
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
EA	Enrolment Authority
EC	Enrollment Credential
EE	End-entity (ITS Station)
ECTL	European Certificate Trust List
GDPR	General Data Protection Regulation
ITS-S	ITS Station
PA	Policy Authority
PKI	Public Key Infrastructure
RA	Registration Authority
Sub CA	EA and AA
TLM	Trust List Manager

Terms Definition

Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Initial Certificate was created (initialization), 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.
Authorization Authority	In this document, the term Authorization Authority (AA) includes not only the specific function of AA but also the legal and/or operational entity managing the AA.
Crypto-agility	Describes 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 cryptographic module is a secure hardware based element, within which keys are generated and/or stored, random numbers are generated and data are signed or encrypted.

Enrollment Authority	In this document, the term root Enrollment Authority (EA) includes not only the specific function of EA but also the legal and/or operational entity managing the EA.
Re-Keying	This subcomponent is used to describe the following elements related 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 ([3])
Repository	It is the repository used for storing the certificates and information about certificates as 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) includes not only the specific function of CA but also the legal and/or operational entity managing the CA.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subscriber	A natural person or Legal Entity to whom a Certificate is issued and who 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.

1.4. Document Name and Identification

This CP is identified by the following information:

- Name: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)
- Version: 1
- OID: {iso(1) identified-organization(3) european-commission(130) information-systems(1) *(TBD-proposed but not formalized yet)*
- Location: https://ec.europa.eu/transport/themes/its/c-its_en *(TBD - proposed but not formalized yet)*

1.5. PKI Participants

1.5.1. Introduction

PKI participants play a role in the PKI defined by the present policy. Unless explicitly prohibited, it is possible for a participant to assume multiple roles at the same time. Reasons for prohibiting specific roles to be assumed by the same entity are avoiding conflicts of interest or the implementation of segregation of duties.

Additionally, it is also possible for a participant to delegate parts of its 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. However, a CA may delegate the responsibility for issuing CRLs to a different entity.

PKI roles are distinguished in:

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

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

provides a pictorial description of the C-ITS Trust model architecture. A brief description of the architecture is provided here, but a detailed description of the main elements is found from sections 1.5.2 to 1.5.6.

The Policy Authority appoints the Trust List Manager and therefore provides trust in the operation of the Trust List Manager to all PKI participants. The Policy Authority approves the root CA operation and confirms that the TLM can trust the root CA(s). The TLM issues the ECTL that provides trust in the approved root CAs to all PKI participants. The root CA issues certificates to the EA and AA and therefore provide trust to their operation. The EA issues Enrolment Certificates to the sending and relaying ITS-Station (as End-Entity), providing trust in its operation. The AA issues Authorization Tickets to the ITS-Stations based on the trust in the EA.

The receiving and relaying ITS-Station (as relying party) can trust other ITS-Stations since the ATs are issued by an AA which is trusted by a RCA, which is trusted by the TLM and the PA.

Note that Figure 1 only describes the root CA level of the C-ITS trust model. Details on 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 about the information flows between the PKI participants. The green dots indicate flows that necessarily 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 defined in the rest of this document) to the Central Point of Contact (CPOC) through a secure protocol (e.g., link certificates), which is defined by CPOC.

A root CA can be operated by a governmental or a private organization. At least one root CA (the EU root CA with the same level like the other root CAs) is present in the C-ITS Trust model architecture. The EU root CA is delegated by all the entities participating to the C-ITS trust model and which do not want to set up their own root CA. The CPOC transmits the received root CA certificates to the Trust List Manager (TLM), which is responsible for collecting and signing the list of root CA certificates and sending them back to the CPOC, which make them public to everybody as described in this Certificate Policy.

The trust relationships between the described entities of the C-ITS trust model are described in the following paragraph.

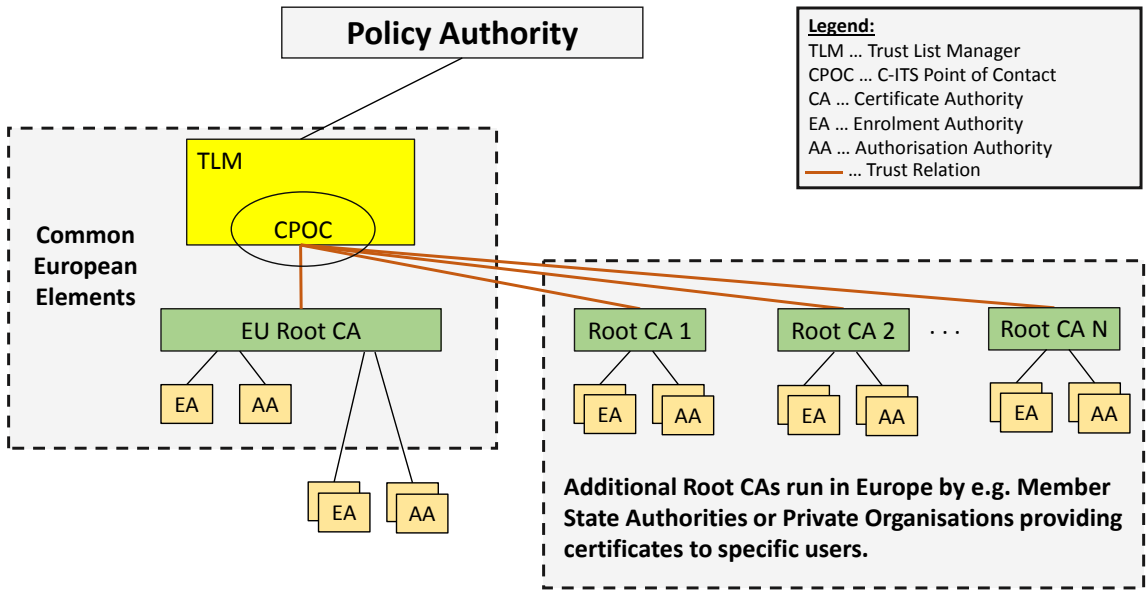

Figure 1: C-ITS Trust model architecture

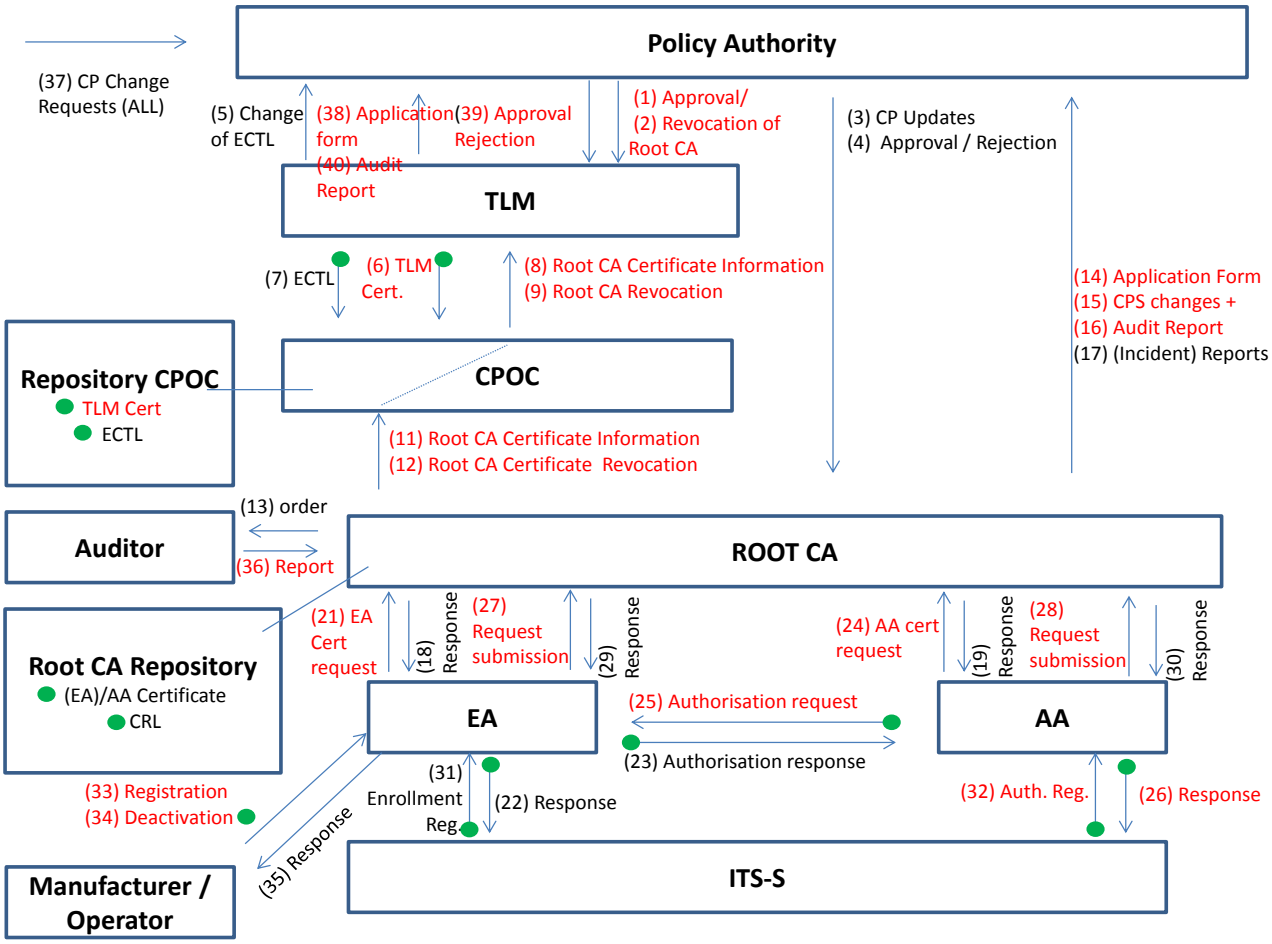

Figure 2: C-ITS Trust model information flows

Flow Id	From	To	Content	Reference
(1).	PA	TLM	Approval of RCA Application	8
(2).	PA	TLM	Information on Revocation of RCA	8.5
(3).	PA	RCA	CP Updates	Security Policy
(4).	PA	RCA	Approval/Rejection of the root CA application form or the CPS request changes or the Audit process.	8.5, 8.6
(5).	TLM	PA	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	PA	root CA Application Form – Initial request	4.1.2.1
(15).	root CA	PA	root CA Application Form – CPS changes	Security Policy
(16).	root CA	PA	root CA Application Form – Audit report	8.6
(17).	root CA	PA	root CA Incident reports including the revocation of a Sub-CA (EA,AA)	Security Policy, 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	ITS-S	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	ITS-S	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).	ITS-S	EA	Enrolment Credential request	4.2.2.4
(32).	ITS-S	AA	Authorisation Ticket request	4.2.2.5
(33).	Man/Op	EA	Registration	4.2.1.4
(34).	Man/Op	EA	Deactivation	7.3
(35).	EA	Man/Op	Response	4.2.1.4
(36).	Auditor	root CA	Report	8.1
(37).	All	PA	CP Change Requests	Security Policy
(38).	TLM	PA	Application Form	4.1.2.2
(39).	PA	TLM	Approval/Rejection	4.1.2.2
(40).	TLM	PA	Audit Report	4.1.2.2

Table 1 Detailed description of the information flows among the elements of the C-ITS trust model

1.5.2. Policy Authority

The Policy Authority is a role composed by the representatives of public and private stakeholders (e.g. Member States, Vehicle Manufacturers, etc.) participating to the C-ITS trust model. The Policy Authority is responsible for two sub roles:

Certificate policy management, including the following tasks:

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

PKI authorisation management, including the following tasks:

- 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,
- the approval of the root CA's CPS if in line with the common and valid CP,
- scrutiny of the audit reports from the Accredited Auditor for all root CAs,
- notifying the Trust List Manager about the approved and not approved root CAs and their certificates on the basis of the received approval reports of the root CAs and the regular operations reports.

It is the responsibility of the Policy Authority's Authorized Representative to authenticate the TLM's authorized representative and to approve the TLM's enrolment process application form. It is the responsibility of the Policy Authority to authorize the TLM to operate as mentioned in this section.

Details on which body implements the sub-roles of the policy authority are defined in the Security Policy document.

1.5.3. Trust List Manager

The TLM is a unique entity appointed by the Policy Authority.

The Trust List Manager is responsible for:

- operation of the ECTL according to the common valid CP and regular activity reporting to the policy authority for the overall secure operation of C-ITS trust model,
- reception of root CA certificates from the CPOC,
- the inclusion/exclusion of root CA certificates in ECTL upon notification by the Policy Authority,
- signing of the ECTL,
- regular and fast transmission of ECTL to the CPOC.

1.5.4. Accredited Auditor

The Accredited Auditor is responsible for:

- performing or organizing audits of root CAs, TLM and sub-CAs.,
- distribution of the audit report (related to either an initial or periodic audit) to the Policy Authority according to the requirements defined in section 8 of this Certificate Policy. The audit report includes the recommendations proposed by the accredited auditor,
- notification to the entity managing the root CA on the successful or unsuccessful execution of an audit for the sub-CAs either initial or periodic,
- Assessing compliance of CPSs to this CP.

1.5.5. C-ITS Point of Contact (CPOC)

The CPOC is a unique entity appointed by the Policy Authority. It is the responsibility of the Policy Authority's Authorized Representative to authenticate the CPOC authorized representative and to approve the CPOC enrolment process application form. It is the responsibility of the Policy Authority to authorize the CPOC to operate as mentioned in this section.

The CPOC is responsible for:

- Establish and contribute to secure communication exchange between all entities of the C-ITS trust model in an efficient and fast way,
- reviewing of procedural change requests and recommendations submitted by other trust model participants (i.e., root CAs),
- transmitting the root CA certificates to the Trust List Manager,
- publication of the common trust anchor (public key certificate of the Trust List Manager),
- publication of the ECTL.

The complete and specific details of the ECTL can be found in section 7.

1.5.6. Operational roles

The following entities defined in [2] play an operational role as defined in RC 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 enrolment credentials, respectively authorization tickets
Enrolment Authority	Subscriber to root CA Subject of EA certificate CA/RA	Authenticates an ITS-S and grants it access to ITS communications
Authorization Authority	Subscriber to root CA/ Subject of AA certificate CA/RA	Provides an ITS-S with authoritative proof that it may use specific ITS services
Sending ITS-S	Subject of EE (End Entity) certificate (EC)	Acquires rights from Enrolment Authority to access ITS communications Negotiates rights from Authorization Authority to invoke ITS services Sends single-hop and relayed broadcast messages
Relaying ITS-S (Forwarding ITS-S)	Relying party Subject of EE certificate	Receives broadcast message from the sending ITS-S and forwards them to the receiving ITS-S if required
Receiving ITS-S	Relying party	Receives broadcast messages from the sending or relaying ITS-S
Manufacturer	Subscriber to EA	Installs necessary information for security management in ITS-S at production.
Operator	Subscriber to EA / AA	Installs and updates necessary information for security management in ITS-S during operation.

Table 2: Operational roles

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

Note: the roles Root Certification Authority, Enrolment Authority, Authorization Authority are cumulatively referred to as CA.

Registration authorities:

The role of a registration authority for end-entities shall be performed by the EA. The registration of new end-entities (ITS Stations) in an EA can only be done by an authenticated and authorized subscriber. The role of registration authorities for EAs and AAs shall be performed by the respective root CAs.

1.6. Certificate Usage

1.6.1. Applicable domains of use

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].

Certificate uses for TLM, root CAs, EAs, AAs and end-entities are defined by the certificate profiles in [5].

1.6.2. Limits of Responsibility

Certificates are not intended and authorized for use in:

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

1.7. Policy Administration

1.7.1. Organization administering this document of the Certificate Policy

This document is administered on behalf of the entities of the EU C-ITS Trust model by the Policy Authority.

1.7.2. Updating of this certificate policy

This certificate policy is subject of continuous improvement. The update process is managed by the Policy Authority and follows five major steps:

1. Submission of the change request.
2. Change processing.
3. Change approval.
4. Change publication and announcement.
5. Change implementation.

This Policy shall be checked and updated every 3 years and if there are no applicable changes at least an empty change request shall be submitted and approved to update the date.

1.7.2.1. Submission of the Change Request

The change process is initialized by a change request of a stakeholder. Every stakeholder can submit a change request. The change request shall contain:

- A brief description of the change.
- A rationale for the change.

- Criticality classification for security of the system.
- The exact proposal including the line/paragraphs to be changed, the old text and the new text.
- A change requester contact.

The change requester should be prepared to answer requests for additional information and/or defend the change proposal at the policy authority.

1.7.2.2. Change Processing

Within one working day after receiving the change request, the Policy Authority shall confirm reception of the change request. Within 2 weeks after receiving a change request, the policy authority shall start processing the change. Processing of a change request means:

- Assessing the applicability of the change request.
- Assessing the completeness of the change request.
- Assessing the criticality of the change request.
- Assessing the impact of the change.

The change processing may confirm that the change is seen as critical for the security of the C-ITS system. If a change requests is seen as critical, the change request becomes an Emergency Change Request**.** To ensure to resolve security critical situations as quickly as possible, emergency change requests will be handled in a shortened process as described in the next steps.

The change processing phase is concluded with scheduling the processed change request for decision in the next change approval meeting of the policy authority. If the change has been classified as an emergency change request due a disaster recovery scenario, the change approval meeting shall be scheduled for immediate decision, with at least 60% of the members of the Policy Authority present, as quickly as possible but at least within 48 hours.

1.7.2.3. Change Approval

The policy authority conducts change approval meetings to discuss and finally decide if a change request is accepted. Given that change requests have been received, the policy authority shall conduct a change approval meeting half-yearly. The policy authority may invite change requestor contacts and stakeholder experts to participate in the discussion. After discussion, the change approval meeting can decide to:

1. Fully accept the change request without any changes and proceed directly to the change publication and announcement step.
2. Partially accept the change request and proceed to the change publication and announcement step.
3. Decide on a modified change request and proceed to the change publication and announcement step.
4. Request modification of the change request and resubmission of the change request.
5. Fully reject the change request.

In case of an emergency change request, the policy authority shall hold an emergency change approval meeting within 48 hours after conclusion of the change processing. The change approval meeting shall not fully reject security critical change requests. The change approval meeting should not request modification and resubmission of the modified change request to avoid any unnecessary delay.

1.7.2.4. Change Publication and Announcement

Once a change request is approved by the policy authority's change approval meeting, the policy authority shall publish an updated provisional version of the CP and announce the implementation with a due date to become effective and an implementation time frame for the transition beginning once the new policy becomes effective to all root CAs listed on the ECTL.

Non-emergency changes shall not become effective until at least two weeks after the next change approval meeting. Any root CAs listed on the ECTL shall take appropriate preparation to ensure that the implementation can be achieved during the implementation time frame. Stakeholders may submit change requests to modify announced changes for decision on the next change approval meeting. Stakeholders may also submit change request limited on the due-date or the implementation time-frame. Changes increasing the time periods can be decided to be scheduled before the next change approval meeting.

In case of emergency changes, the new policy shall become effective as quickly as feasible and the implementation timeframe shall be as short as feasible. The effectiveness of new policies after emergency changes are not restrained to follow-up change approval meetings. Instead, in these conditions, the change requests affecting announced and not yet implemented emergency changes, automatically follow the emergency change process.

1.7.2.5. Change Implementation

Within the announced implementation period, each root CA listed on the ECTL shall implement the changes and provide appropriate evidence to fulfil the changed requirements to the policy authority.

After implementation, the Policy Authority updates the CP to match the provisional CP as published in the previous step. At this time, the updated CP replaces the previous version of the CP.

1.7.3. Updating of CPS's of CAs listed in the ECTL

Each root-CA listed on the ECTL shall publish its own CPS which is in compliance to this policy. A root CA may add additional requirements but shall ensure that all requirements of this CP are met at all time.

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

The change process shall ensure that all changes to this CP are carefully analysed and, if necessary for compliance to an updated CP, the CPS is updated within the timeframe defined in the implementation step of the change process of the CP as described in section 1.7.2. Especially, the change process shall define emergency change procedures that ensure timely implementation of security relevant changes to the CP.

The change process shall include appropriate measures to verify CP compliance for all changes to its CPS. Any changes to the CPS shall be clearly documented. Before implementing a new version of a CPS, its compliance to CP must be confirmed by an accreted auditor.

The root-CA shall notify the Policy Authority about any change made to the CPS with at least the following information:

- Exact description of the change.
- Rationale of the change.
- Report of the accredited auditor confirming compliance to the CP.
- Responsible contact to the CPS.
- Planned time to implementation.

1.7.4. Contact point

Policy Authority:

MOVE-JRC-C-ITS-POLICY-AUTHORITY@ec.europa.eu *(TBD - Proposed but not formalized yet. This email address is just an alias to include representatives from European Member States and other participating stakeholders according to the C-ITS Security Policy).*

1.7.5. CPS approval procedures

A prospective root CA shall present its CPS to an Accredited Auditor as part of an order for compliance audit (flow 13) and to the Policy Authority for approval (flow 15) before starting its operations.

A root CA shall present changes to its CPS to an Accredited Auditor as part of an order for compliance audit (flow 13) and to the Policy Authority for approval (flow 15) before those changes become effective.

An EA/AA shall present its CPS or changes to its CP to the root CA. The root CA may order an certificate of conformity by the national body or private entity responsible for approval of the EA/AA as defined in sections 4.1.2 and 8.

The Accredited Auditor shall assess the CPS according to what described in section 8.

The auditor shall communicate the results of the CPS assessment as part of the audit report, as defined in 8.1. The CPS shall be accepted or rejected as part of the audit report acceptance defined in 8.5 and 8.6.

2. Publication and repository responsibilities

2.1. Methods for the publication of certificates information

Publication of certification information, (as defined in section 2.5) can be done in two possible ways:

Firstly in a regular or periodic way and secondly as a publication on request from one of the participating entities. For both ways different urgencies for publication and therefore time schedules apply, but entities need to be able to support both publication mechanisms.

The **regular publication** of the certificate information enables to achieve a maximum time frame in which certificate information is updated for all nodes of the C-ITS Network. The frequency how often all

certification information should be published is specified in section 2.2. The detailed process steps of this publication are defined in section 3.2.6.

The publication of certification information **on request** of participating entities of the C-ITS Network can be started at any time by one of the participants, and depending on its status, it will request a current set of certification information to be able to become a fully trusted node of the C-ITS network. This publication on request of single entities has mainly the purpose to update them to the overall current status of certification information in the network and enables them to communicate on a trusted basis till the next regular publication of certification information.

A similar way to start a publication of certificate information at any point in time, but from a single root CA, is to push an updated set of certificates to all the "subscribed members" of the C-ITS network which regularly get certification information. This mechanism supports the operation of the CAs and their options to address members also between the regular and scheduled publication dates of the certificates.

For the mechanism used to publish root CA certificates and the ECTL with all procedures, refer to section 2.5.

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

Root CAs shall publish their EA/AA certificates and CRLs and shall be able to support all three mentioned publication mechanisms to their subscribed members and to their relying parties, taking into account all necessary steps for a secure transmission as mentioned in section 4.

2.2. Time or Frequency of Publication

The requirements regarding the publication schedule of certificates and CRLs need to be defined taking into account 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 stations involved.

- For the regular publication of updated certification information (e.g., changes in the ECTL composition), a period of maximum 3 months is required for safe operation of the C-ITS Network.

- In case of a security breach, a publication on request is needed. For publications on request the maximum time allowed for a CA to process the publication of a new set of certificate information to a single C-ITS Entity (EA, AA) shall not exceed 60 minutes in normal operating conditions.

- For a publication initiated by the root CA to all C-ITS Entities, the processing time of the publication shall not exceed a maximum time of 3 hours measured from the root CA point of view.

- For the publication of the CRL the root CA repository shall be used and the same parameters of processing and transmission times respected as for ECTL publication.

Additionally, the CPS for each CA shall specify the period of time within which a certificate will be published after the CA issues the certificate, the processing times for this process should be similar to a publication on request.

Note that this section specifies only the time or frequency of the publication. Means of connectivity to update C-ITS stations with the ECTL within 1 week after their publication (under normal operation conditions with e.g. cellular coverage, vehicle in actual operation, etc.) and CRLs shall be implemented according to the requirements listed in this document.

2.3. Repositories

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 his own currently active EA /AA certificate information and CRL to publish certificates for the other PKI participants (e.g. a LDAP based directory service). The repository of each root CA shall support all requested access controls (section 2.4) and transmission times (section 2.2) for every method of distribution of C-ITS related information.

- The repository of the TLM, ECTL and TLM certificates published by the CPOC should be based on a distribution center service (the distribution center service is based on the same publication mechanism as the root CA) able to respect the defined transmission times of section 2.2 for every method of distribution. e.g. for root CA certificates and ECTL e.g. an online certificate repository, a CRL.

Requirements to Authorization Authorities are not defined, but need to support the same security levels as the other entities and need to be declared in their CPS.

2.4. Access Controls on Repositories

The requirements on access control to repositories of certification Information shall at least comply with the general standards of secure information handling, outlined in ISO/IEC 27001 and with the requirements as defined in section 4 and additionally respect the process security needs to be established for the single process steps of the publication of certification information.

- This includes the implementation of TLM Certificates and ECTL in the CPOC, each CA or repository operator that 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 unauthorized entities from adding, modifying, or deleting repository entries at all.

- 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 too the same requirements for access control procedures independently from the place or contractual link to the respective service provider operating the repository.

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

2.5. Publication of Certification Information

2.5.1. Publication of Certification Information from TLM

The TLM inside 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 of the CPOC repository to provide the signed list of root CA´s, ECTL
- General Information point for ECTL and new C-ITS Organizations

2.5.2. Publication of Certification Information from CAs

A root CA inside 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 repository named in section 2.3,
- All valid EA, AA entities with their operator ID and their planned period of operation
- Issued CA certificates in the repositories named in section 2.3,
- The Certificate Revocation Lists for all revoked CA certificates covering its subordinate EAs and AAs,
- access point information of the RCA to get the CRL and CAs information,

All certification information shall be categorized according to three levels of confidentiality and documents for general public need to be publicly available without restrictions.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

3.1.1.1. Names for Trust List Manager, RCAs, EAs, AAs

The name in the TLM certificate shall consist of a single subject_name attribute with the reserved value “ECTL”.

The name for RCAs shall consist of a single subject_name attribute with a value allocated by the Policy Authority. The uniqueness of names is the sole responsibility of the Policy Authority and the TLM shall maintain the registry of RCA names upon notification of the Policy Authority (approval, revocation/removal

of a root CA). Subject names in certificates are limited to 32 bytes. Each root CA proposes its name to the PA in the application form (flow (14)). The PA is responsible to check name uniqueness. If name is not unique then the application form is rejected (flow (4)).

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 CA.

The EA and AA certificates shall not use a name greater than 32 bytes, because Subject names in certificates are limited to 32 bytes.

Authorization Tickets shall not contain a name.

3.1.1.2. Names for End entities

Each ITS station shall be assigned with two kinds of unique identifiers:

- A canonical ID that is stored at initial registration of the ITS station under the responsibility of the manufacturer. The canonical ID shall contain a substring identifying the manufacturer or operator to make uniqueness of this identifier possible.
- A subject_name that may be part of the ITS station's EC, under the responsibility of the EA.

3.1.1.3. Identification of certificates

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

The AA shall ensure that pseudonymity of an ITS station is established by provisioning the ITS-S with Authorization Tickets 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

Names for TLM, RCAs, EAs, AAs and canonical IDs for ITS stations shall be unique.

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

The HashedId8 of an EC shall be unique within the issuing CA. The HashedId8 of an AT does not need to be unique.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The RCA shall prove that it rightfully holds the private key corresponding to the public key which is inside the self-signed certificate. The CPOC shall check this proof.

The EA/AA shall prove that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The RCA shall check this proof.

The method to proof possession of new private key (for re-keying) is to sign the request with the new private key (inner signature) and after that, generate an outer signature over the signed request with the current valid private key (to guarantee the authenticity of the request). The signed certificate request is to be submitted by the applicant to the issuing CA via a secure communication. The issuing CA shall verify that applicant's digital signature of the request message was created using the private key corresponding to the public key attached to the certificate request. The RCA shall specify which certificate request and responses it supports in its CPS.

3.2.2. Authentication of organization identity

3.2.2.1. Authentication of root CAs organization identity

The root CA shall provide in application form (i.e., flow (14)) the identity of the organization and registration information, composed of:

- organization name,
- postal address,
- e-mail address,
- contact name of an organization physical person,
- telephone number,
- digital fingerprint of the root CA`s certificate in printed form.

The application form contains at minimum the following information

- Cryptographic information (e.g. cryptographic algorithms, key lengths, signature) of the Sub-CA certificate.
- Permissions for applications to be included in the Sub-CA certificate as mentioned in [5]

The PA shall check the identity of the organization and other registration information provided by the certificate applicant for the insertion of a RCA certificate into the ECTL.

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

Verification of the subject's identity shall be at time of registration by appropriate means and in accordance with the present Certificate Policy.

At each certificate application, organization evidence shall be provided of:

- the full name of the organizational entity (private organization, government entity or non-commercial entity);
- the reference to a nationally recognized registration, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

[extract from TS 102 042: *The CA shall ensure that evidence of 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 authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.*]

3.2.2.2. Authentication of TLM organization identity

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

Verification of the subject's identity shall be at time of certificate creation or re-keying by appropriate means and in accordance with the present Certificate Policy.

Organization evidence shall be provided as specified in section 3.2.2.1.

3.2.2.3. Authentication of CAs organization identity

The RCA shall check the identity of the organization and other registration information provided by certificate applicants for EA/AA certificate.

At a minimum the RCA shall:

- determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filled with the applicable government agency or recognized authority that confirms the existence of the organization,
- confirmatory postal mail, or comparable procedure to the certificate applicant certain information about the organization, that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the organization, the employment of that individual and his/her authority to act on behalf of the organization shall also be confirmed.

Validation procedures for issuing CA certificates shall be documented in a CPS of the RCA.

3.2.2.4. Authentication of End-entities Subscriber organization

Before the Subscriber of end-entities (manufacturer/ operator) can register to a trusted EA to enable its end-entities for sending EC certificate requests, the EA shall check identity of the Subscriber organization and

other registration information provided by the certificate applicant. (e.g. the device has passed all compliance assessment criteria defined by the CA Governing Body (defined in the C-ITS Security Policy) and the manufacturer provided the evidence that all compliance requirements are satisfied, e.g. results published in a C-ITS Device Compliance Assessment Registry (defined in the C-ITS Security Policy).

At a minimum the EA shall:

- determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filled with the applicable government agency or recognized authority that confirms the existence of the organization,

- confirmatory postal mail, or comparable procedure to the certificate applicant certain information about the organization, that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the organization, the employment of that individual and his/her authority to act on behalf of the organization shall also be confirmed.

Validation procedures for ITS-S registration 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

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

- full name (including surname and given names, consistently with the applicable law and national identification practices) of the subject;

- date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name;

- full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);

- any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;

- evidence that the subject is associated with the legal person or other organizational entity.

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

To verify the identity of the authorized representative of a RCA, EA, AA or Subscriber, the certificate applicant representative shall provide documentation proving that he is indeed a person which is working at this organization (certificate of authorization). The person shall also show an official ID Document to prove its identity.

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

The personnel at the root CA shall verify the identity of the certificate applicant representative and all associated documents and they shall follow the requirements of 'trusted personnel' as defined in section 5.2.1 (the process for validating application information and for generating the certificate by the root CA shall be done by 'trusted persons' under at least dual supervision because they are sensitive operations see section 5.2.2).

3.2.3.2. Authentication of ITS stations' subscriber identity

Subscribers are represented by authorized end-users within the organization which are registered at the issuing EA and AA. These end-users designated by organizations (manufacturers or operators) shall prove their identity and authenticity before:

- registering the EE at its corresponding Enrolment Authority (EA) including its canonical public key, canonical ID (unique identifier) and the permissions according to the End Entity;
- registering at the AA and getting a proof of subscriber agreement that may be sent to the EA as described in the Security Policy.

3.2.3.3. Authentication of ITS stations identity

End-entities (EE) subjects of ECs shall authenticate themselves when requesting ECs 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 ITS-S manufacturer or operator and the EA.

End-entities subjects of ATs shall authenticate themselves when requesting ATs by using their unique Enrolment private key. The AA shall forward the signature to the EA for validation; the EA shall validate it and confirm the result to the AA.

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

Every organisation shall define in the CPS at least one representative person responsible (e.g. security officer) for the request of new certificates and renewals. The naming rules defined in section 3.2.3 have to be followed. See section 3.2.3.

3.2.5.2. Validation of ITS Station subscribers

At least one physical person responsible for registration of ITS Stations at an EA (e.g. security officer) shall be known and approved by the EA, see section 3.2.3.

3.2.5.3. Validation of ITS Stations

An ITS stations' subscriber may register ITS stations at a specific EA as long as it is authenticated at this EA.

When the ITS station is registered at an EA with a unique canonical ID and a canonical public key, the ITS station is able to request an enrolment certificate using a request signed by the canonical private key that is related to the previously registered public key.

3.2.6. Criteria for Interoperation

For communication between ITS stations and EA (respectively AAs), the ITS-S shall be able to establish a secure (authenticated and confidential) communication with EA (respectively AAs) as specified in [1]. Other protocols may also be used granted that [1] is implemented. The EA and AA shall support this secure communication.

The EA and AA should support certificate request and responses compliant to [1] which provides secure ATs request/response protocol supporting anonymity of the requester against the AA and separation of duties between AA and EA. To prevent disclosure of ITS-Ss long-term identity, the communication between a mobile ITS station and an EA shall be encrypted in an end-to-end way.

The AA shall submit an authorization validation request for each authorization 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-AIDs and permissions,
- the status of service provision of the AA to the subscriber.

The regular publication schedule every six months includes the requirement for all ITS-S, that they should check their current status of the certification information when starting their operation.

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

The TLM generates a key pair and two certificates: one self-signed and one link certificate.

3.3.1.2. RCA certificates

Not applicable.

3.3.1.3. EA/AA certificates renewal or re-keying

Prior to the expiration of an existing EA/AA certificate, the EA/AA shall request a new certificate 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 (technically defined as “rekey”). The EA or AA generates a new key pair and signs the request with the new private key (inner signature) to proof possession of the new private key. After that 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, a proof of possession for private decryption keys shall be done (for detailed description of re-keying see section 4.7.3.3).

The method for identification & authentication for a routine re-keying is the same as for the initial issuance of an initial RCA certificate validation as described in section 3.2.2.

3.3.1.4. End-entities enrolment certificates

Prior to the expiration of an existing EC, the EE shall request a new certificate 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 enrolment credential private key.

The EE may optionally sign the request with the new created private key (inner signature) to proof possession of the new private key. After that the whole request is 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 also be used granted that [1] is implemented.

3.3.1.5. End-entities authorization tickets

The Certificate re-key for an Authorization Tickets is based on the same process of the initial authorization as defined in [1]. Other protocols may also be used granted that [1] is implemented.

3.3.2. Identification & Authentication for Re-key Requests after revocation

3.3.2.1. CA Certificates

The authentication of a CA organization for RCA, EA, AA certificate re-keying after revocation is handled in the same way as for the initial issuance of a CA certificate, described in section 3.2.2.

3.3.2.2. End-entities enrolment certificates

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

3.3.2.3. End-entities authorization requests

Not applicable since Authorization tickets are not revoked.

3.4. Identification and authentication for revocation request

3.4.1. RCA/EA/AA Certificates

The request to delete an RCA certificate from the ECTL shall be authenticated by the RCA to the TLM (flows 12 and 9). The request to revoke an EA/AA certificate shall be authenticated by the respective RCA and Sub-CA itself.

Acceptable procedures for authenticating the revocation requests of a subscriber include:

- Receiving a written and signed message on corporate letter sheet from the subscriber that requests revocation with reference to the certificate to be revoked,
- Communication with the subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the subscriber. Such communication, depending on the circumstances, may include one or more of the following: e-mail, postal mail, or courier service.

3.4.2. ITS-S enrolment certificates

The ITS-S Subscriber may revoke the EC of a previously registered ITS-S at an EA. The requesting subscriber shall create a request for revocation of a given ITS-S or for a list of ITS-Ss. The revocation request shall be authenticated by the EA before the EA processes the request and confirm the revocation of the ITS-Ss and the revocation of their Enrolment Credentials.

The EA can revoke the EC of an ITS station according to section 7.3

3.4.3. ITS-S authorization tickets

Authorization tickets are not revoked. This implies that the validity of authorization tickets cannot be long. 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

Section 4.1 specifies the requirements for an initial application for certificate issuance.

The term certificate application refers to the following processes:

- Registration and setup of trust relation of TLM with PA.
- Registration and setup of trust relation of root CA with PA and TLM, incl. insertion of first root CA certificate into ECTL.
- Registration and setup of trust relation of EA/AA with root CA, incl. issuance of new EA/AA certificate.
- Registration of ITS-S at EA by the manufacturer
- Request of ITS-S for EC/AT.

4.1.1. Who can submit a Certificate Application

4.1.1.1. Root CAs

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.

4.1.1.2. TLM

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 organization representative under the control of the PA.

4.1.1.3. EA and AA

An Authorized Representative of the EA or the AA may submit the Sub-CA (EA or/and AA) certificate request application to the Authorized Representative of the respective root CA (flow 27/28).

4.1.1.4. ITS-S

Subscribers shall register each ITS-S at the EA according to section 3.2.5.3.

Each ITS-S, registered at the EA, may send Enrollment Credential certificate requests.

Each ITS-S may send Authorization Tickets requests without requesting any Subscriber interaction. Before requesting an AT, an ITS-S shall have an EC.

4.1.2. Enrolment process and responsibilities

Permissions for root-CAs and Sub-CAs issuing certificates for special (governmental) purpose (i.e. special vehicle and RSUs) must only be granted by the corresponding Member States, where the organizations are located.

4.1.2.1. Root CAs

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

The root CA's application form shall be signed by its authorized representative.

In addition to the application form root CA's Authorized representative shall provide a copy of the root CA`s CPS (flow 15), the CP and its audit report to the PA for approval (flow 16). In case of positive approval the PA sends the certificate of conformity to the TLM and the corresponding root CA.

After that the root CAs authorized representative shall bring its application form (containing fingerprint of self-signed certificate), official ID-Document and proof of authorization to the TLM. The self-signed certificate shall be delivered electronically to the TLM. The TLM verifies all documents and the self-signed certificate.

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

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

4.1.2.2. TLM

After being audited, TLM may enroll to the PA. The enrolment process is based on a signed manual application form that shall be physically delivered to the PA (flows 38) by the TLM's Authorized Representative and that contains at minimum the following information (section 3.2.2.2, section 3.2.3).

The TLM's application form shall be signed by its authorized representative.

First, the TLM generates its self-signed certificate and transmits it to the PA in a secure way. After that the TLM brings its application form (containing the fingerprint of the self-signed certificate), a copy of its CPS, an official ID document, a proof of authorization and its audit report to the PA (flow 40). The PA shall check all the aforementioned documents and the self-signed certificate. In case of a positive verification of all the documents, the self-signed certificate and the fingerprint, the PA shall confirm the enrolment process by sending its approval to the TLM and to the CPOC (flow 39). The PA shall store the application information sent by the TLM. After that the TLM certificate is issued via the CPOC.

4.1.2.3. EA and AA

During the enrolment process the EA/AA shall bring the relevant documents (e.g. the CP its CPS and the audit report) to the corresponding root CA for approval. In case of positive checks of the documents the root CA sends an approval to the corresponding root Sub-CAs. After that, the Sub-CA (EA or AA) shall transmit electronically its signed request, and physically deliver its application form (according to section 3.2.2.1), proof of authorization and ID document to the corresponding root CA. The root CA verifies the request and the received documents (application form (containing fingerprint), proof of authorization 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.

Additionally, to the Sub-CA application form, the Sub-CA's authorized representative shall join a copy of the CPS to the RCA.

Information shall be given to an Accredited Auditor for auditing according to section 8.

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 related to the root CA service.

4.1.2.4. ITS-S

The initial registration of end-entities subjects (ITS-S) shall be done by the responsible subscriber (manufacturer /operator) with the EA (flows 33 and 35) after a successful authentication of the subscriber organization and of one of its representative as specified in section 3.2.2.4 and section 3.2.5.2.

An ITS-S may generate an EC key pair (refer to section 6.1) and create a signed EC request according to [1]. Other protocols may also be used granted that [1] is implemented.

During the registration of a normal ITS-S (no special vehicle or RSU) the EA must verify/ensure that the permissions inside the initial request are not for governmental usage. Permissions for governmental use are defined by the corresponding Member States. The detailed procedure should be defined in the corresponding CPS of the EA.

An ITS station shall be enrolled at an EA (section 3.2.5.3) by sending its initial EC request according to [1].

Upon initial registration by an authenticated Subscriber representative, the EA approves which authorization tickets the End-entity subject (i.e. the ITS-S) may obtain. Furthermore, each end-entity is assigned a trust assurance level which is reflecting the certification of the end-entity according to one of the Protection Profiles listed in section 6.1.5.2.

Regular vehicles shall have only one 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 ITS station for authorizations that are in scope of the special purpose. Special vehicles where such an exemption applies shall be defined by individual Member State. Permissions for RSUs and special vehicles shall only be granted by the responsible Member States. How the certificate process applies for such vehicles shall be defined within the CPS of root CAs or sub CAs issuing certificates for such vehicles in those Member States.

When the subscriber is in the process of migrating an ITS-station from one EA to another EA it may happen that an ITS station is registered at two (similar) EA's.

An ITS-S generates an AT key pair (refer to section 6.1) and creates an AT request according to [1]. Other protocols may also be used granted that [1] is implemented.

ITS-S sends an authorization request to the AA's URL (flows 32 and 26) by sending at the least the required information (section 3.2.3.3). The authorization validation for each request is done between AA and EA as specified in 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

It is the responsibility of the Policy Authority's Authorized Representative to authenticate the root CA's authorized representative and to approve the root CA's enrollment process according to section 3.

4.2.1.2. Identification and authentication TLM

It is the responsibility of the Policy Authority's Authorized Representative to authenticate the TLM's authorized representative and to approve the TLM's enrolment process application form according to section 3.

4.2.1.3. Identification and authentication of EA and AA

It is the responsibility of the corresponding root CA, to authenticate the EA/AA's authorized representative and to approve the EA/AA's enrollment process application form according to section 3.

A positive validation of the application form shall be confirmed to the EA/AA by the root CA. The EA/AA may then request certificates to the root CA (flow 21/24) and the root CA shall issue certificates to the corresponding EA/AA (flow 18/19).

4.2.1.4. Identification and authentication of EE subscriber

Before an ITS-S can request an EC certificate, the EE subscriber shall transmit the ITS-S identifier information to the EA in a secure way (flow 33).). The EA shall verify the request and in case of positive verification the EA shall register the ITS-S information in its database and confirms this to the EE subscriber (flow 35). This operation is done only once by the Manufacturer or Operator for each ITS-S. When an ITS-S is registered by an EA, it can request a single EC certificates it needs (flow 31) at a time. EA authenticates and verifies that the information in the EC certificate request is valid for an ITS-S.

4.2.1.5. AT

During AT request (flow 32), according to [1], the AA has to authenticate the EA from which the ITS-S received its EC. Other protocols may also be used granted that [1] is implemented. If the AA is not able to authenticate the EA, then the AT certificate request is rejected (flow 26). As a requirement, AA shall possess the EA certificate to authenticate EA and verify its response (flow 25 and 23, section 3.2.5.3).

EA authenticates the ITS-S 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

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

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

4.2.2.2. Approval or rejection of TLM certificate

The PA is responsible for approving or rejecting TLM certificates.

4.2.2.3. Approval or rejection of EA and AA certificates

The root CA verifies Sub-CA certificate requests (flow 21/24) and its respective audit reports (issued by the Accredited Auditor) upon its reception (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 thus no certificate shall be submitted to the EA/AA.

4.2.2.4. Approval or rejection of EC

Verification and validation of an EC request is performed by EA according to section 3.2.3.2 and 3.2.5.3.

If the certificate request is correct and valid, then the EA shall generate the requested certificate.

In case, the certificate request is invalid, then EA refuses the certificate request and send a response containing the reason of the certificate issuance refusal according to [1]. If an ITS-S still wants an EC, it shall make a new certificate request. Other protocols may also be used granted that [1] is implemented.

4.2.2.5. Approval or rejection of AT

The certificate request is checked by EA. The AA shall establish a communication with EA to validate the request (flow 25). The EA shall authenticate the requesting ITS-S and shall validate whether the ITS-S is entitled to get the requested AT following the CP policy (e.g. check revocation status and validate certificate time/region validity, permissions, assurance level…). The EA shall return a validation response (flow 23) and the AA shall generate the requested certificate if the response is positive and transmits it to the ITS-S. If the AT request is not correct or the EA validation response is negative, then AA refuses the AT request. If an ITS-S still wants an AT certificate, it shall make a new AT request.

4.2.3. Time to process the certificate application

4.2.3.1. Root CA certificate application

The time to process the identification and authentication process of a certificate application is during working day and shall be acted under a maximum time limit defined in the root CA CPS.

4.2.3.2. TLM certificate application

The time to process the TLM certificate application shall be acted under a maximum time limit defined in the TLM CPS.

4.2.3.3. EA and AA certificate application

The time to process the identification and authentication process of a certificate application is during working day according agreement and contract between Member State/ Private Organisation root CA and Sub-CA. The time to process a Sub-CA certificate application shall be acted under a maximum time limit defined in the Sub-CA CPS.

4.2.3.4. EC application

The time to process the EC certificate application shall be acted under a maximum time limit defined in the EA CPS.

4.2.3.5. AT application

The time to process the AT certificate application MUST be acted under a maximum time limit defined in the AA CPS

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

4.3.1.1. Root CA certificate issuance

Root CAs are issuing its own self-signed root CA certificate, link certificates, Sub-CA certificates and CRLs.

After PA approval (flow 4), the root CA certificate is sent by the root CA 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 if the root CA certificate has been approved by the PA (flow 1).

4.3.1.2. TLM certificate issuance

TLM is issuing self-signed TLM certificate to the CPOC (flow 6).

4.3.1.3. EA and AA certificate issuance

The Sub-CAs are generating a signed certificate request and transmit this request to the corresponding root CA (flow 21 and flow 24). This root CA verifies the request and issues a certificate to the requesting Sub-CA according [5].
The root CA should update the repository containing the certificates of the Sub-CAs.

4.3.1.4. EC issuance

The ITS-S shall send an EC request to the EA according to TS 102 941. The EA shall authenticate and verify that the information in the certificate request is valid for an ITS-S. Other protocols may also be used granted that [1] is implemented.

In case of positive validation, the EA shall issue a certificate according to the ITS-S registration (see 4.2.1.4) and send it to the ITS-S using an EC response message according to [1]. Other protocols may also be used granted that [1] is implemented.

If there is no registration, the EA shall generate an error code and send it to the ITS-S using an EC response message according to [1]. Other protocols may also be used granted that [1] is implemented.

EC request and EC response shall be encrypted to ensure confidentiality and signed to assure authentication and integrity.

4.3.1.5. AT issuance

The ITS-S shall send an AT Request message to the AA, according to [1]. Other protocols may also be used granted that [1] is implemented. The AA shall send an AT validation request according to [1] to the EA. The EA shall send an AT validation response to the AA. In case of a positive response, the AA shall generate an AT and send it to the ITS-S using an AT response message according to [1]. In case of a negative response, the AA shall generate an error code and send it to the ITS-S using an AT response message according to [1].

AT request and AT response shall be encrypted (only needed for vehicular ITS-S) to ensure confidentiality and signed to assure authentication and integrity.

4.3.2. Notification to Subscriber by the CA 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

The EA/AAs shall verify the certificate type, the signature and the information within the received certificate. The EA/AA shall discard all EA/AA certificates that are not correctly verified and do a new request.

4.4.1.4. ITS-S

The ITS-S shall verify the EC/AT response received from EA/AA against its original request, including the signature and the certificate chain. The ITS-S shall discard all EC/AT responses that are not correctly verified. In this case a new EC/AT request should be sent.

4.4.2. Publication of the Certificate

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

Root CA certificates are published by the TLM in the ECTL.

Sub-CAs certificates are published by the root CA.

EC and AT certificates 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 Keys and Certificates Usage

4.5.1.1. Private Keys and Certificates Usage for TLM

TLM shall use their private keys to sign its own certificates (TLM- and link certificate) and the ECTL.

TLM Certificate shall be used to verify the ECTL and to authenticate the TLM.

4.5.1.2. Private Keys and Certificates Usage for RCA

RCA shall use their private keys to sign its own certificate, CRL, link certificates and the EA/AA certificates.

RCA Certificates shall be used to verify the associated AA and EA certificates, link certificates and the CRLs.

4.5.1.3. Private Keys and Certificates Usage for EA and AA

EA shall use their private keys to sign EC certificate and for EC request decryption.

EA Certificate shall be used to verify the signature of the associated EC certificates and for EC and AT request encryption.

AA shall use their private keys to sign AT certificate and for AT request decryption.

AA Certificate shall be use to verify associated AT certificates and for AT request encryption.

4.5.1.4. Private Keys and Certificates Usage for End Entity

EE shall use their valid EC private keys to sign new EC requests. The new EC private key should be used to build inner signature in the request to proof possession of private key for EC public verification key.

EE shall use their EC private keys associated to sign AT requests. AT private key should be used to build inner signature in the request to proof possession of private key for AT public verification key.

EE shall use their AT private keys associated to sign ITS-S Message.

EE shall use their AT for ITS-S to identify themselves as the issuer of ITS-S Message.

4.5.2. Relying party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained by the certificates and to authenticate the trusted common identity of EC and AT certificates.

A root CA, EA, AA, EC and AT certificate can't be used without preliminary check from a relying party.

4.6. Certificate Renewal

Not allowed.

4.7. Certificate Re-key

4.7.1. Circumstances for certificate re-key

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 is still existing. 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

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

Root CA shall do re-keying either with link certificates (see section 4.7) or like initial certificate request (see 4.1.2.1).

4.7.2.2. TLM

The TLM does not request re-key. The re-keying process is an internal process for TLM because the TLM certificate is self-signed.

4.7.2.3. EA and AA

The Sub-CA certificate request has to be submitted in a due time in order to be sure to have a new Sub-CA certificate and operational Sub-CA's key pair before the expiration of the current Sub-CA's private key. The date of submission has also to take in account the time required for approval.

4.7.2.4. ITS-S

Not applicable**.**

4.7.3. Re-Keying process

4.7.3.1. TLM certificate

The TLM decides to re-key based on the requirement of section 6.1 and 7.2. The detailed process is defined in its CPS.

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

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

4.7.3.2. RCA certificate

The root CA decides to re-key based on the requirements of section 6.1.5 and 7.2. The detailed process should be defined in its CPS.

The root CA shall execute the re-key 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 validity of the root CA certificate start (see 5.6.2). The re-keying process shall either be done via link certificates or like an initial request.

4.7.3.3. EA and AA certificates

The EA or AA shall request a new certificate as described in the following table:

Step	Indication	Re-keying Request
1	**Key Pair Generation**	The Sub-CAs (EAs and AAs) shall generate new key pairs according to section 6.1.
2	**Generation of certificate Request and inner signature**	The Sub-CA generates a certificate request out of the new generated public key considering the naming scheme (subject_info) of section 3, the signature algorithm, if necessary the SSPs 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 proof 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 the 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 the root CA shall check the outer signature, if the verification leads to a positive result the inner signature shall be checked. In case a proof of possession of the private decryption key is done, the root CA shall also check this proof.
6	**Accept or Reject the**	If all checks lead to a positive result the request is accepted by the

	request	root CA otherwise it is rejected.
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 (if certificate was received or not) to the root CA certificate.

Table 3: Re-keying process of EA and AA

During automatic re-keying for Sub-CAs, the root CA certificate authority 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 key the inner signature should be used.

4.7.3.4. ITS-S 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. Performing 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

The infrastructure is composed by root CA, TLM, EA/AA, CPOC and TLM including their ICT components (e.g., networks and servers).

In this section, it is adopted the convention that the entity responsible for an element of the PKI, it 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…".

In addition, it is adopted the convention that term "C-ITS Trust model elements" include root CA, TLM, EA/AA, CPOC and secure network.

5.1. Physical Controls

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

The entities managing the C-ITS Trust model elements shall describe the physical, procedural and personnel security controls in their CPS. Notably, the CPS shall cover information about the site location and construction of the buildings and their physical security controls which guarantee a controlled access to all the 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

The location and construction of the facility housing the root CA, CPOC, TLM equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) 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.

Root CA, CPOC, TLM shall implement policies and procedures to ensure that the physical environments, in which the root CA equipment are installed, maintains a high level of security that guarantee:

- Is isolated from networks outside from the trust model.
- Is separated into a series of progressively secure physical perimeter (at least 2).
- Sensitive data (HSM, key pair backup, activation data …) stored in dedicated safe located in dedicated physical area under multiple access control.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include at minimum:

- Perimeter alarms, closed circuit television, reinforced walls and motion detectors.
- Two-factor authentication (e.g., smartcard and PIN) for every person and badge to go in and out in the root CA facilities and safe physical secured area.

Root CA, CPOC, TLM uses authorized 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 authorized.

5.1.1.2. EA/AA

The same applies as in the previous section 5.1.1.1.

5.1.2. Physical access

5.1.2.1. Root CA, CPOC, TLM

Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) shall always be protected from unauthorized access. The physical security mechanisms for equipment at a minimum shall be in place to:

- Monitor, either manually or electronically, for unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure container.

- Any individual non-authorized on permanent basis, who is entering secure areas shall not be left without oversight by an authorized employee of the facilities (i.e., root CA, CPOC and TLM facilities)
- Ensure an access log is maintained and inspected periodically.
- Provide at least 2 layers of increasing security such as perimeter, building, and operational room.
- Require two trusted role physical access controls to both the cryptographic HSM and activation data.

A security check of the facility housing equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation.
- For off-line component, all equipment is shut down.
- Any security containers (temper envelop, safe, ...) are properly secured.
- Physical security systems (e.g., door locks, vent covers, electricity, ...) are functioning properly.
- The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in safe. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module in a way to avoid only one person having access to private key.

A person or group of trusted role shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. 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 asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2. EA/AA

The same applies as in the previous section 5.1.2.1.

5.1.3. Power and air conditioning

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 case of external power failure and graceful shutdown of the C-ITS Trust Model equipment in case of 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

Secure facilities of C-ITS Trust Model elements (root CA, CPOC, TLM, EA and AA) should be protected in a way that minimizes 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

To prevent damaging exposure by 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.

C-ITS Trust Model elements shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorized 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

Media used within the C-ITS Trust Model elements (root CA, CPOC, TLM, EA and AA) are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Sensitive data shall be protected against being through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

An inventory shall be maintained for all information assets, with the definition of the protection requirements to those assets 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

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 unauthorized 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

Full back-ups of root CA, CPOC and TLM component off-line, sufficient to recover from system failure, are made 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 taken 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.

Access to backup data is subject to the same access requirements as the operational data. Backup data shall be encrypted and stored off-site. In case of complete loss of data, the required information for putting the root CA, CPOC and TLM back in operation shall be completely recovered from the backup data.

Private root CA, CPOC and TLM key material shall not be backed up using standard back up mechanism, but it should be done by the Backup function of the HSM.

5.1.8.2. EA/AA

The same processes described in the previous section 5.1.8.1 apply to this section.

5.2. Procedural Controls

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

5.2.1. Trusted roles

Employees, contractors, and consultants that are designated to fulfil trusted roles shall be considered to be "Trusted Persons". Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of this certificate policy.

Trusted Persons roles 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.

Trusted roles 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.

Trusted roles include, but are not limited to:

- customer service,
- system administration,
- designated engineering, and
- executives that are designated to manage infrastructural trustworthiness.

The CA shall make a clear definition of all trusted roles in its CPS.

5.2.2. Number of persons required per task

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, AA) should conform to [4], plus the requirements specified in the following paragraphs.

Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as the access and the management of CA cryptographic hardware (HSM) and its associated key material have to require the authorization of multiple Trusted Persons.

These internal control procedures shall be designed to ensure that at a minimum, two trusted persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware have to 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

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

C-ITS Trust Model elements shall verify and confirm the identity and authorization of all personnel seeking to become Trusted before such personnel 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.

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

5.2.4. Roles requiring separation of duties

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

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

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.

The part of the root CA and CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to establishing, provisioning and maintaining and suspending of services in conformance 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 which might adversely influence trust in the services it provides.

The EA and AA that serve vehicle ITS-Stations shall be separate operational entities, with separate IT infrastructure and separate IT management teams. The EA and AA shall not transfer any personal data between them according to the GDPR, except for the authorization of AT requests. The EA and AA shall transfer data related to the approval of AT requests only using the Authorization Validation protocol of [1] over a dedicated and secured interface between them.

The logfiles stored by the EA and AA can be used solely for the purpose of revoking misbehaving ECs based on ATs in intercepted malicious CAM/DEMN messages. After a CAM/DEMN message was 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 unauthorized parties and may not be shared with other entities or authorities.

Note: At the moment of drafting this version of the Certificate Policy, the design of the misbehaving function is not defined. It is planned to design the misbehaving function in the next version of the Certificate Policy.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

C-ITS Trust Model elements employ a sufficient number of personnel who possess expert knowledge, experience and appropriate qualifications necessary for the job functions and services offered. PKI personnel fulfill the requirements of "expert knowledge, experience and qualifications" 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 least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness.

5.3.2. Background Check Procedures

C-ITS Trust Model elements shall conduct background checks for personnel seeking to become Trusted Persons. Background checks shall be repeated for personnel holding Trusted Positions at least every five (5) years.

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, and
- Indications of a lack of financial responsibility.

Reports containing such information shall be evaluated by human resources and such personnel shall take actions that are reasonable in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions shall be subject to applicable law.

Background investigation of persons seeking to become a Trusted Person includes but is not limited to:

- a confirmation of previous employment,
- a check of professional references of at least 5 years, more is a plus,
- a confirmation of the highest or most relevant educational degree obtained,
- a search of criminal records.

5.3.3. Training Requirements

C-ITS Trust Model elements shall provide their personnel with the requisite training needed to perform their job responsibilities relating to CA operations competently and satisfactorily.

Training programmes shall also periodically be reviewed, and their training shall address the elements relevant to functions performed by their personnel.

Training programs shall address the elements relevant to the particular environment of the person being trained, 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, and
- disaster recovery and business continuity procedures, as well as
- Sufficient IT knowledge.

5.3.4. Retraining frequency and requirements

The persons assigned to trusted roles are required to continuously refresh their knowledge gained in the training using a training environment. Furthermore, trainings have to be repeated whenever deemed necessary every two years.

C-ITS Trust Model elements shall provide refresher training and updates to their staff to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

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 said plan shall be documented.

5.3.5. Job rotation frequency and sequence

No stipulation as long as the technical skills, experience and access rights are given. The administrators of the C-ITS Trust model elements shall ensure that any change in staff will not affect the security of the system.

5.3.6. Sanctions for unauthorized actions

A formal disciplinary process has to be defined by each C-ITS Trust Model elements to ensure that unauthorised actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges need to be withdrawn.

5.3.7. Independent Contractor Requirements

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 only under the following condition that the contractors or consultants are trusted by the entity to the same extent as if they were employees and they fulfill the same requirements applicable to employees.

Otherwise, independent contractors and consultants shall have access to C-ITS PKI secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8. Documentation Supplied to Personnel

C-ITS Trust Model elements shall provide their personnel with requisite training and access to documentation needed to perform their job responsibilities competently and satisfactorily.

5.4. Audit Logging Procedures

Requirements to the types of events recorded and the management of audit logs.

5.4.1. Types of events recorded and reported by each CA

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

Every C-ITS Trust Model element shall record the following types of audit events (if applicable):

- Physical facility access. The 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 the list of accepted and rejected certificate requests in the previous 7 days.
- Manufacturer registration. An event will be created when a manufacturer is registered.
- ITS-S registration. An event will be created when a ITS-S is registered.
- HSM management. An event will be created when a 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 shutdown 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 5 years minimum unless additional national rules apply.

The audit logs shall not permit access to privacy related data concerning ITS-S private vehicle according to the GDPR.
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.

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 related to a personal identity are encrypted and protected against non-authorized access.

At minimum, each audit record includes the following (either 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

Audit Logs shall be reviewed in response to alerts based on irregularities and incidents within their CA systems and in addition periodically every year.

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. Actions taken based on audit log reviews shall be documented.

Audit log is archived at least weekly. An administrator shall perform a manual archival if the free disk space for audit log is below the expected amount of audit log data produced during one week.

5.4.3. Retention period for audit log

Log records related to certificate life cycles are kept at least five years after the corresponding certificate expires.

5.4.4. Protection of audit log

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

Each log entry shall be signed using key material from HSM.

Event log containing information which can lead to personal identification such as a private vehicle, are encrypted in such a way that only authorized persons can read them.

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 of time that they are required to be held.

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

5.4.5. Audit log backup procedures

Audit logs and audit summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Audit log backups are protected with the same level of trust defined for the original logs.

5.4.6. Audit collection system (internal or external)

C-ITS Trust Model elements equipment 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.

At the end of each operating period and at the rekeying 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

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

The role in charge of conducting audit and roles in charge of realizing 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, 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. Actions taken as a result of these reviews are documented.

The following rules apply:

- Implement detection and prevention organizational and/or technical 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 (i) after any system or network changes that the C-ITS Trust Model elements determines are significant for PKI component, and (ii) at least once per 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 that the C-ITS Trust Model elements for CA's PKI component determines are significant.
- For online system, 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; and
- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

5.5. Records Archival

5.5.1. Types of records archived

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 minimum, the following data shall be archived (if applicable):

- PKI events records:
    - Physical facility access log of C-ITS Trust Model elements (one year minimum).
    - Trusted roles management log for C-ITS Trust Model elements (minimum 10 years).
    - IT access log for C-ITS Trust Model elements (5 years minimum).
    - CA key creation, use and destruction log (minimum 5 years) (not for TLM and CPOC).
    - certificate creation, use and destruction log (minimum 2 years).
    - PA request log (minimum 2 years).
    - Activation data management log for C-ITS Trust Model elements (minimum 5 years).
    - IT and network log for C-ITS Trust Model elements (minimum 5 years).
    - PKI documentation for C-ITS Trust Model elements (minimum 5 years).

- Security incident and audit report for C-ITS Trust Model elements (minimum 10 years).
- System equipment, software and configuration (minimum 5 years).

The C-ITS Trust Model elements shall retain all documentation relating to certificate requests and the verification thereof, and all TLM, root CAs and CA Certificates and CRL thereof, for at least 7 years after any Certificate based on that documentation ceases to be valid:

- PKI audit documentation kept by C-ITS Trust Model elements.
- CP document kept by C-ITS Trust Model elements.
- CPS documents kept by C-ITS Trust Model elements.
- Contract between PA and different 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.

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

As long as no legal regulations require a longer archival period, all records shall be maintained at least five years after the corresponding certificate has expired by the C-ITS Trust Model elements.

5.5.3. Protection of archive

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 or better than those of the PKI.

The archive shall be protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system.

The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4. System archive and storage

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 off-site secure facility.

5.5.5. Requirements for time-stamping of records

C-ITS Trust Model elements managing a revocation database shall ensure that the records contain time and date information when revocation records are created. The integrity of such time information will be implemented with cryptographic-based solutions.

5.5.6. Archive collection system (internal or external)

The archive collection system is internal.

5.5.7. Procedures to obtain and verify archive information

All the components of the C-ITS trust model shall only allow authorized Trusted Personnel Persons are able to obtain access to the archive. A root CA and CA shall describe the procedures detailing how to create, verify, package, transmit, and store archive information in the CPS.

A root CA and CA equipment shall verify integrity of the information before it is restored.

5.6. Key Changeover for C-ITS trust model elements

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

5.6.1. TLM

The TLM shall delete its private key at the end of validity of the corresponding certificate. The TLM shall generate a new key pair and corresponding TLM certificate before deactivation of the current valid private key. The TLM shall take care that the new certificate (link certificate) is inserted in the ECTL in time to be distributed to all ITS-S before the start of its validity. The link certificate and the new self-signed certificate is transferred to the CPOC.

5.6.2. Root CA

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

The root CA shall generate a new key pair and corresponding RCA 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 RCA 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 ITS-S before the start of its validity.

The root CA shall activate the new private key at the start of validity of the corresponding RCA certificate.

5.6.3. EA/AA Certificate

The EA/AA shall deactivate the current private key so that it will not issue EC/AT which have a validity that extends beyond the validity of the EA/AA certificate.

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 ITS-S before the start of its validity.

The EA/AA shall activate the new private key at the start of validity of the corresponding EA/AA certificate.

5.6.4. Auditor

No provisions.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and compromise handling

C-ITS Trust Model elements shall continuously monitor its equipment and detect potential hacking attempts or other form of compromise. In positive case the C-ITS Trust Model elements shall perform an investigation in order to determine the nature and the degree of damage

If the personnel responsible for the management of the root CA or TLM detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. In case of compromise of private key the root CA certificate shall be revoked. The scope of potential damage is assessed by the IT security experts of the PA in order to determine if the PKI needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI has been compromised. In addition, the PA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the PA business continuity plan.

Incident, Compromise and Business continuity are covered in the CPS, which may also rely upon other enterprise resources and plans for implementation.

If the personnel responsible for the management of the EA/AA/CPOC detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the personnel responsible for the management of the CA or the CPOC entity in order to determine if the PKI component needs to be rebuilt, if only some certificates need to be revoked, and/or if 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. The CA entity shall alert its own root CA and the TLM through the CPOC, in case of compromised PKI component.

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 upon other enterprise resources and plans for implementation.

Root CA and CA alerts with precise consequence of the incident each Member State representative and root CA which are under agreement with root CA and CA for C-ITS context in order to allow them to activate their own incident management plan.

5.7.2. Computing resources, software and/or data are corrupted

If a disaster is discovered that prevents the proper operation of a C-ITS Trust Model elements, the C-ITS Trust Model elements shall suspend its operation and investigated whether also the private key has been compromised (except CPOC). Defective hardware shall be replaced as fast as possible and the procedures described in 5.7.3and 5.7.4 apply.

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 need to be included in the periodic report of the CA to the TLM.

5.7.3. Entity private key compromise procedures

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
- root CA must be revoked,
- investigate on the "key-issue", which generated the compromised situation and notify the Policy Authority, which will revoke the root-CA certificate through the TLM (see section 7),
- alert all subscribers with which an agreement exists.

If an EA/AA key is compromised, lost, destroyed or suspected of being compromised, the EA/AA shall:

- suspend its operation,
- Sub-CA must be revoked
- investigates on the "key-issue" and notify the root CA,
- alert subscribers with which an agreement exists.

If an ITS-S key (whether an EC key or an AT key) is compromised, lost, destroyed or suspected of being compromised, the EA/AA to which the ITS-S is subscribed shall:

- revoke the EC of the affected ITS,
- investigate on the "key-issue" and notify the root CA,
- alert subscribers with which an agreement exists.

When any of the algorithms, or associated parameters, used by the root CA and/or CA or C-ITS-S becomes insufficient for its remaining intended usage then the PA (with recommendation of cryptographic experts) shall inform the root CA entity with which an agreement exist and change the used algorithms. See section 6 for details and the CPSs of the root CA and sub-CA.

5.7.4. Business continuity capabilities after a disaster

The C-ITS trust elements operating secure facilities for CA operations shall develop, test, maintain and implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions.

After an incident of a certain risk level, the compromised CA has to be re-audited by an accredited auditor described in section 8.

A migration plan must be defined to transfer the functions of the compromised CA to another root CA if the compromised CA shall not be able to operate any longer after the most severe incidents. At least the EU root CA shall be available to support the migration plan. The compromised CA shall cease its functions.

The Root CAs shall define the disaster recovery plan and the migration plan in the CPS.

5.8. Termination and transfer

5.8.1. TLM

The TLM is not allowed to terminate its operation but an entity managing the TLM can take over another entity.

In the event of changing the managing entity, the following shall be implemented:

- Request of change of TLM management from the old entity to the new entity to the Policy Authority.
- Approval of the Policy Authority of the change of TLM management.
- Delivery of all the audit logs and archived records from the old management entity to the new management entity.

5.8.2. Root CA

The root CA is not allowed to terminate/start its operation without establishing a migration plan (described in the related CPS), which guarantees the successive operation for all subscribers.

In the event of the termination of the root CA service, the root CA shall:

- Notify the Policy Authority.
- Notify the TLM to delete the RCA certificate from the ECTL.
- Revoke the corresponding root CA by issuing a CRL containing itself.
- Alert root CAs with which an agreement for renewal of EA/AA certificates exists.
- 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.
- Archived records are transferred to an appropriate authority.

The TLM shall delete the corresponding RCA certificate from the ECTL.

5.8.2. EA/AA

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 is not allowed to terminate/start its operation without establishing a migration plan (described in the related CPS), which guarantees the successive operation for all subscribers:

- Inform root CA by registered letter.
- Destroy the CA private key.
- Transfer its database to entity appointed by root CA.
- Stop to deliver Certificates.
- During the transfer of database and until transfer is fully operational in a new entity, maintain capability to authorize request from the responsible Privacy Authority.
- In the case of a compromised sub-CA, the root-CA shall revoke the sub-CA and shall issue a new CRL with the list of revoked sub-CAs.
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to an entity designated by root CA.

In the event of the termination of the CA 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, RCA, EA, AA

The key pair generation process shall fulfill the following requirements:

- Each participant shall be able to generate its own key pairs according to section 6.1.4 and 6.1.5.
- The key generation process shall use the algorithms and key lengths, which are described in section 6.1.4.1.
- During the key pair generation process, the requirements of “Secure storing of private keys” (see section 6.1.5) shall be satisfied.
- 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 participants.

6.1.2. EE - Vehicles

- Each vehicle shall generate its own key pairs according to section 6.1.4 and 6.1.5.

- One key pair is used for signing and verifying of signatures and the other key pair is used for deriving symmetric encryption keys and a MAC key for certificate requests (ECIES).
- The key generation processes shall use the algorithms and key lengths, which are described in section 6.1.4.1
- During key pair generation processes, the requirements of "Secure storing of private keys" (see section 6.1.5) shall be satisfied.

6.1.3. EE - Road Side Units

- Each RSU shall generate its own key pair according to section 6.1.4 and 6.1.5.
- The key generation processes shall use the algorithms and key lengths, which are described in section 6.1.4.1.
- During key pair generation processes, the requirements of "Secure storing of private keys" (see section 6.1.5) shall be satisfied.

6.1.4. Cryptographic Requirements

There are several cryptographic requirements concerning signature algorithm, key length, random number generator and link certificates (definition in ISO/IEC 14516-2) defined in the following paragraphs, which shall be achieved by the V2X-PKI participants.

6.1.4.1. Algorithm and Key Length

6.1.4.1.1. Signature Algorithms

All PKI participants (TLM, root CA, EA, AA, ITS-S) shall be able to generate key pairs and use the private key for signing operations with selected algorithms according Table 4.

All PKI participants that need to check the integrity of the ECTL, certificates and/or signed messages according to their role defined in section 1.5.6, shall support the corresponding algorithms listed in Table 5 for verification. In particular, the ITS-S station shall be able to check integrity of the ECTL.

	TLM	**root CA**	**EA**	**AA**	**ITS-S**
ECDSA_nistP256_with_SHA256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA256	-	X	X	X	O
ECDSA_brainpoolP384r1_with_SHA384	X	X	X	-	-
X indicates mandatory support O indicates optional support					

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

	TLM	root CA	EA	AA	ITS-S
ECDSA_nistP256_with_SHA256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA384	X	X	X	X	X
X indicates mandatory support O indicates optional support					

Table 5: Verification overview

If the policy authority decides, on the basis of newly found cryptographic weaknesses, all ITS-S shall be able to switch to one specific of the two algorithms ECDSA_nistP256_with_SHA256 or ECDSA_brainpoolP256_with_SHA256 as soon as possible. The actual algorithm(s) that is/are used shall be defined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

Latest four years after publication of this Certificate Policy, the PKI participants shall be able to generate key pairs and use the private key for signing operations with selected algorithms according to Table 6 This means that only newly provisioned C-ITS stations which are put into operation four years after publication of this Certificate Policy shall comply with Table 6. ITS-S already in operation should be able to generate key pairs and use the private key for signing operations with selected algorithms according to Table 6.

	TLM	root CA	EA	AA	ITS-S
ECDSA_nistP256_with_SHA256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA384	X	X	X	-	-
X indicates mandatory support O indicates optional support					

Table 6: After four years: Generating key pairs and use of private key for signing operations

6.1.4.1.2. Encryption Algorithms for Enrolment and Authorization

The PKI participants (EA, AA, ITS-S) shall be able to use public keys for encryption of Enrolment and Authorization requests/responses with selected algorithms according to Table 7. The actual algorithm that is/are used shall be defined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

The named algorithms in Table 7 indicate the key length and hash algorithm length and shall be implemented according to [5].

	TLM	**root CA**	**EA**	**AA**	**ITS-S**
ECIES_nistP256_with_AES128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	O
X indicates mandatory support O indicates optional support					

Table 7: Use of public keys for encryption of Enrolment and Authorization requests/responses

The PKI participants shall be able to generate key pairs and use the private key for the decryption of Enrolment and Authorization requests/responses with selected algorithms according to Table 8:

	TLM	**root CA**	**EA**	**AA**	**ITS-S**
ECIES_nistP256_with_AES128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	O
X indicates mandatory support O indicates optional support					

Table 8: Generate key pairs and use of private key for the decryption of Enrolment and Authorization requests/responses

Latest four years after publication of this Certificate Policy, the PKI participants shall be able to use public keys for encryption of Enrolment and Authorization requests/responses with selected algorithms according to Table 9.

	TLM	**root CA**	**EA**	**AA**	**ITS-S**
ECIES_nistP256_with_AES128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	X
X indicates mandatory support O indicates optional support					

Table 9: After four years: Use of public keys for encryption of Enrolment and Authorization requests/responses

Latest four years after publication of this Certificate Policy, the PKI participants shall be able to generate key pairs and use the private key for the decryption of Enrolment and Authorization requests/responses with selected algorithms according to Table 10:

	TLM	root CA	EA	AA	ITS-S
ECIES_nistP256_with_AES128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	X
X indicates mandatory support O indicates optional support					

Table 10: After four years: Generate key pairs and use of private key for the decryption of Enrolment and Authorization requests/responses

6.1.4.2. Crypto agility

Requirements on key lengths and algorithms need to be changed over time to keep an appropriate level of security. The Policy Authority shall monitor the need of key lengths and algorithm changes considering actual vulnerabilities, state-of-the-art cryptography. The Policy authority will draft, approve and publish an update of this Certificate Policy if it decides that the cryptographic algorithms shall be updated. In the case of a change of algorithm and/or key length indicated by a new issue of this CP, the Policy Authority will decide on a migration strategy which includes transition periods on how long old algorithms and key lengths need to be supported.

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

Changes of Root and TLM certificates shall be supported and shall be done with the help of Link certificates (see section 4.6) which are used to guarantee the transition period between the old and new Root certificates otherwise called migration of the trust model.

6.1.5. Secure storing of private keys

This section describes the requirements for secure storing and generation of key pairs and random numbers for CAs and End Entities like vehicles and RSUs. 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

A cryptographic module shall be used for:

- Generating, using, administering and storing of private keys
- Generating and using of random numbers, according to section 6.1.5.3
- Creating backups of the private keys, according to section 6.1.6
- Deletion of private keys
- The cryptographic module shall be certified with one of the following Protection Profiles (PPs), with the Assurance Level EAL-4 or higher:

  For HSM PPs:

- CEN PP HSM 419221-2 Cryptographic Module for CSP Signing Operations with Backup
- CEN PP HSM 419221-4 Cryptographic Module for CSP Signing Operations without Backup
- CEN PP HSM 419221-5 Cryptographic module for Trust Services

For SSCS PPs:

- CEN PP SSCD 419211-2 Protection Profiles for a Secure Signature Creation Device (devices with key generation)
- CEN PP SSCD 419211-3 Protection Profiles for Secure Signature Creation Device (devices with key import)

- The manual access to the cryptographic module shall claim a two factor authentication for the administrator. Additionally, this shall require an involvement of two authorized persons.
- The implementation of a cryptographic module shall ensure that keys are not accessible outside the cryptographic module. A cryptographic module shall include an access control mechanism to prevent unauthorised use of private keys.

6.1.5.2. End Entity

A cryptographic module for EEs shall be used for:

- Generating, using, administering and storing of private keys
- Generating and using of random numbers, according to section 6.1.5.3
- Secure deletion of a private keys

The cryptographic module shall be protected against unauthorized removal, replacement and modification. The cryptographic module for the End Entities shall be assessed using an approved security evaluation scheme according to suitable Protection Profiles that shall be based on ISO 15408 standard (Common Criteria). *(TBD - The Protection Profile (PP) must still be defined. A time-plan for the drafting and formalization of the PP is being defined. There may be two separate PPs for the roadside ITS-S and the vehicular ITS-S).*

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

6.1.5.3. Random Number Generator

Random numbers for key pairs shall be generated by a cryptographic module correspondent to a hybrid RNG_PTG.3. (see: W. Killmann, W. Schindler: A proposal for: Functionality classes for random number generators. Bundesamt für Sicherheit in der Informationstechnik, Version 2.0, 18.09.2011,https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_classes_for_random_number_generators_e. html). *(TBD – Depends on the outcome of the definition of the PP in section 6.1.5.2.)*

6.1.6. Backup of private keys

Generating, storing and use of Backups of private keys shall fulfill the requirements of at least the same security level as required for the original keys.

Backup of private keys shall be done by root CAs, Enrolment Authorities (EA) and Authorization Authorities (AA).

Backup of private keys shall not be done for enrolment credentials and authorization tickets.

6.1.7. Destruction of private keys

The root CAs, Enrolment-Authorities (EAs), Authorization Authorities (AAs), vehicles and RSUs shall destroy their private key and the corresponding Backups (if any), if a new key pair and corresponding certificate has been generated, successfully installed and the overlapping time (if any – CA only) has passed off. The destruction of the private key shall be done by using the mechanism, which is offered by the cryptographic module used for the key storage or as described in the corresponding Protection Profile as defined in clause 6.1.5.2.

6.2. Activation Data

Activation data refers to authentication factors which are required to operate cryptographic modules to prevent unauthorized access. The usage of Activation Data of a cryptographic device of a CA shall require action by two authorized persons.

6.3. Computer Security Controls

The Computer Security Controls of the CAs shall be designed according to the high security level by adhering to the requirements of ISO/IEC 27002.

6.4. Life Cycle Technical Controls

The CA's technical controls shall be designed including the whole life cycle of the CA. This includes especially the requirements of clause 6.1.1.2 'Crypto agility'.

6.5. Network Security Controls

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

The availability of the CA's networks shall be designed according to the estimated traffic.

7. Certificate, CRL and Trust List Profile

7.1. Certificate Profile

The certificate profiles of [5] shall be used for the Trust List Manager, Root certificates, EA certificates, AA certificates, authorization tickets and enrolment credentials. National governmental EAs may use other certificate profiles for enrolment credentials.

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

On the basis of [5] the following applies:

- Each RCA 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

All C-ITS certificate profiles shall include an issuing and an expiration date, which represents the validity time of the certificate. At each PKI level certificate generation shall be done in good time before expiration.

The validity time of the CA and enrolment credential certificates shall include an overlapping time. The TLM and root CA certificates shall be issued and put on the ECTL a maximum of 3 months and at least 1 month before their validity starts based on the start time in the certificate. This preloading phase is required to safely distribute these certificates to all correspondent relying parties according to clause 2.2. This ensures that from the beginning of the overlapping time all relying parties are already able to verify messages that are issued with a new certificate.

At the beginning of the overlapping time the successive CA, enrolment credential and authorization ticket certificates shall be issued (if applicable), distributed to and installed by the correspondent relying parties, while the current certificate shall only be used for verification, during the overlapping time.

The validity periods listed in Table 11 must not exceed the validity period of the superior certificate. Therefore there are the following restrictions:

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

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.

The following Table 11 defines the maximum validity time for C-ITS CA certificates; for AT validity period see section 7.2.1.

Entity	Max. Private Key Usage period	Maximum Validity time
Root-CA	3y	8y
EA	2y	5y
AA	4y	5y
EC	3y	3y
TLM	3y	4y
		y = years, m = months

Table 11: Validity periods of the certificates inside the C-ITS trust model

7.2.1. Pseudonym Certificates

In this context, pseudonyms are implemented by Authorization Tickets. As a consequence, the term Authorization Ticket is used rather than pseudonym in this section.

The requirements defined in this section do only apply to ATs of vehicular ITS-S sending CAM and DENM messages where the risk of location privacy is applicable. ATs for roadside ITS-S and vehicular ITS-S used for special functions where location privacy is not applicable (e.g., marked emergency and law enforcers vehicles) do not have specific requirements on ATs certificates.

Definitions:

- Definition of the *validity period* for ATs. The validity period is the duration of time during which an AT is valid, i.e., the time period between the AT's starting date and its expiration date.
- Definition of *preloading period* for ATs: Preloading is the possibility for 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.
- Definition of *usage period* for ATs. The usage period is the amount of time during which an AT is effectively used to sign CAM/DENM messages.
- Definition of *number of maximum parallel ATs:* is the number of ATs from which an ITS station can choose at any given time when signing a CAM/DENM message, i.e., it is the number of different ATs issued to one ITS station that are valid at the same time.

Requirements:

- The preloading period for ATs shall not exceed 3 months.
- The validity period for ATs shall not exceed 1 week. *(TBD – the final value still needs to be decided/adapted in conjunction with discussions on preserving privacy, which is not the scope of this document)*.

- The number of maximum parallel ATs for ITS-S shall not be more than 60 to mitigate the risk of a Sybil attack *(TBD – the final value still needs to be decided/adapted in conjunction with discussions on preserving privacy)*.

- The usage period of an AT depends on the AT change strategy and on the amount of time that a vehicle is in operation, but is limited by the number of maximum parallel ATs and the validity period. Namely, the average usage period for one ITS station is at least the operational time of the vehicle during one validity period divided by the number of maximum parallel ATs.

7.2.2. Authorisation Tickets for roadside ITS-S

Requirements (same definitions of terms apply as in section 7.2.1):

- The preloading period for ATs shall not exceed 3 months.

- The number of maximum parallel ATs for ITS-S shall not be more than 2 per ITS-AID.

7.3. Revocation of certificates

Authorization tickets are not revoked by its corresponding CAs. Therefore these certificates shall have a short lifetime and cannot be issued too long before they will become valid. The allowed certificate lifecycle parameter values are mentioned in 7.2.

7.3.1. Revocation of CA certificates

The root CAs, Enrolment Authority and Authorization Authority certificates shall be revocable. Revoked certificates of root CAs, EAs and AAs shall be published on a Certificate Revocation List (CRL). This CRL shall be signed by its corresponding root CA and shall use the profile described in section 7.4. For revocation of root CA certificates, the corresponding root CA issues a CRL containing itself. Additionally, the Trust List Manager shall remove the revoked root CA from the Trust List and shall issue a new Trust List. Expired certificates shall be removed from the corresponding CRL and Trust List.

Revocation of certificates is done for following circumstances:

- The root CAs have reason to believe or strongly suspects that compromise of the corresponding private key has occurred.

- 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) within the certificate is incorrect or has changed.

- If a security incident that addresses the certificate owner takes place.

- If the audit (see section 8) leads to a negative result.

A Subscriber shall immediately notify the CA of a known or suspected compromise of its private key. It has to be assured, that only authenticated requests will result in revoked certificates.

7.3.2. Revocation of Enrolment Credential

Revocation of enrolment credentials is done with an internal blacklist in a revocation database with a timestamp, which is generated and maintained by each Enrolment Authority. The blacklist of revoked vehicle EC's is never published and shall be kept confidential and only used by the corresponding Enrolment Authority to verify the validity of the corresponding enrolment credentials during the request of authorization tickets and new enrolment credentials.

7.4. Certificate Revocation List Profile

The CRL profile defined in [1] shall be used for all certificate revocation lists mentioned in Section 7.3.1. *(TBD: CRL Profile is currently not published yet in the ETSI standard)*

The C-ITS stations shall be able to interpret and process CRLs according to [1].

7.5. European Certificate Trust List Profile

The ECTL is a signed list, which is created and issued by the Trust List Manager and contains the root CAs of the C-ITS trust model to guarantee trust relations.

The format and content of the ECTL is defined in ETSI TS XX XXXX *(TBD. An ETSI standard will define it)*.

Each ECTL shall be timestamped. The ECTL is containing the root CAs of all vehicles and infrastructures.

The C-ITS stations shall be able to interpret and process the ECTL according to [1].

8. Compliance Audit and Other Assessments

8.1. Topics covered by audit and audit basis

The purpose of a compliance audit is to verify that TLM, root CA, EA, AA operate in accordance with the applicable CP. The TLM, root CAs, EAs and AAs shall select an independent acting and certified auditor for auditing this CP and its CPS. The audit shall be combined with an ISO 27001 and ISO 27002.

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

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

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

1. Conformity the TLM, root CA, EA, AA Certification Practice Statement has with this Certificate Policy.
2. Conformity of the TLM, root CA, EA, AA intended practices with its Certification Practice Statement prior to operation.
3. Conformity of the TLM, root CA, EA, AA practices and operational activities its Certification Practice Statement during operation.

In this case, the audit shall include all requirements of this Certificate Policy to be fulfilled by the TLM, root CA, EA, AA to be audited. The scope of the audit shall cover the proceeding of the CA in the C-ITS PKI including all processes mentioned in its CP and CPS, the premises and responsible persons

The auditor shall provide a detailed report of the audit to whom it ordered: root CA (flow 36), EA, AA or the PA (flow 16 and 40).

8.2. Frequency of the audits

A root CA, TLM, EA and AA shall order a compliance audit for itself to an independent and Accredited Auditor in the following cases:

- At First set-up of root CA, TLM, EA/AA (level 1 and 2 compliance).
- At every change of CPS, CP of root CA, TLM, EA/AA (level 1, 2 and level 3 compliance).
- Regularly, and at least every three years during operation of a root CA, TLM and EA/AA (level 3 compliance)

8.3. Identity/qualifications of auditor

The CA to be audited shall select an independently acting and accredited company/organisation ("Auditing Body") or Accredited Auditors to audit the CA according to this Common Certificate Policy. The Auditing Body shall be accredited and certified by a member of the European Accreditation[1].

8.4. Auditor's relationship to audited entity

The auditor shall be independent to the audited entity.

8.5. Actions taken as a result of deficiency

In case of a TLM with a non-compliant audit report, the PA shall order the TLM to take immediate preventive actions.

In case of a new application of root CA with a non-compliant audit report, the PA shall reject the application and send a corresponding rejection to the root CA (flow 4). In this case the root CA will be suspended, it need to take corrective actions, re-order the audit and request a new PA approval. The root CA shall not be allowed to issue certificates during the suspension.

In case of a regular root CA audit, or case of a change of root CA's CPS, and depending on the nature of the incompliance described in the audit report, the PA 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 the root CA on the CRL. The PA shall send a corresponding rejection to the root CA (flow 4). In this case the root CA will need to take corrective actions, re-order a full audit (level 1 to 3) and request a new PA approval. Alternatively the PA may decide to not revoke the root CA, but to give it a grace period in which

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

the root CA shall undertake corrective actions, re-order an audit and re-submit the audit report to the PA. In this case, the root CA operation must be suspended and it is not allowed to issue certificates and CRLs.

In case of an EA/AA audit, the root CA /private company shall decide to accept the report. Depending on the audit result the root CA shall decide to or revoke the EA/AA certificate according to rules defined in the root CA's CPS. The root CA shall at all time assure compliance of the EA/AA to this CP.

8.6. Communication of results

The root CA and the TLM shall provide the audit report for the root CA itself to the PA (flow 16). The root CA and TLM shall store all audit reports it has ordered. The PA shall send a corresponding approval rejection (flow 4) to the root CA and TLM.

The root CA shall provide a certificate of conformity to the corresponding EA/AA.

9. Other Business and Legal Matters

9.1. Fees

One principle of the implemented EU C-ITS trust model is that the root CAs together are fully financing the regularly recurring costs of operation of the Policy Authority and the central elements TLM and CPOC for performing the activities as defined in this Certificate Policy.

The root CAs are entitled to take fees from their sub CAs. This rule also applies to the EU Root CA.

For the full time of operation at least one root CA, EA and AA shall always be available for every participant of the C-ITS Trust model on a non-discriminatory basis.

Each root CA is entitled to charge the fees it pays for policy authority and the central elements TLM and CPOC to the own registered participants of the C-ITS trust model including the enrolled and authorized C-ITS stations.

9.2. Financial Responsibility

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

Each root CA needs to demonstrate the financial viability of the legal entity implementing the root CA for at least three years. This financial viability plan is part of the initial set of documents for enrolment and needs to be updated every three years and reported to policy authority.

Each root CA must report the applied charges structure for EA /AA and the enrolled and authorized C-ITS Stations per year to Operations Manager (see Security Policy) and the policy authority to demonstrate its financial sustainability.

All financial and legal responsible entities of the roots CA, EA, AA and the central elements (CPOC, TLM) of the C-ITS Trust model are required to cover their operational duties with insurance levels adequate to compensate for errors of operations and for financial recoverage of their duties if one of the technical elements fails.

9.3. Confidentiality of Business Information

The following records of shall be kept confidential and private:

- Root CA, EA, AA application records whether approved or disapproved,
- Root CA, EA, AA and TLM audit reports
- Root CAs, EA, AA, CPOC and TLM 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 PA, root CAs, EA, AA, TLM and CPOC needs to be kept confidential

9.4. Privacy Plan

The CPSs of the root CAs and the EAs/AAs shall define the plan and the requirements for the treatment of personal information and privacy on the basis of the General Data Protection Regulation (GDPR) and other applicable legislative frameworks (e.g., national frameworks).

References

[1]. ETSI TS 102 941 Ver. 1.1.12, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. *(TBD. Standard not yet published)*.

[2]. ETSI TS 102 940 V1.2.1, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, June 2012.

[3]. Policy, Certificate. 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 V2.0.5, Intelligent Transport Systems (ITS); Security; Security header and certificate formats. *(TBD. Standard not yet published)*.

[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.

[8]. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119, 1997