



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

*EU C-ITS Certificate Policy
Release 3.0 – May 2024*

2024

This document is a publication by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Email: JRC-CPOC@ec.europa.eu

EU Science Hub

<https://joint-research-centre.ec.europa.eu>

JRC137554

Ispra: European Commission, 2024

© European Union, 2024



The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that is not owned by the European Union permission must be sought directly from the copyright holders.

How to cite this report: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) - Release 3.0, European Commission, Joint Research Centre, Ispra, 2024, JRC137554.

Contents

Abstract	10
1 Introduction	11
1.1 Overview and scope of this policy	11
1.1.1 Target audience	13
1.2 Version History	13
1.3 PKI participants	14
1.3.1 Introduction	14
1.3.2 C-ITS certificate policy authority	18
1.3.3 Trust list manager	19
1.3.4 Accredited PKI auditor	19
1.3.5 C-ITS point of contact (CPOC)	20
1.3.6 Operational roles	20
1.4 Certificate usage	22
1.4.1 Applicable domains of use	22
1.4.2 Limits of responsibility	22
1.5 Certificate policy administration	22
1.5.1 Updating of CPSs of CAs listed in the ECTL	22
1.5.2 CPS approval procedures	23
2 Publication and repository responsibilities	24
2.1 Methods for the publication of certificate information	24
2.2 Time or frequency of publication	24
2.3 Repositories	25
2.4 Access controls on repositories	25
2.5 Publication of certificate information	26
2.5.1 Publication of certificate information by the TLM	26
2.5.2 Publication of certificate information by CAs	26
3 Identification and authentication	27
3.1 Naming	27
3.1.1 Types of name	27
3.1.1.1 Names for TLM, root CAs, EAs, AAs	27

3.1.1.2	Names for end-entities.....	27
3.1.1.3	Identification of certificates.....	27
3.1.2	Need for names to be meaningful	27
3.1.3	Anonymity and pseudonymity of end-entities.....	28
3.1.4	Rules for interpreting various name forms.....	28
3.1.5	Uniqueness of names.....	28
3.2	Initial identity validation.....	28
3.2.1	Method to prove possession of private key.....	28
3.2.2	Authentication of organisation identity.....	28
3.2.2.1	Authentication of root CAs' organisation identity.....	28
3.2.2.2	Authentication of TLM organisation identity	29
3.2.2.3	Authentication of sub-CAs organisation identity.....	30
3.2.2.4	Authentication of end-entities' subscriber organisation.....	30
3.2.3	Authentication of individual entity.....	31
3.2.3.1	Authentication of TLM/CA individual entity	31
3.2.3.2	Authentication of C-ITS stations' subscriber identity.....	32
3.2.3.3	Authentication of C-ITS stations' identity.....	32
3.2.4	Non-verified subscriber information.....	32
3.2.5	Validation of authority.....	32
3.2.5.1	Validation of TLM, root CA, EA, AA.....	32
3.2.5.2	Validation of C-ITS station subscribers	32
3.2.5.3	Validation of C-ITS stations.....	32
3.2.6	Criteria for interoperation.....	33
3.3	Identification and authentication for re-key requests.....	33
3.3.1	Identification and authentication for routine re-key requests.....	33
3.3.1.1	TLM certificates.....	33
3.3.1.2	Root CA certificates.....	33
3.3.1.3	EA/AA certificate renewal or re-keying	33
3.3.1.4	End-entities' enrolment credentials.....	34
3.3.1.5	End-entities' authorisation tickets.....	34
3.3.2	Identification and authentication for re-key requests after revocation.....	34

3.3.2.1	CA certificates	34
3.3.2.2	End-entities' enrolment credentials.....	34
3.3.2.3	End-entities' authorisation requests	34
3.4	Identification and authentication for revocation request.....	35
3.4.1	Root CA/EA/AA certificates.....	35
3.4.2	C-ITS station enrolment credentials	35
3.4.3	C-ITS station authorisation tickets.....	35
4	Certificate Life-cycle operational requirements.....	36
4.1	Certificate application.....	36
4.1.1	Who can submit a certificate application	36
4.1.1.1	Root CAs	36
4.1.1.2	TLM.....	36
4.1.1.3	EA and AA	36
4.1.1.4	C-ITS station.....	36
4.1.2	Enrolment process and responsibilities.....	37
4.1.2.1	Permissions for special purposes.....	37
4.1.2.2	Root CAs	37
4.1.2.3	TLM.....	37
4.1.2.4	EA and AA	38
4.1.2.5	C-ITS station.....	38
4.2	Certificate application processing	39
4.2.1	Performing identification and authentication functions.....	39
4.2.1.1	Identification and authentication of root CAs.....	39
4.2.1.2	Identification and authentication of the TLM.....	39
4.2.1.3	Identification and authentication of EA and AA.....	40
4.2.1.4	Identification and authentication of EE subscriber	40
4.2.1.5	Authorisation tickets.....	40
4.2.2	Approval or rejection of certificate applications	40
4.2.2.1	Approval or rejection of root CA certificates	40
4.2.2.2	Approval or rejection of TLM certificate.....	40
4.2.2.3	Approval or rejection of EA and AA certificates.....	40

4.2.2.4	Approval or rejection of EC	41
4.2.2.5	Approval or rejection of AT	41
4.2.3	Time to process the certificate application.....	41
4.2.3.1	Root CA certificate application.....	41
4.2.3.2	TLM certificate application.....	41
4.2.3.3	EA and AA certificate application	42
4.2.3.4	EC application.....	42
4.2.3.5	AT application.....	42
4.3	Certificate issuance.....	42
4.3.1	CA actions during certificate issuance.....	42
4.3.1.1	Root CA certificate issuance	42
4.3.1.2	TLM certificate issuance.....	42
4.3.1.3	EA and AA certificate issuance	42
4.3.1.4	EC issuance.....	42
4.3.1.5	AT issuance.....	43
4.3.2	CA's notification to subscriber of issuance of certificates.....	43
4.4	Certificate acceptance	43
4.4.1	Conducting certificate acceptance.....	43
4.4.1.1	Root CA.....	43
4.4.1.2	TLM.....	43
4.4.1.3	EA and AA	43
4.4.1.4	C-ITS station.....	43
4.4.2	Publication of the certificate.....	44
4.4.3	Notification of certificate issuance	44
4.5	Key pair and certificate usage	44
4.5.1	Private key and certificate usage.....	44
4.5.1.1	Private key and certificate usage for TLM.....	44
4.5.1.2	Private key and certificates usage for root CAs	44
4.5.1.3	Private key and certificate usage for EAs and AAs.....	44
4.5.1.4	Private key and certificate usage for end-entity.....	45
4.5.2	Relying party public key and certificate usage	45

4.6	Certificate renewal.....	45
4.7	Certificate re-key	45
4.7.1	Circumstances for certificate re-key	45
4.7.2	Who may request re-key	45
4.7.2.1	Root CA.....	45
4.7.2.2	TLM.....	45
4.7.2.3	EA and AA	46
4.7.2.4	C-ITS station.....	46
4.7.3	Re-keying process.....	46
4.7.3.1	TLM certificate	46
4.7.3.2	Root CA certificate	46
4.7.3.3	EA and AA certificates	46
4.7.3.4	C-ITS station certificates.....	47
4.8	Certificate modification	47
4.9	Certificate revocation and suspension	47
4.10	Certificate status services	48
4.10.1	Operational characteristics	48
4.10.2	Service availability	48
4.10.3	Optional features.....	48
4.11	End of subscription	48
4.12	Key escrow and recovery	48
4.12.1	Subscriber	48
4.12.1.1	Which key pair can be escrowed	48
4.12.1.2	Who can submit a recovery application	48
4.12.1.3	Recovery process and responsibilities	48
4.12.1.4	Identification and authentication	48
4.12.1.5	Approval or rejection of recovery applications	48
4.12.1.6	KEA and KRA actions during key pair recovery.....	48
4.12.1.7	KEA and KRA availability	48
4.12.2	Session key encapsulation and recovery policy and practices	49
5	Facility, management and operational controls.....	50

5.1 Physical controls	50
5.1.1 Site location and construction	50
5.1.1.1 Root CA, CPOC, TLM.....	50
5.1.1.2 EA/AA.....	51
5.1.2 Physical access	51
5.1.2.1 Root CA, CPOC, TLM.....	51
5.1.2.2 EA/AA.....	52
5.1.3 Power and air conditioning.....	52
5.1.4 Water exposures	52
5.1.5 Fire prevention and protection.....	53
5.1.6 Media management	53
5.1.7 Waste disposal	53
5.1.8 Off-site backup.....	53
5.1.8.1 Root CA, CPOC and TLM.....	53
5.1.8.2 EA/AA.....	54
5.2 Procedural controls.....	54
5.2.1 Trusted roles.....	54
5.2.2 Number of persons required per task.....	55
5.2.3 Identification and authentication for each role.....	55
5.2.4 Roles requiring separation of duties.....	55
5.3 Personnel controls.....	56
5.3.1 Qualifications, experience and clearance requirements.....	56
5.3.2 Background check procedures.....	57
5.3.3 Training requirements.....	57
5.3.4 Retraining frequency and requirements	58
5.3.5 Job rotation frequency and sequence	58
5.3.6 Sanctions for unauthorised actions.....	58
5.3.7 Independent contractor requirements	58
5.3.8 Documentation supplied to personnel.....	59
5.4 Audit logging procedures.....	59
5.4.1 Types of event to be recorded and reported by each CA.....	59

5.4.2	Frequency of processing log.....	60
5.4.3	Retention period for audit log.....	61
5.4.4	Protection of audit log.....	61
5.4.5	Audit log backup procedures.....	61
5.4.6	Audit collection system (internal or external).....	61
5.4.7	Notification to event-causing subject.....	61
5.4.8	Vulnerability assessment.....	62
5.5	Record archiving.....	62
5.5.1	Types of record archived.....	62
5.5.2	Retention period for archive.....	63
5.5.3	Protection of archive.....	64
5.5.4	System archive and storage.....	64
5.5.5	Requirements for time-stamping of records.....	64
5.5.6	Archive collection system (internal or external).....	64
5.5.7	Procedures to obtain and verify archive information.....	64
5.6	Key changeover for C-ITS trust model elements.....	64
5.6.1	TLM.....	64
5.6.2	Root CA.....	65
5.6.3	EA/AA certificate.....	65
5.6.4	Auditor.....	65
5.7	Compromise and disaster recovery.....	65
5.7.1	Incident and compromise handling.....	65
5.7.2	Corruption of computing resources, software and/or data.....	66
5.7.3	Entity private key compromise procedures.....	66
5.7.4	Business continuity capabilities after a disaster.....	67
5.8	Termination and transfer.....	68
5.8.1	TLM.....	68
5.8.2	Root CA.....	68
5.8.3	EA/AA.....	68
6	Technical security controls.....	70
6.1	Key-pair generation and installation.....	70

6.1.1	TLM, root CA, EA, AA.....	70
6.1.2	End-entity — C-ITS station.....	70
6.1.3	Void.....	70
6.1.4	Cryptographic requirements.....	70
6.1.4.1	Algorithm and key length - signature algorithms.....	71
6.1.4.2	Algorithm and key length - encryption algorithms for enrolment and authorisation.....	72
6.1.4.3	Crypto-agility.....	72
6.1.5	Secure storing of private keys.....	73
6.1.5.1	Root CA, sub-CA and TLM level.....	73
6.1.5.2	End-entity.....	73
6.1.6	Backup of private keys.....	74
6.1.7	Destruction of private keys.....	75
6.2	Activation data.....	75
6.3	Computer security controls.....	75
6.4	Life-cycle technical controls.....	75
6.5	Network security controls.....	75
7	Certificate profiles, CRL, CTL and ECTL.....	76
7.1	Certificate profile.....	76
7.2	Certificate validity.....	76
7.2.1	General.....	76
7.2.2	AT for C-ITS-Stations of type Itss_WithPrivacy [2].....	77
7.2.3	AT for C-ITS stations of type Itss_NoPrivacy [2].....	78
7.3	Revocation of certificates.....	78
7.3.1	Revocation of Root CA, EA and AA certificates.....	78
7.3.2	Blocklisting of enrolment credentials.....	79
7.3.3	Revocation of authorisation tickets.....	79
7.4	Certificate revocation list.....	79
7.5	Certificate trust list.....	79
7.6	European certificate trust list.....	79
8	Compliance audit and other assessments.....	80
8.1	Topics covered by audit and audit basis.....	80

8.2	Frequency of the audits	80
8.3	Identity/qualifications of auditor	81
8.4	Auditor's relationship to audited entity.....	81
8.5	Action taken as a result of deficiency	81
8.6	Communication of results	81
9	Other provisions.....	82
9.1	Fees.....	82
9.2	Financial responsibility	82
9.3	Confidentiality of business information	82
9.4	Privacy plan.....	83
10	Conclusions.....	84
	References	85
	List of abbreviations and definitions	86
	List of figures.....	89
	List of tables.....	90

Abstract

This document is the Certificate Policy for the deployment and operation of European Cooperative Intelligent Transport Systems (C-ITS). The purpose of this policy is to define the European C-ITS trust model based on public key infrastructure (PKI), the scope of the overall EU C-ITS security credential management system (EU CCMS) and the requirements for the management of public key certificates for C-ITS applications.

The document is the Release 3.0 and it is an update of Release 2.0 prepared for the C-ITS Delegated Act proposal in 2019. Release 3.0 is based on the contributions and active review by the members of the Editing Team of the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941).

1 Introduction

Since 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" on 30th of November 2016, the Commission has worked, 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.

This document is the Release 3.0 of the Certificate Policy for Deployment and Operation of European C-ITS, which was approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in April 2024.

1.1 Overview and scope of this policy

This certificate policy defines the European C-ITS trust model based on public key infrastructure (PKI) and the scope of the overall EU C-ITS security credential management system (EU CCMS). It also defines requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. At its highest level, the PKI is composed of a set of root CAs 'enabled' as a result of the trust list manager (TLM) inserting their certificates in a European certificate trust list (ECTL), which is issued and published by the central entity TLM (see section 1.3). Level 1 and Level 2 are the operational ECTLs as defined in the CPOC Protocol [10].

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

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

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

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

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

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

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

The CP also defines mandatory obligations applying to:

- the TLM;
- each root CA whose certificates are listed in the ECTL;
- each sub-CA certified by a root CA;

- all end-entities;
- each member organisation responsible for, or operating, one of the C-ITS trust model entities.

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

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

1.1.1 Target audience

The target audience of this document are all the stakeholders involved in the deployment and operation of C-ITS in Europe, including the European Commission, Member States' competent authorities, notably the Ministries for Transport, road infrastructure operators responsible, vehicle manufacturers implementing and deploying C-ITS, C-ITS station manufacturers, C-ITS PKI service providers, and sectorial/Industry associations (e.g. Car2Car Communication Consortium, C-ROADS).

1.2 Version History

The Certificate Policy will continue to be revised in the implementation process of the EU CCMS based on the needs of the C-ITS stakeholders, and in particular the CPA.

A first version was published in June 2017. The document was prepared by 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. Following a broad consultation process, the contents were updated and Release 1.1 published in June 2018.

Release 2.0 was prepared for the C-ITS Delegated Act proposal in March 2019.

Release 3.0 (2024) has been heavily revised and multiple sections have been updated while keeping the original structure and whenever possible the requirements numbering of earlier versions of this policy.

Table 1. Releases

Release	Date
Release 1	June 2017
Release 1.1	June 2018
Release 2.0	March 2019
Release 3.0	May 2024

1.3 PKI participants

1.3.1 Introduction

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

PKI roles consist of:

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

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

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

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

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

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

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

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

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

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

Figure 1: C-ITS trust model architecture

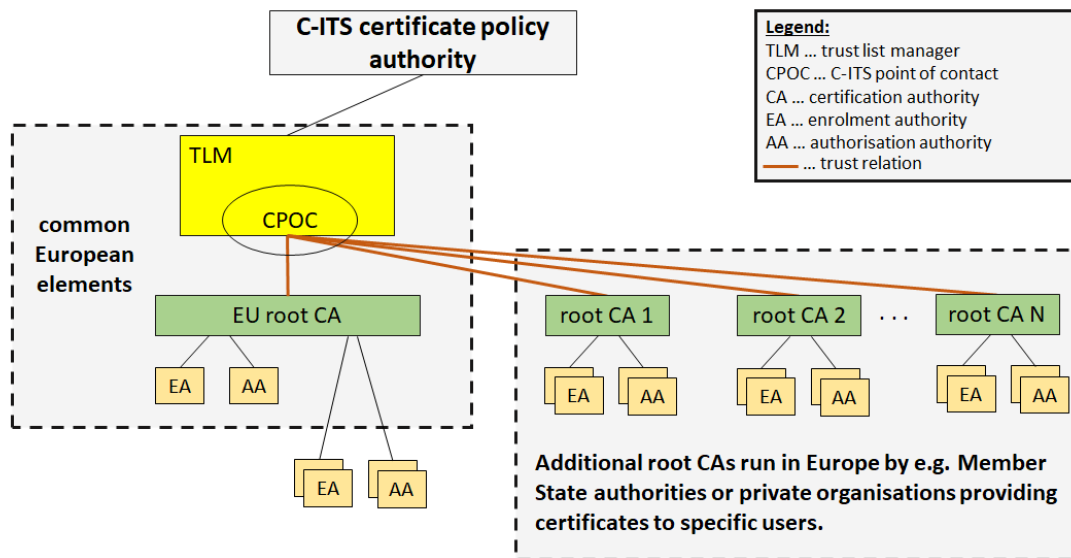


Figure 2: C-ITS Trust model information flows including butterfly key mechanism

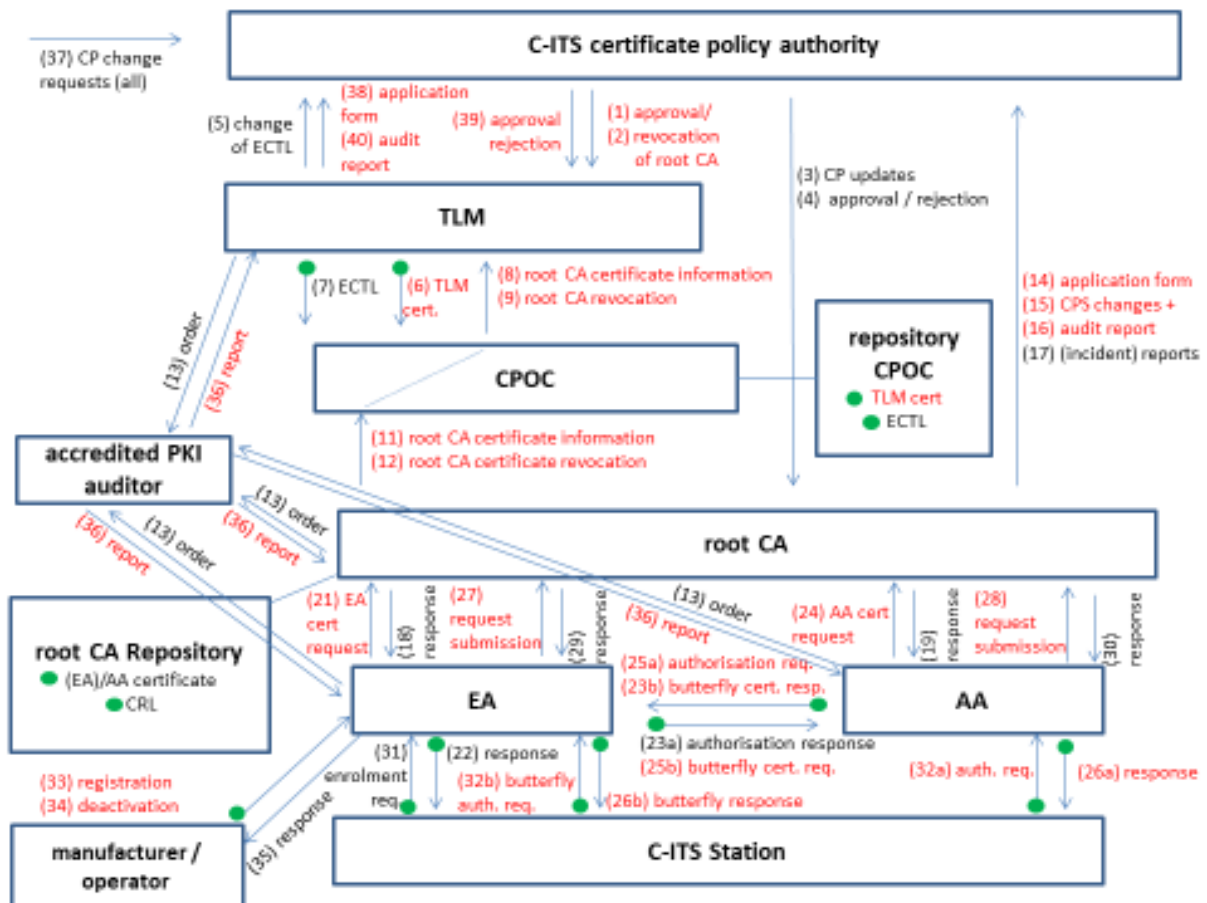


Table 2: Detailed description of information flows in the C-ITS trust model

Flow ID	From	To	Content	Reference
flow 1	CPA	TLM	approval of root CA application	8
flow 2	CPA	TLM	information on revocation of root CA	8.5
flow 3	CPA	root CA	CP updates	1.5
flow 4	CPA	root CA	approval/rejection of root CA application form or the CPS request changes or the audit process.	8.5, 8.6
flow 5	TLM	CPA	notification of change of ECTL	4, 5.8.1
flow 6	TLM	CPOC	TLM certificate	4.4.2
flow 7	TLM	CPOC	ECTL	4.4.2
flow 8	CPOC	TLM	root CA certificate information	4.3.1.1
flow 9	CPOC	TLM	root CA certificate revocation	7.3
flow 10	CPOC	all end-entities	TLM certificate	4.4.2
flow 11	root CA	CPOC	root CA certificate information	4.3.1.1
flow 12	root CA	CPOC	root CA certificate revocation	7.3
flow 13	root CA/EA/AA	auditor	audit order	8
flow 14	root CA	CPA	root CA application form — initial request	4.1.2.2

flow 15	root CA	CPA	root CA application form — CPS changes	1.5.2
flow 16	root CA	CPA	root CA application form — audit summary report	8.6
flow 17	root CA	CPA	root CA incident reports, including revocation of a sub-CA (EA, AA)	[9], 7.3.1
flow 18	root CA	EA	EA certificate response	4.2.2.3
flow 19	root CA	AA	AA certificate response	4.2.2.3
flow 20	root CA	All	EA/AA certificate, CRL	4.4.2
flow 21	EA	root CA	EA certificate request	4.2.2.3
flow 22	EA	C-ITS station	enrolment credential response	4.3.1.4
flow 23	EA	AA	23a: authorisation response 23b: butterfly certificate response	4.2.2.5
flow 24	AA	root CA	AA certificate request	4.2.2.3
flow 25	AA	EA	25a: authorisation request 25b: butterfly certificate request	4.2.2.5
flow 26	AA	C-ITS station	26a: authorisation ticket response 26b: butterfly response	4.3.1.5
flow 27	EA	root CA	request submission	4.1.2.4
flow 28	AA	root CA	request submission	4.1.2.4
flow 29	root CA	EA	response	4.12 and 4.2.1

flow 30	root CA	AA	response	4.12 and 4.2.1
flow 31	C-ITS station	EA	enrolment credential request	4.2.2.4
flow 32	C-ITS station	AA	32a: authorisation ticket request 32b: butterfly authorization request	4.2.2.5
flow 33	manufacturer / operator	EA	registration	4.2.1.4
flow 34	manufacturer / operator	EA	deactivation	7.3
flow 35	EA	manufacturer / operator	response	4.2.1.4
flow 36	auditor	root CA/EA/AA/TLM	report	8.1
flow 37	all	CPA	CP change requests	1.5
flow 38	TLM	CPA	application form	4.1.2.3
flow 39	CPA	TLM	approval/rejection	4.1.2.3
flow 40	TLM	CPA	Audit summary report	4.1.2.3

1.3.2 C-ITS certificate policy authority

- (1) The C-ITS certificate policy authority (CPA) is composed of the representatives of public and private stakeholders (e.g. Member States, vehicle manufacturers, etc.) participating in the C-ITS trust model. It is responsible for three sub-roles:
- Policy documents (notably this CP as well as the C-ITS Security Policy [9] and CPOC protocol [10]) management, including the following tasks:
 - approval of the present version and future change requests;
 - deciding on the review of the document change requests and recommendations submitted by other PKI participants or entities;

- deciding on the release of new versions;
 - PKI authorisation management, including:
 - defining, deciding and publishing the CPS approval and CA audit procedures (collectively referred to as 'CA approval procedures');
 - scrutiny of the audit summary reports from the accredited PKI auditor for all root CAs and the TLM in order to ascertain that the operations and CPS are compliant with this CP;
 - authorising the CPOC to operate and report regularly;
 - authorising the TLM to operate and report regularly;
 - authorising the root CAs to operate and report regularly;
 - notifying the TLM about the list of approved or non-approved root CAs and their certificates on the basis of received approval reports of the root CAs and regular operations reports.
 - Defining, deciding and publishing the detailed procedures for change management of policy documents, reporting and of operational procedures for handling requests from TLM/CPOC and root CAs (collectively referred to as 'CPA Terms of Reference').
- (2) The CPA's authorised representative is responsible for authenticating the TLM's and root CAs' authorised representative and approving the TLM's and root CAs' enrolment and application forms.

1.3.3 Trust list manager

- (3) The TLM is a single entity appointed by the CPA.
- (4) The TLM is responsible for:
- the operation of the ECTL in accordance with the common valid CP and regular activity reporting to the CPA for the overall secure operation of the C-ITS trust model;
 - receiving root CA certificates from the CPOC;
 - including/excluding root CA certificates in/from the ECTL upon notification by the CPA;
 - signing the ECTL;
 - the regular and timely transmission of the ECTL to the CPOC.

1.3.4 Accredited PKI auditor

- (5) The accredited PKI auditor is responsible for:
- performing or organising audits of root CAs, TLM and sub-CAs;

- providing the audit report and audit report summary (from an initial or periodic audit) to the contractor of the audit in line with the requirements in section 8 below. The audit report shall include recommendations from the accredited PKI auditor;
- notifying the entity managing the root CA of the successful or unsuccessful execution of an initial or periodic audit of the sub-CAs;
- assessing CPSs' compliance with this CP.

1.3.5 C-ITS point of contact (CPOC)

- (6) The CPOC is a single entity appointed by the CPA. The CPA's authorised representative is responsible for authenticating the CPOC's authorised representative and approving the CPOC enrolment process application form. The CPA is responsible for authorising the CPOC to operate as set out in this section.
- (7) The CPOC is responsible for:
- establishing and contributing to the secure communication exchange between all entities of the C-ITS trust model in an efficient and fast way;
 - reviewing procedural change requests and recommendations submitted by other trust model participants (e.g. root CAs);
 - Receiving initial registration/enrolment requests according to the CPOC Protocol [10];
 - transmitting root CA certificates to the TLM;
 - publication of the common trust anchor (current public key and link certificate of the TLM);
 - publication of the ECTL.

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

1.3.6 Operational roles

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

Table 3: Operational roles

Functional element	PKI role ([3] and [4])	Detailed role ([2])
root certification authority	CA/RA (registration authority)	Provides EA and AA with proof that it may issue ECs or ATs

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

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

(9) *Registration authorities:*

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

1.4 Certificate usage

1.4.1 Applicable domains of use

- (10) Certificates issued under the present CP are intended to be used to validate digital signatures in the cooperative ITS communication context in accordance with the reference architecture of [2].
- (11) The certificate profiles in [5] determine certificate uses for the TLM, root CAs, EAs, AAs and end-entities.

1.4.2 Limits of responsibility

- (12) Certificates are not intended, nor authorised, for use in:
 - circumstances that offend, breach or contravene any applicable law, regulation (e.g. GDPR), decree or government order;
 - circumstances that breach, contravene or infringe the rights of others;
 - breach of this CP or the relevant subscriber agreement;
 - any circumstances where their use could lead directly to death, personal injury or severe environmental damage (e.g. through failure in the operation of nuclear facilities, aircraft navigation or communication, or weapons control systems);
 - circumstances that contravene the overall objectives of greater road safety and more efficient road transport in Europe.

1.5 Certificate policy administration

1.5.1 Updating of CPSs of CAs listed in the ECTL

- (13) Each root CA listed in the ECTL shall publish its own CPS, which must be in compliance with this policy. A root CA may add additional requirements, but shall ensure that all requirements of this CP are met at all times.
- (14) Each root CA listed in the ECTL shall implement an appropriate change process for its CPS document. The key properties of the change process shall be documented in the public part of the CPS.
- (15) The change process shall ensure that all changes to this CP are carefully analysed and, if necessary for compliance with the CP as amended, the CPS is updated within the timeframe laid down in the implementation step of the change process for the CP. In particular, the change process shall involve emergency change procedures that ensure timely implementation of security-relevant changes to the CP.
- (16) The change process shall include appropriate measures to verify CP compliance for all changes to the CPS. Any changes to the CPS shall be clearly documented. Before a new version of a CPS is implemented, its compliance with the CP shall be confirmed by an accredited PKI auditor.

- (17) The root CA shall notify the CPA of any change made to the CPS with at least the following information:
- an exact description of the change;
 - the rationale for the change;
 - a report from the accredited PKI auditor confirming compliance with the CP;
 - contact details of the person responsible for the CPS;
 - planned timescale for implementation.

1.5.2 CPS approval procedures

- (18) Before starting its operations, a prospective root CA shall present its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and the audit report summary to the CPA as part of the approval of the root CA enrolment request (flow 15, flow 16).
- (19) A root CA shall present changes to its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and the audit result will be forwarded to the CPA for information (flow 15).
- (20) An EA/AA shall present its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and the audit report summary to the root CA as part of the approval of the EA/AA enrolment request.
- (21) The accredited PKI auditor shall assess the CPS in accordance with section 8.
- (22) The accredited PKI auditor shall communicate the results of the CPS assessment as part of the audit report, as set out in section 8.1. The CPS shall be accepted or rejected as part of the audit report acceptance referred to in sections 8.5 and 8.6.

2 Publication and repository responsibilities

2.1 Methods for the publication of certificate information

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

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

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

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

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

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

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

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

(29) Root CAs shall be able to support at least the regular publication defined in this section for publishing them to their subscribed members and relying parties, taking all necessary steps to ensure secure transmission, as referred to in section 4.

2.2 Time or frequency of publication

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

- For the regular publication of updated certificate information (e.g. changes in the ECTL or CRL composition), a maximum period of three months is required for the safe operation of the C-ITS network.

- Root CAs shall publish their CA certificates and CRLs as soon as possible after issuance.
- For the publication of the CRL and CTL, the root CA repository shall be used.

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

(30b) This section specifies only the time or frequency of the regular publication. Means of connectivity to update C-ITS stations with the applicable ECTLs, CTLs (or AA certificates) and CRLs within a week of their publication (under normal operation conditions, e.g. with cellular coverage, vehicle in actual operation, etc.) shall be implemented in accordance with the requirements in this document.

2.3 Repositories

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

- all root CAs shall use a repository implementing the interface (Rest-API) standardised in [1] of its own currently active EA/AA certificate information and CRL to publish certificates for the other PKI participants. The repository of each root CA shall support all required access controls (section 2.4) and transmission times (section 2.2) for every method of distribution of C-ITS-related information;
- the TLM's repository (which stores the ECTL L1 and L2 and TLM certificates published by the CPOC, for example) should be based on a publication mechanism able to ensure the transmission times set out in section 2.2 for every method of distribution.

2.4 Access controls on repositories

(32) The requirements on access control to repositories of certificate information shall at least comply with the general standards of secure information handling outlined in ISO/IEC 27001 [6] and with the requirements in section 4. In addition, they shall reflect the process security needs to be established for the single process steps in the publication of certificate information:

- This includes the implementation of the repository for TLM certificates and the ECTL in the TLM/CPOC. Each root CA or repository operator shall implement access controls to prevent unauthorised entities from adding to, amending or deleting repository entries.
- The exact access control mechanisms shall be part of the respective CPS.
- For each root CA repositories shall comply with the same requirements for access control procedures regardless of the place or contractual link to the service provider operating the repository.

2.5 Publication of certificate information

2.5.1 Publication of certificate information by the TLM

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

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

2.5.2 Publication of certificate information by CAs

(34) Root CAs in the European common C-ITS trust domain shall publish the following information in the repository referred to in section 2.3:

- The CTL for all valid CA certificates covering their subordinate EAs and AAs;
- the CRLs for all revoked CA certificates covering their subordinate EAs and AAs;

Root CAs may also optionally publish their root certificate(s) and EA/AA certificates.

All certificate information and documents for the general public shall be publicly available without restrictions.

3 Identification and authentication

3.1 Naming

3.1.1 Types of name

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

- (35) The name in the TLM certificate shall consist of a single CertificateID attribute with the reserved value 'EU-TLM'.
- (36) The name for root CAs shall consist of a single CertificateID attribute with a value allocated by the CPA. The uniqueness of names is the sole responsibility of the CPA and the TLM shall maintain the registry of root CA names upon notification by the CPA (approval, revocation/removal of a root CA). CertificateIDs in certificates are limited to 32 bytes. Each root CA proposes its name to the CPA in the application form (flow 14). The CPA is responsible for checking name uniqueness. If the name is not unique, the application form is rejected (flow 4). Further details on this process shall be defined in the CPOC protocol [10].
- (37) The name in each EA/AA certificate may consist of a single CertificateID attribute with a value generated by the issuer of the certificate. The uniqueness of names is the sole responsibility of the issuing root CA.
- (38) The EA and AA certificates shall not use a name greater than 32 octets, because subject_name in certificates are limited to 32 octets.
- (39) Void.

3.1.1.2 *Names for end-entities*

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

3.1.1.3 *Identification of certificates*

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

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity and pseudonymity of end-entities

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

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

- (43) Names for the TLM, root CAs, EAs, AAs and canonical IDs for C-ITS stations shall be unique.
- (44) The TLM shall ensure in the registration process of a given root CA in the ECTL that its certificate identifier (HashedId8) is unique. The root CA shall ensure in the issuance process that the certificate identifier (HashedId8) of each subordinate CA is unique.
- (45) The HashedId8 of an EC shall be unique within the issuing CA. The HashedId8 of an AT does not have to be unique.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of organisation identity

3.2.2.1 **Authentication of root CAs' organisation identity**

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

- postal address;
 - e-mail address;
 - the name of a physical contact person in the organisation;
 - telephone number;
 - digital fingerprint (i.e. SHA 256 hashvalue) of the root CA's certificate in printed form;
 - cryptographic information (i.e. cryptographic algorithms, key lengths) in the root CA certificate;
 - all permissions that the root CA is allowed to use and to pass to the sub-CAs.
- (50) The CPA shall check the identity of the organisation and other registration information provided by the certificate applicant for the insertion of a root CA certificate in the ECTL.
- (51) The CPA shall collect either direct evidence, or an attestation from an appropriate and authorised source (e.g. company registration document), of the identity (e.g. name) and, if applicable, any specific attributes of subjects to which a certificate is issued. Submitted evidence may be in the form of paper or electronic documentation.
- (52) The subject's identity shall be verified at the time of registration by appropriate means (e.g. company registration document).
- (53) At each certificate application, evidence shall be provided of:
- the full name of the organisational entity (private organisation, government entity or non-commercial entity);
 - nationally recognised registration or other attributes that may be used, as far as possible, to distinguish the organisational entity from others with the same name.

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

3.2.2.2 Authentication of TLM organisation identity

- (54) The organisation operating the TLM shall provide evidence of the identification and accuracy of the name and associated data in order to enable appropriate verification at initial creation and re-keying of the TLM certificate.
- (55) The subject's identity shall be verified at the time of certificate creation or re-keying by appropriate means and in accordance with the present CP.
- (56) Organisation evidence shall be provided as specified in section 3.2.2.1.

3.2.2.3 *Authentication of sub-CAs organisation identity*

- (57) The root CA shall check the identity of the organisation and other registration information provided by certificate applicants for sub-CA (EA/AA) certificates.
- (58) At a minimum, the root CA shall:
- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
 - use postal mail or a comparable procedure requiring the certificate applicant to confirm certain information about the organisation, that it has authorised the certificate application and that the person submitting the application on behalf of the applicant is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.
- (59) Validation procedures for issuing CA certificates shall be documented in a CPS of the root CA.

3.2.2.4 *Authentication of end-entities' **subscriber organisation***

- (60) Before the subscriber of end-entities (manufacturer/operator) can register with a trusted EA to enable its end-entities for sending EC certificate requests, the EA shall:
- check the identity of the subscriber organisation and other registration information provided by the certificate applicant;
 - check that the C-ITS station operator is in compliance with the C-ITS Security Policy [9];
 - check that the C-ITS station type (i.e. the concrete product based on brand, model and version of the C-ITS station) meets all of the following compliance assessment criteria:
 - Certification of compliance with the C-ITS Security Policy [9].
 - Self-declaration of full conformity with all relevant standards for interoperability based on relevant profiles [11] [12].
 - check if an IVI *serviceProviderId* [12] delegation is requested, that a valid delegation agreement is in place between delegator and delegate [12].
- (61) At a minimum, the EA shall:
- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
 - use postal mail or a comparable procedure to require the certificate applicant to confirm certain information about the organisation, that it has authorised

the certificate application and that the person submitting the application on its behalf is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.

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

3.2.3 Authentication of individual entity

3.2.3.1 *Authentication of TLM/CA individual entity*

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

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

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

- (64) To verify his/her identity, the authorised representative of a root CA, EA, AA or subscriber shall provide documentation proving that he/she works for the organisation (certificate of authorisation). He/she shall also show an official ID.
- (65) For the initial enrolment process (flow 31/flow 32), a representative of the EA/AA shall provide the corresponding root CA with all necessary information (see section 4.1.2).
- (66) The personnel at the root CA shall verify the identity of the certificate applicant's representative and all associated documents, applying the requirements of 'trusted personnel' as set out in section 5.2.1. The process of validating application information and generating the certificate by the root CA shall be carried out by 'trusted persons' at the root CA, under at least dual supervision, as they are sensitive operations within the meaning of section 5.2.2.

3.2.3.2 *Authentication of C-ITS stations' subscriber identity*

- (67) Subscribers are represented by authorised end-users in the organisation who are registered at the issuing EA and AA. These end-users designated by organisations (manufacturers or operators) shall prove their identity and authenticity before:
- registering the EE at its corresponding EA, including its canonical public key, canonical ID (unique identifier) and the permissions in accordance with the EE;
 - registering at any AA to which the organisation is a subscriber.

3.2.3.3 *Authentication of C-ITS stations' identity*

- (68) EE subjects of ECs shall authenticate themselves when requesting ECs (flow 31) by using their canonical private key for the initial authentication. The EA shall check the authentication using the canonical public key corresponding to the EE. The canonical public keys of the EEs are brought to the EA before the initial request is executed, by a secure channel between the C-ITS station manufacturer or operator and the EA (flow 33).
- (69) EE subjects of ATs shall authenticate themselves when requesting ATs (flow 32a and 32b) by using their unique enrolment private key. The AA shall forward the signature to the EA (flow 25a) for validation; the EA shall validate it and confirm the result to the AA (flow 23a). When using the butterfly key mechanism, the EA shall send the individual butterfly certificate requests to the AA (flow 25b) after validation; the AA shall issue the individual ATs and return them to the EA (flow 23b) according to [1].

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

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

- (70) Every organisation shall identify in the CPS at least one method to contact the organisation (e.g. a security contact e-mail) to request new certificates and renewals. The naming rules in section 3.2.3 shall apply.

3.2.5.2 *Validation of C-ITS station subscribers*

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

3.2.5.3 *Validation of C-ITS stations*

- (72) A C-ITS station's subscriber may register C-ITS stations at a specific EA (flow 33) as long as it is authenticated at that EA. The authentication process shall be defined in the CPS of the EA.

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

3.2.6 Criteria for interoperation

- (73) For communication between C-ITS stations and EAs (or AAs), the C-ITS station shall be able to establish secure communication with EAs (or AAs), i.e. to implement authentication, confidentiality and integrity functions, as specified in [1].
- (74) The EA and AA shall support certificate requests and responses that comply with [1], which provides for a secure AT request/response protocol supporting the anonymity of the requester *vis-à-vis* the AA and separation of duties between the AA and the EA. Other protocols may be used, provided that [1] is implemented. To prevent disclosure of C-ITS stations' long-term identity, communication between a mobile C-ITS station and an EA shall be confidential (e.g. communication data shall be encrypted end-to-end).
- (75) The AA shall submit an authorisation validation request (flow 25a) for each authorisation request it receives from an EE certificate subject. The EA shall validate this request as well as all butterfly authorization requests from EE (flow 32b) with respect to:
 - the status of the EE at the EA;
 - the validity of the signature;
 - the requested ITS Application IDs (ITS-AID) and permissions;
 - the status of service provision of the AA to the subscriber.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key requests

3.3.1.1 TLM certificates

- (76) The TLM shall generate a key pair and two certificates: one self-signed and one link certificate (details on TLM Link Certificates see [10]) as referred to in section 7.

3.3.1.2 Root CA certificates

Not applicable.

3.3.1.3 EA/AA certificate renewal or re-keying

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

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

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

3.3.1.4 *End-entities' enrolment credentials*

- (79) Prior to the expiry of an existing EC, the EE shall request a new certificate (flow 31) to maintain continuity of certificate usage. The EE shall generate a new key pair to replace the expiring key pair and request a new certificate containing the new public key; the request shall be signed with the current valid EC private key.
- (80) The EE may sign the request with the newly created private key (inner signature) to prove possession of the new private key. The whole request is then signed (oversigned) with the current valid private key (outer signature) and encrypted to the receiving EA as specified in [1], to ensure the confidentiality, integrity and authenticity of the request.

3.3.1.5 *End-entities' authorisation tickets*

- (81) Issuing of ATs shall be based on the processes defined in [1]. Other protocols may be used, provided that [1] is implemented.

3.3.2 Identification and authentication for re-key requests after revocation

3.3.2.1 *CA certificates*

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

3.3.2.2 *End-entities' enrolment credentials*

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

3.3.2.3 *End-entities' authorisation requests*

Not applicable, since ATs are not revoked.

3.4 Identification and authentication for revocation request

3.4.1 Root CA/EA/AA certificates

- (84) Requests to delete a root CA certificate from the ECTL shall be authenticated by the root CA to the TLM (flow 12 and flow 9). Requests to revoke an EA/AA certificate shall be authenticated by the relevant root CA and sub-CA itself.
- (85) Acceptable procedures for authenticating a subscriber's revocation requests include:
- a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked;
 - communication with the subscriber providing reasonable assurances that the person or organisation requesting revocation is in fact the subscriber. Depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.2 C-ITS station enrolment credentials

- (86) The C-ITS station subscriber may request to blocklist one or more ECs of a previously registered C-ITS station at an EA (flow 34). The requesting subscriber shall create a request for blocklisting of the relevant ECs. The EA shall authenticate the blocklisting request before processing it and confirm the blocklisting of the ECs. The EA shall consider blocklisted ECs as invalid.
- (87) The EA may blocklist one or more ECs of a C-ITS station in accordance with section 7.3.

3.4.3 C-ITS station authorisation tickets

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

4 Certificate Life-cycle operational requirements

4.1 Certificate application

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

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

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

4.1.1 Who can submit a certificate application

4.1.1.1 Root CAs

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

4.1.1.2 TLM

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

4.1.1.3 EA and AA

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

4.1.1.4 C-ITS station

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

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

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

4.1.2 Enrolment process and responsibilities

4.1.2.1 *Permissions for special purposes*

- (97) In addition to the security baseline, the issuance of certificates for special (governmental) purposes (i.e. special mobile and fixed C-ITS stations) by the PKI shall only be enabled to PKI participants proving the authorization by the competent public authorities of the respective Member State.
- (97b) The issuance of certificates with delegated IVI *serviceProviderId* [12], as part of a Delegation according to [12], shall only be enabled to subscribers duly referenced in the corresponding delegation agreement.

4.1.2.2 *Root CAs*

- (98) The CPOC shall lay down the practical rules in agreement with the CPA in the CPOC protocol ([10]) on the enrolment process based on the guidelines in this section: After being audited (flow 13 and flow 36, section 8), root CAs may apply for insertion of their certificate(s) in the ECTL at the CPA (flow 14). The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA by the root CA's authorised representative and that contains at least the information referred to in sections 3.2.2.1, 3.2.3 and 3.2.5.1.
- (99) The root CA's application form shall be signed by its authorised representative.
- (100) In addition to the application form, the root CA's authorised representative shall provide a copy of the root CA's audit report summary to the CPA for approval (flow 16). In cases of positive approval, the CPA generates and sends a certificate of conformity to the CPOC/TLM and the corresponding root CA.
- (101) The root CAs authorised representative shall then bring its application form (containing the fingerprint of the self-signed certificate), the official ID and a proof of authorisation to the CPOC/TLM. The self-signed certificate shall be delivered electronically to the CPOC/TLM. The CPOC/TLM shall verify all documents and the self-signed certificate.
- (102) In cases of positive verifications, the TLM shall add the root CA's certificate to the ECTL based on the notification from the CPA (flow 1 and flow 2). The detailed process is described in the CPS of the TLM.
- (103) Void.

4.1.2.3 *TLM*

- (104) After being audited, the TLM may enrol with the CPA. The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA (flow 38) by the TLM's authorised representative and contains at least the information referred to in sections 3.2.2.2 and 3.2.3.
- (105) The TLM's application form shall be signed by its authorised representative.
- (106) First, the TLM shall generate its self-signed certificate and transmits it securely to the CPA. The TLM then shall bring its application form (containing the fingerprint of the

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

4.1.2.4 *EA and AA*

- (107) During the enrolment process, the EA/AA shall bring the relevant documents (e.g. the CPS and the audit report) to the corresponding root CA for approval (flow 27/flow 28). In cases of positive checks of the documents, the root CA shall send an approval to the corresponding sub-CAs (flow 29/flow 30). The sub-CA (EA or AA) shall then transmit its signed request electronically, and physically deliver its application form (in accordance with section 3.2.2.1), proof of authorisation and ID document to the corresponding root CA. The root CA shall verify the request and the received documents (application form containing the fingerprint, which is the SHA 256 hashvalue of the sub-CA request, proof of authorisation and ID Document). If all checks lead to a positive result, the root CA shall issue the corresponding sub-CA certificate. Detailed information how an initial request is done is described in its specific CPS.
- (108) In addition to the sub-CA application form, the sub-CA's authorised representative shall attach a copy of the CPS to the root CA.
- (109) Information shall be given to an accredited PKI auditor for auditing in accordance with section 8.
- (110) If a sub-CA is owned by an entity different than the entity that owns the root CA, before issuing a sub-CA certificate request, the sub-CA's entity shall sign a contract regarding the root CA service.

4.1.2.5 *C-ITS station*

- (111) The initial registration of end-entities subjects (C-ITS stations) shall be carried out by the responsible subscriber (manufacturer /operator) with the EA (flow 33 and flow 35) after successful authentication of the subscriber organisation and one of its representatives in line with sections 3.2.2.4 and 3.2.5.2.
- (112) A C-ITS station may generate an EC key pair (see section 6.1) and create a signed EC request in accordance with [1].
- (113) During the registration of a normal C-ITS station (as opposed to a special mobile or fixed C-ITS station), the EA shall verify the validity of permissions in the initial request. The requirement for handling permissions for governmental use is defined in section 4.1.2.1. The detailed procedure for the registration and response of the EA to the manufacturer/operator (flow 33 and flow 35) shall be set out in the corresponding CPS of the EA.
- (114) A C-ITS station shall be enrolled at an EA (section 3.2.5.3) by sending its initial EC request in accordance with [1].

- (115) Upon initial registration by an authenticated subscriber representative, the EA approves which ATs the end-entity subject (i.e. the C-ITS station) may obtain. Furthermore, each end-entity is assigned a trust assurance level, which is related to the certification of the end-entity in accordance with one of the protection profiles listed in section 6.1.5.2.
- (116) Regular vehicles shall have only one C-ITS station that is registered at one EA. Special-purpose vehicles (such as police cars and other special-purpose vehicles with specific rights) may be registered at an additional EA or have one additional C-ITS station for authorisations within the scope of the special purpose. Vehicles to which such an exemption applies shall be defined by the Member States responsible. Permissions for special mobile and fixed C-ITS stations shall be granted only by the Member States responsible. The CPS of root CAs or sub-CAs issuing certificates for such vehicles in those Member States shall determine how the certificate process applies to such vehicles.
- (117) Where the subscriber is in the process of migrating a C-ITS station from one EA to another EA, the C-ITS station may be registered at two (similar) EAs.
- (118) A C-ITS station shall generate an AT key pair (see section 6.1) and creates an AT request in accordance with [1].
- (119) C-ITS stations shall send an authorisation request to the AA's URL (flow 32a and flow 26b) by sending at least the required information referred to in section 3.2.3.3. The AA and EA shall validate the authorisation for each request in accordance with sections 3.2.6 and 4.2.2.5. When the butterfly key mechanism is used, C-ITS stations shall send a butterfly authorization request to the EA (flow 32b and flow 26b) by sending at least the required information referred to in Section 3.2.3.3. The EA and AA shall validate the butterfly authorization for each request in accordance with Sections 3.2.6 and 4.2.2.5.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

4.2.1.1 *Identification and authentication of root CAs*

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

4.2.1.2 *Identification and authentication of the TLM*

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

4.2.1.3 Identification and authentication of EA and AA

- (122) The corresponding root CA is responsible for authenticating the EA/AA's authorised representative and approving its enrolment process application form in accordance with section 3.
- (123) The root CA shall confirm its positive validation of the application form to the EA/AA. The EA/AA may then send a certificate request to the root CA (flow 21/flow 24), which shall issue certificates to the corresponding EA/AA (flow 18/flow 19).

4.2.1.4 Identification and authentication of EE subscriber

- (124) Registration of C-ITS stations in the EA shall only be allowed to authenticated EE subscribers (3.2.3.2). EE subscribers shall securely transmit the C-ITS stations canonical information to the EA (flow 33). The security associated to the registration operation shall be described in the CPS of the EA. Once registered, a C-ITS station may request an EC certificate (flow 31) in accordance with [1]. C-ITS station operators shall be able to confirm the proper registration of a station (flow 35).

4.2.1.5 Authorisation tickets

- (125) During authorisation requests (flow 32a and 32b), in accordance with [1], the AA and EA shall authenticate each other. If either is not able to authenticate the other, the request is rejected (flow 26a and 26b). As a requirement, AA and EA shall possess the respective other certificate to authenticate and verify the communication (flow 25a, 25b, flow 23a, and 23b, section 3.2.5.3).
- (126) The EA shall authenticate the C-ITS station requesting an AT by verifying its EC (flow 25 and flow 23). When the butterfly key mechanism is used, the EA shall authenticate the C-ITS station using its EC without communication to the AA.

4.2.2 Approval or rejection of certificate applications

4.2.2.1 Approval or rejection of root CA certificates

- (127) The TLM inserts/deletes the root CA certificates into/from the ECTL in accordance with the approval/rejection of the CPA (flow 1/flow 2).
- (128) The TLM shall verify the signature, information and encoding of root CA certificates after receiving an approval by the CPA (flow 1). After positive validation and the CPA's approval, the TLM shall put the corresponding root certificate on the ECTL and notify the CPA (flow 5).

4.2.2.2 Approval or rejection of TLM certificate

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

4.2.2.3 Approval or rejection of EA and AA certificates

- (130) The root CA shall verify sub-CA certificate requests (flow 21/flow 24) and the relevant reports (issued by the accredited PKI auditor) on receiving them (flow 36, section 8) from the corresponding sub-CA of the root CA. If the check of the request leads to a

positive result, the corresponding root CA shall issue a certificate to the requesting EA/AA (flow 18/flow 19); otherwise, the request shall be rejected and no certificate shall be issued to the EA/AA.

4.2.2.4 Approval or rejection of EC

- (131) The EA shall verify and validate EC requests in accordance with sections 3.2.3.2 and 3.2.5.3.
- (132) If the certificate request in accordance with [1] is correct and valid, the EA shall generate the requested certificate.
- (133) Where the certificate request is invalid, the EA shall refuse it and send a response setting out the reason for refusal in accordance with [1]. If a C-ITS station still wants an EC, it shall make a new certificate request.

4.2.2.5 Approval or rejection of AT

- (134) The certificate request is checked by the EA. The AA shall establish communication with EA to validate the request (flow 25a). The EA shall authenticate the requesting C-ITS station and validate whether it is entitled to receive the requested AT following the CP (e.g. by checking the revocation status and validate certificate time/region validity, permissions, assurance level, etc.). The EA shall return a validation response (flow 23a) and, if the response is positive, the AA shall generate the requested certificate and transmit it to the C-ITS station. If the AT request is not correct or the EA validation response is negative, the AA shall refuse the request. If a C-ITS station still requires an AT, it shall make a new authorisation request. When the butterfly key mechanism is used, the certificate request is also checked by the EA. The EA shall authenticate the requesting C-ITS station and validate whether it is entitled to receive the requested AT following the CP (e.g. by checking the revocation status and validate certificate time/region validity, permissions, assurance level, etc.). If the validation is successful, the EA shall return a positive authorization response (flow 22b) and the EA shall send the individual AT requests to the AA. If the AT request is not correct and the EA validation is negative, the EA refuses the request. If a C-ITS station still requires an AT, it shall make a new authorisation request.

4.2.3 Time to process the certificate application

4.2.3.1 Root CA certificate application

- (135) The time to process the identification and authentication of a certificate application shall be subject to a maximum time limit laid down in the CPOC Protocol [10].

4.2.3.2 TLM certificate application

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

4.2.3.3 EA and AA certificate application

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

4.2.3.4 EC application

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

4.2.3.5 AT application

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Root CA certificate issuance

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

(141) After CPA approval (flow 4), the root CA sends its certificate to the TLM through the CPOC to be added to the ECTL (flow 11 and flow 8) (see section 4.1.2.2). The TLM shall check whether the CPA has approved the certificate (flow 1).

4.3.1.2 TLM certificate issuance

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

4.3.1.3 EA and AA certificate issuance

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

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

4.3.1.4 EC issuance

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

- (146) In cases of positive validation, the EA shall issue a certificate in accordance with the C-ITS station registration (see section 4.2.1.4) and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.
- (147) If there is no registration, the EA shall generate an error code and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.
- (148) EC requests and EC responses shall be encrypted to ensure confidentiality and signed to ensure authentication and integrity.

4.3.1.5 *AT issuance*

- (149) EAs and AAs shall support issuance of ATs in accordance with [1]. EAs and AAs shall support individual and/or butterfly authorization management. Other protocols may be used, provided that [1] is implemented.
- (150) AT requests and AT responses shall be encrypted (only needed for mobile C-ITS stations) to ensure confidentiality and signed to ensure authentication and integrity.

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

Not applicable.

4.4 Certificate acceptance

4.4.1 Conducting certificate acceptance

4.4.1.1 *Root CA*

Not applicable.

4.4.1.2 *TLM*

Not applicable.

4.4.1.3 *EA and AA*

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

4.4.1.4 *C-ITS station*

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

4.4.2 Publication of the certificate

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

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

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

(156) ECs and ATs are not published.

4.4.3 Notification of certificate issuance

There are no notifications of issuance.

4.5 Key pair and certificate usage

4.5.1 Private key and certificate usage

4.5.1.1 *Private key and certificate usage for TLM*

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

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

4.5.1.2 *Private key and certificates usage for root CAs*

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

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

4.5.1.3 *Private key and certificate usage for EAs and AAs*

(161) EAs shall use one private key to sign ECs and a different private key for enrolment request and butterfly AT request decryption. A given EA private key shall be used for one purpose only, either signing or decryption of messages.

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

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

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

4.5.1.4 *Private key and certificate usage for end-entity*

- (165) EEs shall use the private key corresponding to a valid EC to sign a new enrolment request as defined in [1]. The new private key shall be used to build the inner signature in the request to prove possession of the private key corresponding to the new EC public key.
- (166) EEs shall use the private key corresponding to a valid EC to sign an authorisation request as defined in [1]. The private key corresponding to the new AT should be used to build the inner signature in the request to prove possession of the private key corresponding to the new AT public key.
- (167) EE shall use the private key corresponding to an appropriate AT to sign C-ITS messages as defined in [5].

4.5.2 Relying party public key and certificate usage

- (168) Relying parties shall use the trusted certification path and associated public keys for the purposes referred to in the certificates and to authenticate the trusted common identity of ECs and ATs.
- (169) Root CA, EA and AA certificates, ECs and ATs shall not be used without a preliminary check by a relying party.

4.6 Certificate renewal

Not allowed.

4.7 Certificate re-key

4.7.1 Circumstances for certificate re-key

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

4.7.2 Who may request re-key

4.7.2.1 *Root CA*

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

4.7.2.2 *TLM*

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

4.7.2.3 EA and AA

(173) The sub-CA's certificate request shall be submitted in due time in order to be sure to have a new sub-CA certificate and operational sub-CA key pair before expiry of the current private sub-CA key. The re-keying shall be done as defined in section 4.7.3.3. The date of submission shall also take account of the time required for approval.

4.7.2.4 C-ITS station

(173b) The C-ITS station shall re-key its EC according to [1] .

4.7.3 Re-keying process

4.7.3.1 TLM certificate

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

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

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

4.7.3.2 Root CA certificate

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

(178) The root CA shall execute the re-keying process in due time (before the root CA certificate expires) in order to allow for insertion of the new certificate in the ECTL before the root CA certificate becomes invalid (see section 5.6.2 and [10]). The re-keying process shall be carried out either via link certificate message or like an initial request.

4.7.3.3 EA and AA certificates

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

Table 4: Re-keying process for EAs and AAs

Step	Indication	Re-keying request
1	Key-pair generation	The sub-CAs (EAs and AAs) shall generate new key pairs in accordance with section 6.1.

2	Generation of certificate request and inner signature	The sub-CA shall generate a certificate request out of the newly generated public key considering the naming scheme (subject_info) of section 3, the signature algorithm, the Service Specific Permissions (SSP) and optional additional parameters, and shall generate the inner signature with the corresponding new private key. If an encryption key is required, the sub-CA shall also prove possession of the corresponding private decryption key.
3	Generate outer signature	The whole request shall be signed with the current valid private key to guarantee the authenticity of the signed request.
4	Send request to root CA	The signed request shall be submitted to the corresponding root CA.
5	Verification of request	The corresponding root CA shall verify the integrity and authenticity of the request. First, it shall check the outer signature. If the verification is positive, it shall check the inner signature. Where there is proof of possession of the private decryption key, it shall also check this proof.
6	Accept or reject request	If all checks lead to a positive result, the root CA shall accept the request; otherwise, it rejects it.
7	Generate and issue certificate	The root CA shall generate a new certificate and distributes it to the requesting sub-CA.
8	Send response	The sub-CA shall send a status message (as to whether or not the certificate was received) to the root CA.

(180) During automatic re-keying for sub-CAs, the root CA may ensure that the requestor is indeed in possession of its private decryption key. Appropriate protocols for proof of possession of private decryption keys shall be applied, for instance as defined in RFC 210 and 4211.

4.7.3.4 C-ITS station certificates

Not applicable for AT.

4.8 Certificate modification

Not allowed.

4.9 Certificate revocation and suspension

See section 7

4.10 Certificate status services

4.10.1 Operational characteristics

Not applicable

4.10.2 Service availability

Not applicable

4.10.3 Optional features

Not applicable

4.11 End of subscription

Not applicable

4.12 Key escrow and recovery

4.12.1 Subscriber

4.12.1.1 Which key pair can be escrowed

Not applicable.

4.12.1.2 Who can submit a recovery application

Not applicable.

4.12.1.3 Recovery process and responsibilities

Not applicable.

4.12.1.4 Identification and authentication

Not applicable.

4.12.1.5 Approval or rejection of recovery applications

Not applicable.

4.12.1.6 KEA and KRA actions during key pair recovery

Not applicable.

4.12.1.7 KEA and KRA availability

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management and operational controls

- (181) The PKI is composed of the root CA, the EA/AA, the CPOC and the TLM, including their ICT components (e.g. networks and servers).
- (182) In this section, the entity responsible for an element of the PKI is identified by the element itself. In other words, the sentence 'the CA is responsible for executing the audit' is equivalent to 'the entity or personnel managing the CA is responsible for executing ...'.
- (183) The term 'C-ITS trust model elements' includes the root CA, the TLM, the EA/AA, the CPOC and the secure network.

5.1 Physical controls

- (184) All C-ITS trust model operations shall be conducted in a physically protected environment that deters, prevents and detects unauthorised use of, access to or disclosure of sensitive information and systems. C-ITS trust model elements shall use physical security controls in compliance with ISO 27001 [6] and ISO 27005 [9].
- (185) The entities managing the C-ITS trust model elements shall describe the physical, procedural and personnel security controls in their CPS. In particular, the CPS shall cover information about the site location and construction of the buildings and their physical security controls guaranteeing controlled access to all rooms used in the facility of the C-ITS trust model entities.

5.1.1 Site location and construction

5.1.1.1 Root CA, CPOC, TLM

- (186) The location and construction of the facility housing the root CA, CPOC and TLM equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house high-value and sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components' physical areas.
- (187) The root CA, CPOC and TLM shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the root CA equipment is installed, so as to guarantee that:
- Management is performed exclusively from networks inside the C-ITS trust model;
 - it is separated into a series of (at least two) progressively more secure physical perimeters;
 - sensitive data (HSM, key pair backup, activation data, etc.) are stored in a dedicated safe located in a dedicated physical area under multiple access control.
- (188) The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

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

(189) The root CA, CPOC and TLM shall use authorised personnel to continuously monitor the facility housing equipment on a 24/7/365 basis. The operational environment (e.g. systems) shall never be left unattended while in use and shall be securely stored otherwise. Access to the operational environment shall be granted only if authorized. Access to the operational environment shall be authorized exclusively to designated individuals. Access to the operational environment shall be authorized exclusively in connection to a specific set of procedures.

5.1.1.2 EA/AA

(190) The same provisions of section 5.1.1.1 apply, except for the monitoring of the EA/AA which are operating continuously and may be controlled by system tools rather than physical personnel.

5.1.2 Physical access

5.1.2.1 Root CA, CPOC, TLM

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

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

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

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

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

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

5.1.2.2 EA/AA

(195) The same provisions of section 5.1.2.1 apply.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

- (198) To prevent damaging exposure to flame or smoke, the secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be constructed and equipped accordingly and procedures shall be implemented to address fire-related threats. Media storage should be protected against fire in appropriate containers.
- (199) C-ITS trust model elements shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorised use of, access to or disclosure of such media. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.6 Media management

- (200) Media used in the C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be securely handled to protect them from damage, theft and unauthorised access. Media management procedures are implemented to protect against obsolescence and deterioration of media in the period for which records have to be retained.
- (201) Sensitive data shall be protected against being accessed as a result of re-used storage objects (e.g. deleted files), which may make the sensitive data accessible to unauthorised users.
- (202) An inventory of all information assets shall be maintained and requirements set out for the protection of those assets that are consistent with the risk analysis. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

5.1.8.1 *Root CA, CPOC and TLM*

- (204) Full back-ups of these components, sufficient to recover from system failure, shall be made offline after deployment and after each new key-pair generation. Back-up copies of essential business information (key pair and CRL) and software shall be made regularly. Adequate back-up facilities shall be 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 shall be regularly tested to ensure that they meet the requirements of the business continuity plan. At least one full backup copy shall be stored at an offsite location (disaster recovery). The

back-up copy shall be stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

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

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

5.1.8.2 EA/AA

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

5.2 Procedural controls

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

5.2.1 Trusted roles

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

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

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

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

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

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

5.2.2 Number of persons required per task

- (212) C-ITS trust model elements shall establish, maintain and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that multiple trusted persons are required to perform sensitive tasks. The C-ITS trust model elements (TLM, CPOC, root CA, EA and AA) should comply with [4] and with the requirements in the following paragraphs.
- (213) Policy and control procedures shall be in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and the management of CA cryptographic hardware (HSM) and its associated key material, shall require the authorisation of multiple trusted persons.
- (214) These internal control procedures shall be designed to ensure that at least two trusted persons are required to have physical or logical access to the device. Restrictions on access to CA cryptographic hardware shall be strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3 Identification and authentication for each role

- (215) All persons assigned a role, as described in this CP, shall be identified and authenticated so as to guarantee that the role enables them to perform their PKI duties.
- (216) C-ITS trust model elements shall verify and confirm the identity and authorisation of all personnel seeking to become trusted persons before they are:
- issued with their access devices and granted access to the required facilities;
 - given electronic credentials to access and perform specific functions on CA systems.
- (217) The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4 Roles requiring separation of duties

- (218) Roles requiring separation of duties include (but are not limited to):
- the acceptance, rejection and revocation of requests, and other processing of CA certificate applications;
 - the generation, issuing and destruction of a CA certificate.
- (219) Segregation of duties may be enforced using PKI equipment, procedures or both. No individual shall be assigned more than one identity unless approved by the root CA.
- (220) The parts of the root CA and EA/AA concerned with certificate generation and revocation shall be managed independent of other organisations for its decisions relating to the establishing, provisioning, maintaining and suspending of services in line with the applicable certificate policies. In particular, each PKI service provider shall

have its own senior executives, senior staff and staff assigned to trusted roles ensuring segregation of duties.

(221) In accordance with the GDPR [13] and [1], data protection and privacy of C-ITS users shall be ensured. The data protection impact assessment carried out by the C-ITS station operator shall determine whether the C-ITS station belongs to the category “Itss_WithPrivacy” [2]. Therefore, for “Itss_WithPrivacy” [2] the following applies:

- The EA and AA shall be separated logically and shall have separate all trusted roles and ensure complete data segregation.
- The EA and AA shall support the automated exchange of personal data only using protocols that protect personal data of the AT requester. Examples of such protocols are the authorisation validation protocol or the authorization management with butterfly keys of [1] when used over a dedicated secure interface. AAs and EAs shall support the use of the protocols defined in [1] and additionally may support the use of other protocols.
- The EA and AA shall avoid C-ITS stations' re-identification, i.e. the tracing back of the canonical identifier of the C-ITS station bound to the EC that issued a specific AT, except to investigate security incidents or if required for legal reasons (only based on a written court order or similar, as received by the AA and forwarded by the AA to the responsible EA).
- Re-identification shall always require the involvement of at least one authorized trusted role from EA and AA, none of these roles having access to both EA and AA data at the same time.

(222) The logfiles stored by the EA and AA may be used for the purpose of revoking ECs of a C-ITS station if it is determined that the C-ITS station's continued operation poses unacceptable risk to the system (for example, if its ATs are used to sign malicious C-ITS messages). Once an C-ITS station that owns a specific AT or ATs has been identified as necessary to revoke, the AA will look up the AT 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. The exact conditions leading to revocation are out of scope of the CP and may be set operationally by the appropriate authority.

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

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

(223) C-ITS trust model elements shall employ a sufficient number of personnel with the expert knowledge, experience and qualifications necessary for the job functions and services offered. PKI personnel fulfil those requirements through formal training and credentials, actual experience or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly

identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and privileges, and position sensitivity is determined on the basis of duties and access levels, background screening, and employee training and awareness.

5.3.2 Background check procedures

- (224) C-ITS trust model elements shall conduct background checks on personnel seeking to become trusted persons. Background checks shall be repeated for personnel holding trusted positions at least every five years.
- (225) The factors revealed in a background check that may be considered reasons for rejecting candidates for trusted positions or for taking action against an existing trusted person include (but are not limited to) the following:
- misrepresentations made by the candidate or trusted person;
 - highly unfavourable or unreliable professional references;
 - certain criminal convictions;
 - indications of a lack of financial responsibility.
- (226) Reports containing such information shall be evaluated by human resources personnel, who shall take reasonable action in the light of the type, magnitude and frequency of the behaviour uncovered by the background check. Such action may include measures up to and including cancelling offers of employment made to candidates for trusted positions or terminating the employment of existing trusted persons. The use of information revealed in a background check as a basis for such action shall be subject to applicable law.
- (227) Background investigation of persons seeking to become a trusted person shall include but is not limited to:
- confirmation of previous employment;
 - a check of professional references covering their employment over a period of at least five years;
 - a confirmation of the highest or most relevant educational degree obtained;
 - a search of criminal records.

5.3.3 Training requirements

- (228) C-ITS trust model elements shall provide their personnel with the requisite training to fulfil their responsibilities relating to CA operations competently and satisfactorily.
- (229) Training programmes shall be reviewed periodically and their training shall address matters that are relevant to functions performed by their personnel.
- (230) Training programmes shall address matters that are relevant to the particular environment of the trainee, including:

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

5.3.4 Retraining frequency and requirements

- (231) The persons assigned to trusted roles shall refresh the knowledge they have gained from training on an ongoing basis using a training environment. Training shall be repeated whenever deemed necessary and at least every two years.
- (232) C-ITS trust model elements shall provide their staff with refresher training and updates to the extent and with the frequency required to ensure that they maintain the required level of proficiency to fulfil their job responsibilities competently and satisfactorily.
- (233) Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan and the execution of that plan shall be documented.

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorised actions

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

5.3.7 Independent contractor requirements

- (236) C-ITS trust model elements may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and on condition that the entity trusts the contractors or consultants to the same extent as if they were employees and that they fulfil the requirements applicable to employees.
- (237) Otherwise, independent contractors and consultants shall have access to C-ITS PKI secure facilities only if escorted and directly supervised by trusted persons.

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

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

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

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

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

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

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

(242) In accordance with the GDPR [13], the audit logs shall not permit access to privacy-related data concerning C-ITS station private vehicles.

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

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

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

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

5.4.2 Frequency of processing log

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

(247) Audit-log processing shall consist of a review of the audit logs and documenting the reason for all significant events (as defined in the respective CPS) 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 on the basis of audit-log reviews shall be documented.

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

- (250) The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Internal audit logs shall be accessed only by personnel holding trusted roles with the proper authorization; certificate life-cycle related audit logs may also be accessed by users with the appropriate authorisation via a web page with user login. Access shall only be granted with multi-factor authentication. It shall be technically ensured that users cannot access their own log files.
- (251) EC and AT certificate issuance audit logs shall be signed using key material in the HSM.
- (252) EC and AT certificate issuance audit logs shall be encrypted in such a way that only authorised persons can read them.
- (253) Events shall be logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the period for which the logs have to be held.
- (254) Event logs shall be protected in such a way as to remain readable for the duration of their storage period.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal or external)

- (256) The equipment of the C-ITS trust model elements shall activate the audit processes at system start up and deactivate them only at system shutdown. If audit processes are not available, the C-ITS trust model element shall suspend its operation.
- (257) At the end of each operating period and at the re-keying of certificates, the collective status of equipment should be reported to the operations manager and operation governing body (or equivalent roles defined in the CPS) of the respective PKI element.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessment

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

(260) C-ITS trust model elements shall:

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

5.5 Record archiving

5.5.1 Types of record archived

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

- physical facility access log of C-ITS trust model elements (minimum one year);
- trusted roles management log for C-ITS trust model elements (minimum 10 years);

- IT access log for C-ITS trust model elements (minimum five years);
- CA key creation, use and destruction log (minimum five years) (not for TLM and CPOC);
- EC certificate issuance log (minimum five year);
- AT certificate issuance log (minimum three months);
- CPA request log (minimum two years);
- activation data management log for C-ITS trust model elements (minimum five years);
- IT and network log for C-ITS trust model elements (minimum five years);
- PKI documentation for C-ITS trust model elements (minimum five years);
- security incident and audit report for C-ITS trust model elements (minimum 10 years);
- Root CA and sub-CAs system configuration (minimum five years).

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

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

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

- (265) C-ITS trust model elements shall store the archive of records in a safe, secure storage facility separate from the CA equipment, with physical and procedural security controls equivalent to or better than those of the PKI.
- (266) The archive shall be protected against unauthorised viewing, modification, deletion or other tampering by storage in a trustworthy system.
- (267) The media holding the archive data and the applications required to process them shall be maintained to ensure that they can be accessed for the period set in this CP.

5.5.4 System archive and storage

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

- (270) The archive collection system is internal.

5.5.7 Procedures to obtain and verify archive information

- (271) All C-ITS trust model elements shall allow only authorised trusted persons to access the archive. Root CAs and CAs shall describe the procedures for creating, verifying, packaging, transmitting and storing archive information in the CPS.
- (272) Root CA and CA equipment shall verify the integrity of the information before it is restored.

5.6 Key changeover for C-ITS trust model elements

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

5.6.1 TLM

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

implementation process shall be defined by the TLM and CPOC in agreement with the CPA in the CPOC protocol ([10]).

5.6.2 Root CA

(275) The root CA shall not issue EA/AA certificates with a validity that extends beyond the validity of the root CA certificate. The root CA private key shall be used for issuing CRL until the root CA certificate expires. The root CA shall delete its private key (including backup keys) on expiry of the corresponding certificate.

(276) The root CA shall generate a new key pair and corresponding root CA certificate (and optionally a link certificate) before deletion of the current private key (including backup keys) and send the root CA certificate to the TLM for insertion into the ECTL. The validity period of the new root CA certificate shall start at the planned deactivation of the current private key. The root CA shall take care that the new certificate is inserted in the ECTL in time to be distributed to all C-ITS stations before it becomes valid. Details on the process and use of the concept of RCA link certificates are further defined in the CPOC protocol ([10]).

(277) Void.

5.6.3 EA/AA certificate

(278) The EA/AA shall not issue ECs/ATs with a validity that extends beyond the validity of the EA/AA certificate. The EA/AA shall delete their private keys (including backup keys) on expiry of the corresponding certificate.

(279) The EA/AA shall generate a new key pair and request a corresponding EA/AA certificate before deletion and expiry of the current private key. The validity period of the new EA/AA certificate shall start latest at the planned deletion of the current private key. The EA/AA shall take care that the new certificate can be published in time to be distributed to all C-ITS stations before it becomes valid. If the renewal does not take place before the expiry of the current private key and EA/AA certificate, the request shall be treated as a new sub-CA enrolment.

(280) Void.

5.6.4 Auditor

No provisions.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling

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

(282) If the personnel responsible for the management of the root CA or TLM detect a potential hacking attempt or other form of compromise, they shall investigate in order

to determine the nature and the degree of damage. In the event of the private key being compromised, the root CA certificate shall be revoked. The IT security experts of the CPA shall assess the scope of potential damage in order to determine whether the PKI needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI has been compromised. In addition, the CPA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the CPA business continuity plan.

- (283) Incident, compromise and business continuity are covered in the CPS, which may also rely on other enterprise resources and plans for its implementation.
- (284) If the personnel responsible for the management of the EA/AA/CPOC detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and degree of damage. The personnel responsible for the management of the CA or the CPOC entity shall assess the scope of potential damage in order to determine whether the PKI component needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI component has been compromised. In addition, the sub-CA entity determines which services are to be maintained and how, in accordance with the sub-CA entity business continuity plan. In the event of a PKI component being compromised, the CA entity shall alert its own root CA and the TLM through the CPOC.
- (285) Incident, compromise and business continuity are covered in the CPS of the root CA or the TLM or other relevant documents in the case of the CPOC, which may also rely on other enterprise resources and plans for their implementation.
- (286) The root CA and CA shall alert, with precise information on the consequences of the incident, each Member State representative and root CA with which they have an agreement in the C-ITS context, in order to allow them to activate their own incident management plan.

5.7.2 Corruption of computing resources, software and/or data

- (287) If a disaster is discovered that prevents the proper operation of a C-ITS trust model element, that element shall suspend its operation and investigate whether the private key has been compromised (except CPOC). Defective hardware shall be replaced as quickly as possible and the procedures described in sections 5.7.3 and 5.7.4 shall apply.
- (288) The corruption of computing resources, software and/or data shall be reported to the root CA within 24 hours for the highest levels of risk. All other events shall be included in the periodic report of the root CA, EAs and AAs.

5.7.3 Entity private key compromise procedures

- (289) If the private key (or any of its backups) of a root CA is compromised or suspected of being compromised, the root CA shall:
- suspend its operation;
 - start the disaster recovery and migration plan;

- revoke its root CA certificate;
 - investigate the 'key issue' that generated the compromise and notify the CPA, which will remove the compromised root CA certificate from the ECTL through the TLM (see section 7);
 - alert all subscribers with which it has an agreement.
- (290) If an EA/AA's private key (or any of its backups) is compromised or suspected of being compromised, the EA/AA shall:
- suspend its operation;
 - request the root CA to revoke the compromised certificate;
 - investigate the 'key issue';
 - notify the root CA;
 - alert all their subscribers.
- (291) If a C-ITS station's EC private key (or any of its backups) is compromised or suspected of being compromised, the EA to which the C-ITS station is subscribed shall:
- blocklist the EC of the affected C-ITS stations;
 - investigate the 'key issue';
 - notify the root CA;
 - alert the corresponding subscribers.
- (292) Where any of the algorithms or associated parameters used by the root CA and/or CA or C-ITS stations becomes insufficient for its remaining intended usage, the CPA (with a recommendation from cryptographic experts) shall inform the root CA entity with which it has an agreement and change the algorithms used. (For details, see section 6 and the CPSs of the root CA and sub-CA).

5.7.4 Business continuity capabilities after a disaster

- (293) The C-ITS trust model elements operating secure facilities for CA operations shall develop, test, maintain and implement a disaster recovery plan designed to mitigate the effects of any natural or man-made disaster. Such plans address the restoration of information systems services and key business functions.
- (294) After an incident of a certain risk level, the compromised CA shall be re-audited by an accredited PKI auditor (see section 8).
- (295) Where the compromised CA is unable to operate any longer (e.g. following a severe incident), a migration plan shall be drawn up for the transfer of its functions to another root CA. At least the EU root CA shall be available to support the migration plan. The compromised CA shall cease its functions.
- (296) The root CAs shall include the disaster recovery plan and the migration plan in the CPS.

5.8 Termination and transfer

5.8.1 TLM

(297) The TLM shall not terminate its operation, but the role of TLM may be taken over by another entity.

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

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

5.8.2 Root CA

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

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

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

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

5.8.3 EA/AA

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

- inform the root CA by registered letter;
- destroy their private keys and all existing backups of the private keys;;

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

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

6 Technical security controls

6.1 Key-pair generation and installation

6.1.1 TLM, root CA, EA, AA

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

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

6.1.2 End-entity — C-ITS station

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

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

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

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

6.1.3 Void

(309) Void.

(310) Void.

(311) Void.

6.1.4 Cryptographic requirements

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

6.1.4.1 Algorithm and key length - signature algorithms

(313) All PKI participants (TLM, root CA, EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key for signing operations with selected algorithms in accordance with Table 5.

Table 5: Generating key pairs and use of private key for signing operations

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

(314) All PKI participants that need to check the integrity of the ECTL, certificates and/or signed messages in accordance with their role, as defined in section 1.3.6, shall support the corresponding algorithms listed in Table 6 for verification. In particular, C-ITS stations shall be able to check the integrity of the ECTL.

Table 6: Verification overview

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

(315) The CPA may decide on the basis of newly found cryptographic weaknesses that a certain algorithm is to be deprecated. Thereafter, all PKI participants shall stop using the deprecated algorithm as soon as possible. The actual algorithm(s) that is/are to be used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

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

(316) All PKI participants (EA, AA and C-ITS stations) shall be able to use public keys to encrypt enrolment and authorisation requests/responses with selected algorithms in accordance with Table 7. The actual algorithm(s) that is/are used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

(317) The named algorithms in Table 7 indicate the key length and hash algorithm length and shall be implemented in accordance with [5].

Table 7: Use of public keys for encryption of enrolment and authorisation requests/responses

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

(318) All PKI participants (EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key to decrypt enrolment and authorisation requests/responses with selected algorithms in accordance with Table 8:

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

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

6.1.4.3 Crypto-agility

(319) Requirements on key lengths and algorithms need to be changed over time to maintain an appropriate level of security. The CPA shall monitor the need for such

changes in the light of actual vulnerabilities and state-of-the-art cryptography. It will draft, approve and publish an update of this certificate policy if it decides that the cryptographic algorithms should be updated. Where a new issue of this CP signals a change of algorithm and/or key length, the CPA will adopt a migration strategy, which includes transition periods during which old algorithms and key lengths shall be supported.

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

(321) Changes of root and TLM certificates shall be supported and executed with the help of link certificates (details see [10]) that are used to cover the transition period between the old and new root certificates ('migration of the trust model').

6.1.5 Secure storing of private keys

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

6.1.5.1 Root CA, sub-CA and TLM level

(322) A cryptographic module shall be used for:

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

The cryptographic module shall be certified, configured and operated according to one of the CPA approved protection profiles (PPs), with assurance level EAL-4 or higher. The list of CPA approved cryptographic module protection profiles will be maintained in an annex published on the same website as this policy.

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

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

6.1.5.2 End-entity

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

- generating, using, administering and storing private keys;

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

The cryptographic module for the End-Entities shall be certified against one of the CPA approved protection profiles (PPs), with at least an assurance level EAL4 augmented with AVA_VAN.4. The list of CPA approved cryptographic module protection profiles will be maintained in an annex published on the same website as this policy.

At the time of type approval of a vehicle model with a C-ITS station installed, the secure element of the C-ITS station shall have a valid CC certification or re-assessment (according to the approved PPs listed above) that is not older than three years.

For infrastructure devices like RSUs or OBUs, at the time of the delivery release or sales release of the hardware of a model, the secure element of the C-ITS station shall have a valid CC certification or re-assessment that is not older than three years.

The security of the cryptographic module shall be continuously monitored and maintained as described in the ISMS/CSMS required by the Security Policy. In addition to that, the station operator shall ensure that all vulnerabilities discovered will be addressed (e. g. recorded, mitigated or fixed). If the cryptographic module of the C-ITS station implements a secure soft-/firmware update mechanism (optional package in the protection profile), it shall be part of the common criteria certification, and this mechanism shall be used as preferred option to fix vulnerabilities. If there is a serious vulnerability that cannot be fixed, the affected C-ITS stations shall be excluded from the PKI.

- (324) The cryptographic module shall be protected against unauthorised removal, replacement and modification. All PPs and related documents applicable for the security certification of the cryptographic module shall be evaluated, validated and certified in accordance with ISO 15408, applying the Mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS), or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity legislation.
- (325) Given the importance of maintaining the highest possible security level, security certificates for the cryptographic module shall be issued under the common criteria certification scheme (ISO 15408) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS Agreement, or issued by a conformity assessment body accredited by a national or European cybersecurity certification authority. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

6.1.6 Backup of private keys

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

private keys shall only be done in encrypted and signed/MAC protected way by using the backup mechanism of the secure elements listed above.

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

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

6.1.7 Destruction of private keys

(329) The TLM, root CAs, EAs, AAs, and C-ITS station operators shall destroy their private key and any corresponding backups, if a new key pair and corresponding certificate has been generated and successfully installed, and the overlap time (if any — CA only) has passed. The private key shall be destroyed using the mechanism offered by the cryptographic module used for the key storage or as described in the corresponding PP as referred to in section 6.1.5.1 and 6.1.5.2 and in the list of CPA approved cryptographic module protection profiles.

6.2 Activation data

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

6.3 Computer security controls

(331) The CAs' computer security controls shall be designed in accordance with the high security level by adhering to the requirements of ISO/IEC 27002 [7].

6.4 Life-cycle technical controls

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

6.5 Network security controls

(333) The networks of the CAs (root CA, EA and AA) shall be hardened against attacks in line with the requirements and implementation guidance of ISO/IEC 27001 [6] and ISO/IEC 27002 [7].

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

7 Certificate profiles, CRL, CTL and ECTL

7.1 Certificate profile

- (335) The certificate profiles defined in [5] shall be used for the TLM, root certificates, EA certificates, AA certificates, ATs and ECs. National governmental EAs may use other certificate profiles for ECs.
- (336) Root CA, EA and AA certificates shall indicate the permissions for which these CAs (root CAs, EA and AA) are allowed to issue certificates.
- (337) On the basis of [5]:
- each root CA shall use its own signing private key to issue the root CA self signed certificate and the root CA Link certificate, CRLs, EA/AA certificates and CTLs;
 - the TLM shall use its own signing private key to issue the ECTL, the TLM self-signed certificate and the TLM Link Certificate.

7.2 Certificate validity

7.2.1 General

- (338) All C-ITS certificate profiles shall include the validity period of the certificate.
- (339) The validity period of any new TLM and CA certificates shall overlap with the validity period of the respective previous certificate. The new TLM and root CA certificates shall be issued and put on the ECTL a maximum of three months and at least one month before the end of the private key usage period of the current valid certificate. This is required to safely distribute the certificates to all correspondent relying parties in accordance with section 2.2. This ensures that, from the beginning of the overlap, all relying parties are already able to verify messages issued with a new certificate.
- (340) During the overlap time of root CA certificates, the private key associated to the current certificate shall be used only for CTL/CRL signing (in contrast to what is defined in (337)) and the private key associated to the successive certificate shall be used as defined in (337).
- (341) Void.
- (342) The validity of (Root and TLM) link certificates starts at the corresponding private key usage and ends at the maximum validity time of the root CA or TLM. The details on the use of Link Certificates shall be defined by the CPOC in agreement with the CPA in the CPOC protocol [10].
- (343) Table 9 shows the maximum validity time for C-ITS TLM and root CA certificates (for AT validity periods, see section 7.2.2).

Table 9: Validity periods of the root CA and TLM certificates in the C-ITS trust model

Entity	Max. private key usage period	Maximum validity time
root CA	equal to validity time	5 years
TLM	3 years	4 years

(344) The following definitions shall apply:

- ‘validity period for ATs’ – the period for which an AT is valid, i.e. the period between the AT’s starting date and its expiry date;
- ‘preloading period for ATs’ – preloading is the possibility for C-ITS stations to obtain ATs before the validity period starts. The preloading period is the maximum allowed time period from the request of ATs to the latest end of validity date of any requested AT;
- ‘usage period for ATs’ – the period during which an AT is effectively used to sign C-ITS messages (e.g. CAM/DENM) in accordance with the ITS-AID and SSPs in the AT;
- ‘maximum number of parallel ATs’ – the number of ATs containing a specific pair of (ITS-AID, SSP) from which a C-ITS station can choose at a given time when signing a C-ITS message(e.g. CAM/DENM).

Note: In case of an IVI *serviceProviderId* delegation [12] agreement in place, the number of parallel ATs is counted for each individual *serviceProviderId* that the C-ITS station is delegated for.

7.2.2 AT for C-ITS-Stations of type Itss_WithPrivacy [2]

(345) Void.

(346) Void.

(347) The following requirements shall apply:

- the preloading period for ATs shall not exceed three months;
- the validity period for ATs shall not exceed one week;
- the maximum number of parallel ATs shall not exceed 200 per C-ITS station. The EA shall notify the C-ITS station operator in case more than 100 parallel ATs have been requested by a single C-ITS station. In addition, the EA shall reset the maximum number of parallel ATs per C-ITS station after receiving an authenticated request from the C-ITS station operator. All deviations exceeding 100 parallel ATs per C-ITS station shall be monitored by the C-ITS station operator to ensure that this limit is only exceeded in exceptional and justified cases (e.g. C-ITS station fault, repair);

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

7.2.3 AT for C-ITS stations of type Itss_NoPrivacy [2]

(348) For C-ITS stations of type Itss_NoPrivacy [2], the following requirements apply:

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

7.3 Revocation of certificates

7.3.1 Revocation of Root CA, EA and AA certificates

(348b) Root CA, EA and AA certificates shall be revocable at any time when the certificate is not expired. Revoked certificates of root CAs, EAs and AAs shall be published on a CRL issued by the root CA as soon as possible and without undue delay. This CRL shall be signed by its corresponding root CA and use the profile described in section 7.4:

- For revocation of root CA certificates, the corresponding root CA shall issue a CRL containing its own certificate. In addition, but asynchronously and as a best effort service, the TLM shall remove revoked root CAs from the ECTL and issue a new ECTL.
- For revocation of EA/AA certificates, the root CA shall issue a CRL containing the corresponding EA/AA certificate. In addition, but asynchronously and as a best effort service, the root CA shall also remove the corresponding certificate from the CTL and issue a new CTL.

(348c) Expired certificates shall be removed from the corresponding CRL and trust list.

(349) Certificates are revoked when:

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

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

7.3.2 Blocklisting of enrolment credentials

(351) Blocklisting of ECs may be initiated by the C-ITS station subscriber (flow 34). The EA shall maintain information about which ECs are currently blocklisted. The blocklist shall be kept confidential and used only by the corresponding EA to verify the validity of the corresponding ECs in the context of requests for ATs and new ECs.

7.3.3 Revocation of authorisation tickets

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

7.4 Certificate revocation list

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

7.5 Certificate trust list

(353b) The format and content of the CTL issued by the RCA shall be as laid down in [1].

7.6 European certificate trust list

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

8 Compliance audit and other assessments

8.1 Topics covered by audit and audit basis

- (355) The TLM, root CAs, EAs and AAs shall select an independent acting and accredited PKI auditor to audit. Their operations and CPS shall be audited against this CP and ISO/IEC 27001 [6].
- (356) A compliance audit is ordered by a root CA (flow 13) for the root CA itself, and for a sub-CA by its subordinate EA/AA.
- (357) A compliance audit for the TLM is ordered by the CPA (flow 38).
- (358) When requested, an accredited PKI auditor shall perform a compliance audit on one or more of the following levels:
- (1) conformity of the TLM's, root CA's, EA's or AA's CPS with this CP;
 - (2) conformity of the TLM's, root CA's, EA's or AA's intended practices with its CPS prior to operation;
 - (3) conformity of the TLM's, root CA's, EA's or AA's practices and operational activities with its CPS during operation.
- (359) The audit shall cover all requirements of this CP to be fulfilled by the TLM, root CAs, EAs and AAs to be audited. It shall also cover the operation of the CA in the C-ITS PKI, including all processes mentioned in its CPS, the premises and responsible persons.
- (360) The accredited PKI auditor shall provide a detailed report of the audit to the root CA, EA, AA or TLM (flow 36), as applicable.

8.2 Frequency of the audits

- (361) A root CA, TLM, EA or AA shall order a compliance audit of itself from an independent and accredited PKI auditor in the following cases:
- at its first setting-up (levels 1 and 2 compliance) based on the CP valid at the start of the audit process;
 - regularly, and at least every three years during its operation (level 3 compliance);
 - at every major change of the CP if requested by the CPA. The CPA shall assess the criticality of the change and define the time-plan of deployment and determine the needs and schedule for audits (including the necessary compliance level) accordingly;
 - at every change of its CPS (levels 1, 2 and 3 compliance). Since the managing entities of root CAs, the TLM and EAs/AAs decide what implementation changes follow the update of their CPS, they shall order a compliance audit before implementing those changes. In cases of only minor changes of the CPS (e.g. of an editorial nature), the managing entity may send the CPA a duly justified request for its approval to skip level 1, 2 or 3 compliance audits.

8.3 Identity/qualifications of auditor

(362) The CA to be audited shall select an independently acting and accredited company/organisation ('auditing body') or accredited PKI auditors to audit it in accordance with this CP. The auditing body shall be accredited and certified by a member of European Accreditation¹.

8.4 Auditor's relationship to audited entity

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

8.5 Action taken as a result of deficiency

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

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

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

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

8.6 Communication of results

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

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

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

9 Other provisions

9.1 Fees

- (370) One principle of the implemented EU C-ITS trust model is that the root CAs together fully finance the regular recurrent costs of operation of the CPA and the central elements (TLM and CPOC) relating to the activities set out in this CP.
- (371) The root CAs (including the EU root CA) are entitled to take fees from their sub-CAs.
- (372) Throughout their period of operation, every participant of the C-ITS trust model shall have access to at least one root CA, EA and AA on a non-discriminatory basis.
- (373) Each root CA is entitled to pass on the fees it pays for CPA and the central elements (TLM and CPOC) to the registered participants of the C-ITS trust model, including the enrolled and authorised C-ITS stations.

9.2 Financial responsibility

- (374) The initial establishment of a root CA shall cover a period of at least three years of operation, in order for it to become a member of the EU C-ITS trust model. The CPS of a root CA operator shall also contain detailed provisions on root CA revocation or closure.
- (375) Each root CA shall demonstrate the financial viability of the legal entity implementing it for at least three years. This financial viability plan is part of the initial set of documents for enrolment and shall be updated every three years and reported to the CPA.
- (376) Each root CA shall report the structure of charges applied to EAs/AAs and the enrolled and authorised C-ITS stations each year to the operations manager and the CPA to demonstrate its financial sustainability.
- (377) All financial and legal responsible entities of the root CA, EA, AA and the central elements (CPOC and TLM) of the C-ITS trust model shall cover their operational duties with adequate insurance levels to compensate for operational errors and financial recovery of their duties if one of the technical elements fails.

9.3 Confidentiality of business information

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

9.4 Privacy plan

(379) The CPSs of the root CAs and the EAs/AAs shall set out the plan and the requirements for the treatment of personal information and privacy on the basis of the GDPR [13] and other applicable legislative (e.g. national) frameworks.

10 Conclusions

The contents of Release 3.0 of the Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) were approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in April 2024.

The aim of this document is to lay down, together with the Security Policy, the rules of the European Union C-ITS Security Credential Management System (EU CCMS), the common trust model for the exchange of C-ITS messages. The information contained in this document is expected to have a positive impact on the whole C-ITS ecosystem, providing clear rules and guidelines especially to C-ITS stations manufactures and operators, for their certification and deployment, meeting the IT security and privacy highest requirements.

Until a dedicated entity is appointed as C-ITS Certificate Policy Authority (CPA), the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) will continue to manage future updates of this policy.

The latest version of this document is published online in the documentation section of the C-ITS Point of Contact website: <https://cpoc.jrc.ec.europa.eu/Documentation.html>

References

The following references are used in this Certificate Policy.

- [1] ETSI TS 102 941 V1.4.1 or V2.2.1: "Intelligent transport systems (ITS) – security, trust and privacy management".
- [2] ETSI TS 102 940 V1.3.1 or V2.1.1: "Intelligent transport systems (ITS) – security, ITS communications security architecture and security management".
- [3] Certificate policy and certification practices framework (RFC 3647, 1999).
- [4] ETSI TS 102 042 V2.4.1: "Policy requirements for certification authorities issuing public key certificates".
- [5] ETSI TS 103 097 V1.4.1 or V2.1.1: "Intelligent transport systems (ITS) – security, security header and certificate formats".
- [6] ISO/IEC 27001:2022: "Information security, cybersecurity and privacy protection – Information security management systems – Requirements".
- [7] ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security controls".
- [8] ISO/IEC 27005:2022 "Information security, cybersecurity and privacy protection – Guidance on managing information security risks".
- [9] Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 3.0
- [10] C-ITS Point of Contact (CPOC) in its current release available at <https://cpoc.jrc.ec.europa.eu/Documentation.html>
- [11] Car 2 Car Communication Consortium, "Basic System Profile - v1.6 or newer," [Online]. Available at: <https://www.car-2-car.org/documents/basic-system-profile/>.
- [12] C-ROADS Harmonised C-ITS specifications for Europe - Release 2.0 or newer.
- [13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1, 2016.

List of abbreviations and definitions

The acronyms and definitions in [2], [3], [4] and [9] apply.

Acronyms

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

Definitions

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

Definitions

root certification authority	In this document, the term 'root certification authority' (CA) refers not only to the specific function of the CA, but also to the legal and/or operational entity managing it.
subject	The natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber.
subscriber	A natural person or legal entity to which a certificate is issued and which is legally bound by a subscriber or terms of use agreement.
subscriber agreement	An agreement between the CA and the applicant/subscriber that specifies the rights and responsibilities of the parties.

List of figures

Figure 1: C-ITS trust model architecture	15
Figure 2: C-ITS Trust model information flows including butterfly key mechanism.....	15

List of tables

Table 1: Releases.....	13
Table 2: Detailed description of information flows in the C-ITS trust model.....	16
Table 3: Operational roles.....	20
Table 4: Re-keying process for EAs and AAs.....	46
Table 5: Generating key pairs and use of private key for signing operations.....	71
Table 6: Verification overview.....	71
Table 7: Use of public keys for encryption of enrolment and authorisation requests/responses.....	72
Table 8: Generate key pairs and use of private key for the decryption of enrolment and authorisation requests/responses	72
Table 9: Validity periods of the root CA and TLM certificates in the C-ITS trust model.....	77

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society



EU Science Hub
[Joint-research-centre.ec.europa.eu](https://joint-research-centre.ec.europa.eu)