



C-ITS Point of Contact (CPOC) Protocol in the EU C-ITS Security Credential Management System (EU CCMS)

Release 3.1 – June 2024

This publication is a Technical Report 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>

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.

All content © European Union 2024

How to cite this report: "*C-ITS Point of Contact (CPOC) Protocol in the EU C-ITS Security Credential Management System (EU CCMS) - Release 3.0.1*" European Commission, Ispra, 2024

Contents

Abstract	1
1 Introduction.....	2
1.1 Scope and objectives	2
1.2 Target audience	3
1.3 Version History	3
2 CPOC Protocol.....	4
2.1 Overview of the EU CCMS	4
3 CPOC Protocol Overview.....	6
3.1 Conventions and Definitions	6
3.2 Add a new RCA certificate or add a new RCA certificate with linkage to previous RCA certificate to the ECTL.....	6
3.2.1 Related High level approval view	6
3.2.2 Assurance Goals	7
3.2.3 Prerequisites	8
3.2.4 Protocol flow.....	10
3.3 RCA Certificate revocation from the ECTL.....	12
3.3.1 Overview on revocation scenarios and high level assurance goals	12
3.3.2 Prerequisites	13
3.3.3 Protocol flow for revocation scenarios 1a, 2, 3 and 4	13
3.3.4 Protocol flow for revocation scenario 1b (critical RCA certificate revocation)	14
4 Conclusions	15
References.....	16
List of abbreviations	17
List of figures	18
List of tables.....	19
Annexes	20
Annex I. Requirements & best practices of TLM certificates, RCA certificates and the ECTL.....	20
I.1. Overview	20
I.1.1. Scope of Annex I	20
I.2. TLM Certificate and attributes.....	20
I.2.1. TLM Certificate Overview	20
I.2.1.1. Example TLM certificate in the EU CCMS	20
I.2.2. Implementation choices for the EU CCMS TLM Certificate.....	21
I.2.2.1. TLM CertificateID	21
I.2.2.2. TLM Region	22
I.3. RCA certificate and attributes	23
I.3.1. RCA Certificate Overview.....	23
I.3.1.1. Example RCA certificate	23

I.3.1.2.	Example RCA Certificate – More detailed explanations.....	25
I.3.2.	RCA certificate name / CertificateID	31
I.3.2.1.	Considerations and requirements on the “CertificateID” within the RCA Certificate and RCA Link Certificates.....	31
I.3.2.2.	The mandatory naming/CertificateID format.....	33
I.3.2.3.	Consequences on re-use of CertificateID in re-keying scenarios.....	34
I.3.2.4.	Note regarding EA and AA naming and URLs.....	35
I.3.3.	Validity period of Certificates in the EU CCMS	36
I.3.4.	Omitted attributes.....	37
I.3.5.	ECC key format for an optimal over-the-air bandwidth.....	37
I.3.6.	Unlimited permission and “least privilege” principle.....	38
I.3.7.	appPermissions with predefined values	38
I.3.8.	certIssuePermissions with predefined values.....	38
I.3.9.	Region.....	40
I.4.	Supported Permissions in RCA and TLM Certificates	41
I.4.1.	Minimum Set of Permissions:.....	41
I.4.2.	Maximum Set of Permissions:	41
I.5.	Publications of the TLM/CPOC	44
I.5.1.	Regular publication schedule of the ECTL by the TLM/CPOC	44
I.5.2.	Machine-readable access of TLM Certificates, TLM Link Certificate Messages, ECTLs and delta ECTLs	46
I.5.2.1.	CPOC HOST URL Definition.....	46
I.5.2.2.	Request of TLM certificate	47
I.5.2.3.	Request of TLM link certificate message	47
I.5.2.4.	Request of full ECTL	47
I.5.2.5.	Request of delta ECTL.....	48
I.5.3.	Delivery of Root CA Distribution Centre URLs via the CPOC	48
I.6.	Link Certificates	49
I.6.1.	Introduction.....	49
I.6.2.	Trust Anchor exchange on TLM Level (TLM Certificate).....	49
I.6.2.1.	TLM Certificate Update Option 1 – Out of band delivery of TLM Certificate & TLM Link Certificate:	50
I.6.2.2.	TLM Certificate Update Option 2 – TLM Certificate & TLM Link Certificate available on the CPOC Website:.....	50
I.6.2.3.	TLM Certificate Update Option 3 – new TLM Certificates available on specific versions of the ECTL:	51
I.6.3.	Trust Anchor exchange on RCA level (RCA Certificate):	51
I.6.3.1.	Example use cases of RCA link certificates.....	51
I.6.3.2.	Example use cases where RCA link certificates are NOT needed	52
I.6.4.	Construction and verification of RCA and TLM Link Certificates:.....	52
I.6.4.1.	Construction of Link Certificates	53

I.6.4.2.	Verification of Link Certificates	53
I.6.4.2.1.	Verification of TLM Link Certificates:	53
I.6.4.2.2.	Verification of Single Signed RCA Link Certificates:.....	55
I.6.4.2.3.	Verification of Double Signed RCA Link Certificate Message:	57
I.6.4.3.	Requirements on SSPs.....	59
I.6.5.	Linkage of Certificates inside the ECTL	60
I.6.5.1.	Linkage of TLM certificates	60
I.6.5.2.	Linkage of RCA certificates.....	60
I.6.5.3.	Example of a RCA re-key scenario and its impact on the ECTL for further illustration.....	61
I.6.5.3.1.	Step 1: Creation of the RCA Link Certificate.....	61
I.6.5.3.2.	Step 2: What happens at the CPOC ENTRY?	61
I.6.5.3.3.	Step 3: What is published in the ECTL by the TLM?	61
I.6.5.3.4.	Step 4: Next re-keys of RCA – what happens to linkages?.....	63
I.7.	CPOC ENTRY checks on RCA Certificates	64
Annex II.	RCA Enrolment Form.....	68
II.1.	Type of enrolment application.....	68
II.2.	Information on the RCA organisation.....	68
II.3.	Information on the RCA authorised representative (AR).....	69
II.3.1.	RCA Authorised Representative 1	69
II.4.	Identity and registration information of RCA trusted couriers	70
II.4.1.	RCA Trusted Courier 1	70
II.5.	Personal data processing.....	71
II.6.	Date and Signature.....	71
II.7.	Attachments to the RCA Enrolment Form.....	71
Annex III.	RCA Enrolment Approval Form.....	72
III.1.	Summary of the received RCA Enrolment Form	72
III.2.	CPA assessment of the received RCA Enrolment Form	72
III.3.	CPA approval of the RCA Enrolment form	72
Annex IV.	RCA Application Form.....	73
IV.1.	Identity of the organisation and registration information.....	73
IV.2.	Type of RCA Application	74
IV.3.	RCA Certificate Information of the applicant self-signed RCA ETSI103097Certificate.....	75
IV.4.	RCA Link Certificate Message Information	78
IV.5.	Optional: eIDAS Information	81
IV.6.	Personal data processing.....	82
IV.7.	Date and Signature.....	82
Annex V.	RCA Application Approval Form.....	83
V.1.	Summary of the received RCA Application Form	83
V.2.	CPA assessment of the received RCA Application Form	83

V.3. CPA approval of the RCA application form	83
Annex VI. RCA Revocation Form	84
VI.1. Identity of the organisation and registration information	84
VI.2. Selection of the applicable RCA Revocation Scenario	85
VI.3. Revocation Scenario 1a, 2, 3 and 4	86
VI.3.1. RCA Certificate Information of the self-signed RCA ETSI103097Certificate that is to be revoked	86
VI.4. Revocation Scenario 1b (critical importance)	86
VI.4.1. RCA Certificate Information of the self-signed RCA ETSI103097Certificate that is to be revoked	86
VI.5. Personal data processing	87
VI.6. Date and Signature	87
VI.6.1. IN ADDITION ONLY IN CASE OF Revocation Scenario 1b (critical importance): eIDAS signature	88
Annex VII. RCA Revocation Approval Form	89
VII.1. Summary of the received RCA Revocation Form	89
VII.2. CPA assessment of the received RCA Revocation Form	89
VII.3. CPA approval of the RCA revocation form	89
Annex VIII. EU CCMS Levels & Requirements	90
VIII.1. Scope	90
VIII.2. Definition of EU CCMS Levels	90
VIII.2.1. Overview of the Levels	90
VIII.2.2. Level 0 (L0)	92
VIII.2.3. Level 1 (L1) (including L1 Legacy)	92
VIII.2.4. Level 2 (L2)	93
VIII.3. Access criteria, needed achievements & other considerations on Levels	93
VIII.3.1. Details of L0 access criteria & achievements needed	94
VIII.3.2. Details of L1 access criteria & achievements needed	94
VIII.3.2.1. Level 1 Evaluation Tasks for the C-ITS Station	97
VIII.3.2.2. Guidelines on Documentation for Level 1 C-ITS PKIs	103
VIII.3.3. Details of L2 access criteria & achievements needed	104

Abstract

This report describes one of the key elements of the European Union C-ITS Security Credential Management System (EU CCMS), which supports the deployment of C-ITS systems and technologies in Europe by implementing the trust model and providing the necessary security functions. The EU CCMS is based on central elements to support secure interoperability at European level. One of these central elements is the C-ITS Point of Contact (CPOC), which collects the Root Certification Authorities (RCAs) certificates and provides them to the Trust List Manager (TLM) to create the European Certificate Trust List (ECTL).

This report describes the CPOC protocol, its main objective is the definition of the interface between the CPOC and the RCAs, including additional mandatory requirements, best practices, guidance and clarifications on deployment-relevant issues of various EU CCMS components like the ECTL, RCA Certificates, TLM Certificates, RCA and TLM Link Certificates, and their interaction with C-ITS stations. Templates for various forms for the interaction of RCAs, the CPOC and Certificate Policy Authority (CPA) are also included in this document. Furthermore, it defines three different Levels of trust in the EU CCMS (Level 0, Level 1 and Level 2) in order to support the deployment of C-ITS systems from an initial setup phase to regular operations of large and distributed C-ITS networks.

This document is the Release 3.0. This update 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.

The publication of the first versions of the C-ITS certificate policy and security policy defined the key elements of the EU CCMS and the main entities including the central elements. As further stipulated in the Commission Communication from 17th of May 2018 "On the road to automated mobility: An EU strategy for mobility of the future" (COM(2018) 283) the Commission decided to implement "a pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages according to the published guidance on the certificate and security policy".

The C-ITS Point of Contact (CPOC) is a key central element for the implementation of the EU CCMS. The CPOC Protocol describes how the CPOC collects the Root Certification Authorities (RCAs) certificates and provides them to the Trust List Manager (TLM) to create the European Certificate Trust List (ECTL).

This document is the Release 3.0 of the CPOC Protocol, approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in December 2023.

1.1 Scope and objectives

The first phase of the deployment of the EU CCMS focused on the development of a working prototype of the EU CCMS at European level. The JRC worked on the design of the so called "central elements" defined in the C-ITS certificate policy.

The CPOC is one of the EU CCMS central elements and its role is to implement the interface with the RCAs and to collect the RCA certificates, transmitting them to the TLM, and finally publishing the ECTLs issued by the TLM.

The scope of this report is to define the protocol between the CPOC, the RCAs and the Certificate Policy Authority (CPA) as well as to clarify other implementation related issues within the EU CCMS and its central elements.

The CPOC protocol is primarily a manual protocol where RCA representatives need to come physically to the CPOC facilities (hosted in European Commission premises, Joint Research Centre, Ispra site, Italy) for the initial enrolment and subsequent requests including the re-key/update of RCA certificates. The only exceptions are the RCA re-key with link certificate message (cryptographic linkage) and the revocation case where an additional remote option is described. In case the current framework conditions under which the Commission is hosting and operating the CPOC change, the protocol may be revised in the future.

The structure of this report is the following:

- Chapter 1 presents the policy context and the overall content of the document.
- Chapter 2 provides an overall view of the EU CCMS architecture.
- Chapter 3 is the main part of the report and it describes the CPOC protocol.
- Chapter 4 provides a brief outlook on the impact of this work and future actions.

In addition, this document has several annexes: Annex I contains the description of the requirements, best practices and their implications on PKI participants regarding RCA and TLM certificates as well as the ECTL within the EU C-ITS Security Credential Management System (EU CCMS). Annex II to Annex VII contain several forms for the processes of the CPA/CPOC. Finally, Annex VIII includes the description of the three Levels of trust in the EU CCMS, including access criteria and needed achievements for each of them.

The CPOC protocol is subject to future change and will hence be updated whenever required and consequently published as a new release.

1.2 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).

1.3 Version History

This report 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 revision took place in early 2020 following the two C-ITS security ETSI plug-tests in 2019, updating several parts of this document and adding Annex I on additional requirements and best practices in the EU CCMS.

In summer 2020, the contents of Release 1.1 were approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941).

In December 2021, the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) approved the "EU CCMS Levels & Requirements" document and its inclusion in the CPOC Protocol Release 1.2 as Annex VIII.

Release 3.0* (December 2023) is an update of release 1.2 (December 2021), to delete technical specifications now included in the relevant ETSI standards, to ensure the consistent reference through the document to versions of ETSI standards, to update obsolete references and to amend the planned end date of the "Level 1 transition" phase to the end of 2025 instead of the end of 2023.

Release 3.1 (June 2024) is an update of Release 3.0 with changes in the "ITS-AID values allowed in the EU CCMS" (Table 4) and the "specification of maximum permissions contained in a RCA certificate in the EU CCMS" (Table 5) as well as other minor corrections.

Table 1. Release Versions

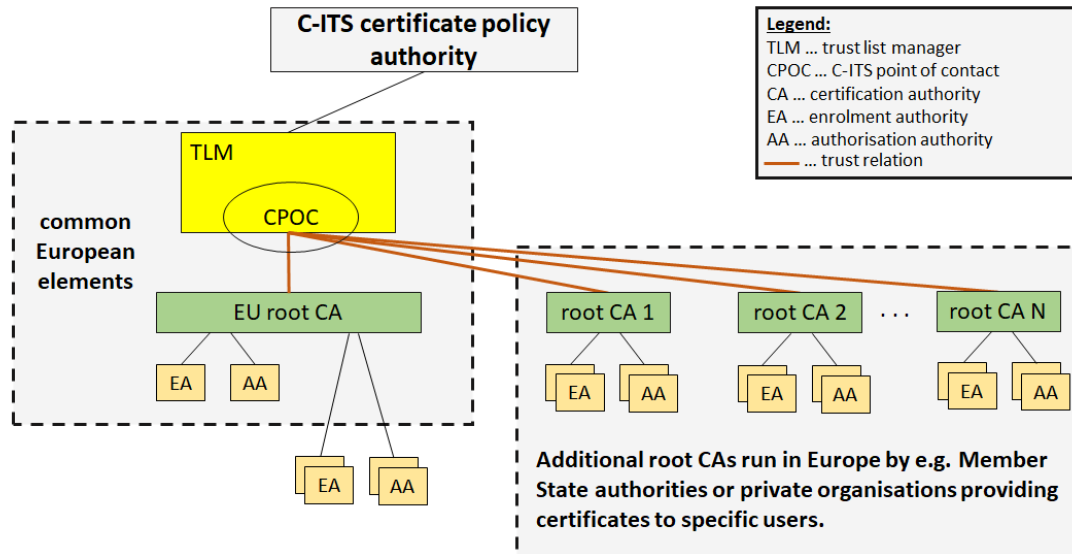
Release Version	Date
Release 1	January 2019
Release 1.1	August 2020
Release 1.2	December 2021
Release 3.0*	December 2023
Release 3.1	June 2024

* Note: The Editing Team of the C-ITS sub-group agreed to jump from release 1.2 to release 3.0 in order to align the versioning of the CPOC Protocol with that of the C-ITS Security Policy and the C-ITS Certificate Policy, these three main EU CCMS / C-ITS policy documents are part of the "Release 3" package.

2 CPOC Protocol

2.1 Overview of the EU CCMS

Figure 1. High level view of the EU CCMS trust model (from [1]).



The high level functional view of the EU CCMS is provided in Figure 1. The main entities and roles are described in [1] and they are briefly reported here:

Trust List Manager

The TLM is a single entity appointed by the CPA.

The TLM is responsible for:

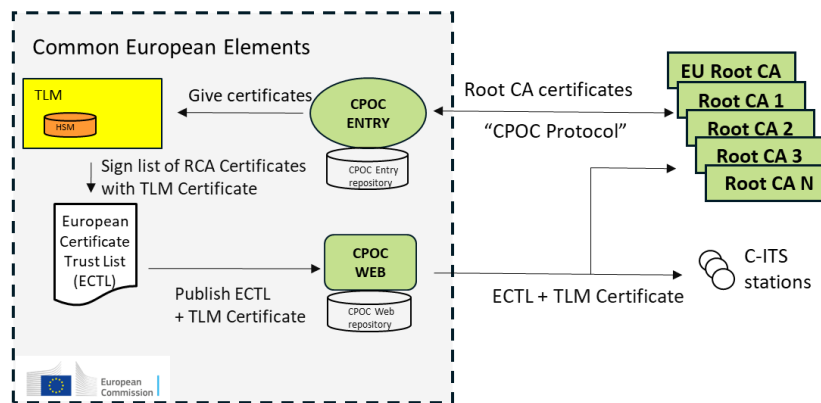
- the operation of the ECTL in accordance with the common valid CP and regular activity reporting to the CPA for the overall secure operation of the C-ITS trust model;
- receiving root CA certificates from the CPOC
- including/excluding root CA certificates in the ECTL upon notification by the CPA¹;
- signing the ECTL;
- the regular and timely transmission of the ECTL to the CPOC.

C-ITS Point of Contact (CPOC)

The CPOC is a unique entity appointed by the CPA. As described in Figure 2, the CPOC is for the purpose of this document divided in the term “CPOC ENTRY”, which is the end-point of the CPOC protocol to receive the RCA certificates and the “CPOC WEB”, which publishes the ECTL and other information.

¹ The TLM automatically removes expired RCA certificates in new versions of the ECTL.

Figure 2. Detailed view of the Common European Elements



The CPOC ENTRY is the endpoint of the CPOC protocol to collect the RCA certificates from the RCAs. The CPOC ENTRY is responsible for:

- establishing and contributing to the secure communication exchange between the CPOC and the CPA and the CPOC and RCAs,
- reviewing the procedural change requests and recommendations submitted by other trust model participants (i.e., RCAs),
- transmitting the RCA certificates to the Trust List Manager.

The CPOC WEB is a public website as well as distribution centre (for machine readable download) maintained by the EC-JRC administration that publishes the ECTL and TLM Certificates together with other information related to the deployment of C-ITS, e.g. additional guidelines or policy documents. The CPOC WEB is responsible for:

- the publication of the common trust anchor (EtsiTS103097Certificate of the TLM containing its public key, as well as any associated TLM link certificate messages) following the structure foreseen in [2] and requirements/clarifications in Annex I of the CPOC protocol,
- publication of the ECTL following the structure foreseen in [2] and requirements/clarifications in Annex I of the CPOC protocol,
- publication of other information related to the deployment of the C-ITS.

This main part of this report is focused on the CPOC protocol between the CPOC ENTRY and the CPA and RCAs. Annex I of this report focuses on descriptions of requirements, best practices and their implications on PKI participants regarding RCA and TLM certificates as well as the ECTL within the EU CCMS.

The terms CPOC ENTRY and CPOC WEB will be used in the rest of this report. Each of the components is also equipped with a repository to store the relevant data (e.g., RCA certificates). The CPOC ENTRY and CPOC WEB are implemented and operated on European Commission premises at DG Joint Research Centre, Via Enrico Fermi, 2749, 21027 Ispra (VA), Italy.

3 CPOC Protocol Overview

3.1 Conventions and Definitions

A manual protocol is used for the delivery of root CA certificates to the CPOC ENTRY in the EU CCMS.

The definitions of [1] apply. Further, the following definitions apply in this document:

- RCA Application Form: the RCA application form is a paper-based document that originates from RCA applicants and is transmitted to the CPA. It is signed by the RCA AR. Amongst other elements defined in [1], the application form includes the hash (SHA-256 or SHA-384) of the self-signed RCA EtsiTS103097 certificate. The current templates used for this process of application interaction of the RCA AR with the CPA AR can be found in the Annex of the CPOC protocol.
- RCA Application Approval Form: the RCA Application Approval Form is a paper-based document that originates from the CPA and is transmitted to RCA applicants and the CPOC/TLM. The current templates used for this process of application approval interaction of the CPA AR with the RCA AR can be found in the Annex of the CPOC protocol.

There are two main flows defined for the CPOC-RCA protocol. Each of these flows are described in the following subsections (as well as in some regards further detailed in Annex I):

- Add a new RCA certificate or add a new RCA certificate with linkage to previous RCA certificate to the ECTL.
- RCA Certificate revocation from the ECTL.

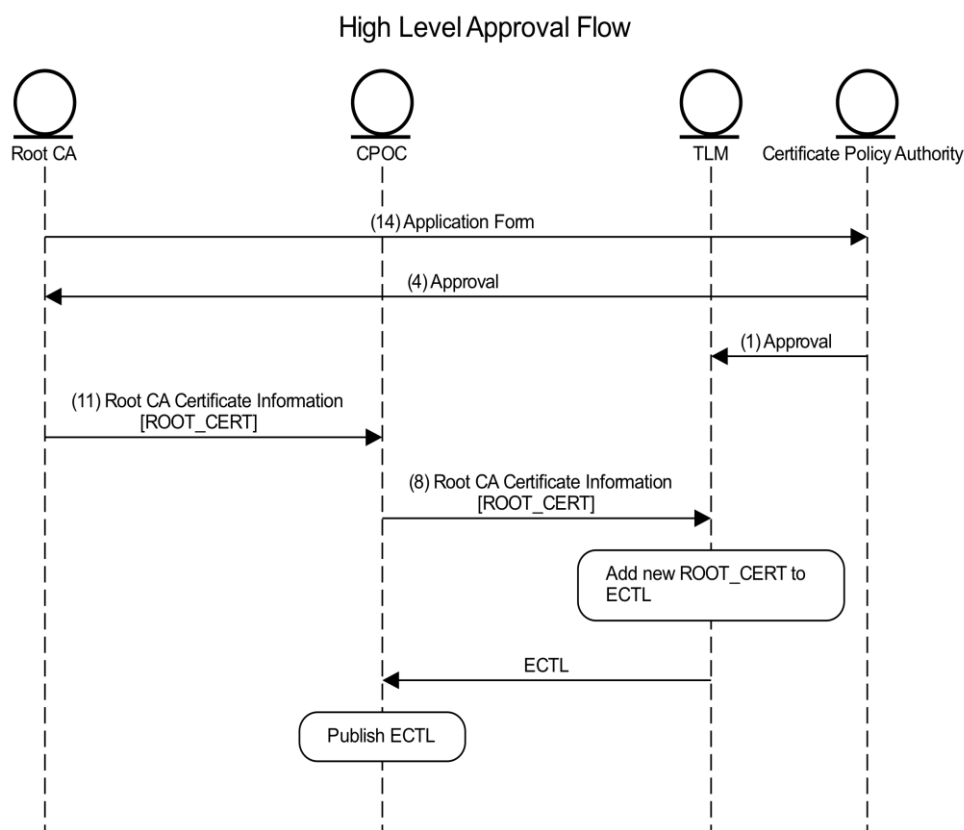
Note: The actual task of adding or removing RCA certificates from the ECTL is done by the TLM – however, in some cases the CPOC protocol describes the overall interaction between the CPOC, RCAs, CPA and TLM to give the full picture.

3.2 Add a new RCA certificate or add a new RCA certificate with linkage to previous RCA certificate to the ECTL

3.2.1 Related High level approval view

The general high-level approval flow of RCA Certificates to be inserted on the ECTL is depicted below:

Figure 3. RCA Certificate Management - High Level Flow (note that this is a subset of Figure 2 in the Certificate Policy [1])



RCA certificates may be added to the ECTL only after the RCA organization has successfully applied and received an RCA Application Approval from the CPA.

Note: While Figure 1 summarises the flows defined in the CP, note that in the EU CCMS implementation the RCA application approval (Flow 1) of the CPA will be transmitted to the CPOC to channel it through to the TLM in order to enable already at the level of the CPOC that only RCAs with valid applications approval forms can submit RCA certificates to the TLM for insertion in the ECTL.

3.2.2 Assurance Goals

Table 2: Assurance Goals between the CPOC ENTRY and RCAs for Flow 1 and Flow 2

Goal	Notes
(Prior to CPOC ENTRY/RCA Interaction) The audited ² system is the system that generated the self-signed RCA certificate	

² Audited means that the RCA has successfully passed the auditing process by an accredited PKI auditor according to the CP.

Goal	Notes
<p>(Prior to CPOC ENTRY/RCA Interaction)</p> <p>The RCA Certificate content is valid and approved by the CPA.</p>	<p>Minimally, the hash (SHA-256 or SHA-384) of the RCA certificate and any metadata (internal certificate fields such as validity period, issuance permissions (PSID-SSPs), etc. as specified in the CP [1]) associated with the RCA certificate needs to be provided to the CPA in the RCA application form (in fact the hash of the Root-CA certificate is part of the RCA Application Form as described in [1]). The process to validate the RCA Certificate is described in the CP in section 4.1.2.1.</p>
<p>(Prior to CPOC ENTRY/RCA Interaction)</p> <p>The RCA certificate is bound to a valid RCA Application Form approved by the CPA (for adding it to the ECTL)</p>	<p>The EU CCMS constrains the applications and permissions issuance rights of a RCA certificate according to the CPOC Protocol Annex I.</p>
<p>(Prior to CPOC ENTRY/RCA Interaction)</p> <p>Validation Checks are performed and verified for the RCA certificates as specified in the CP [1].</p>	<p>Validation checks as specified in the CP [1] as well as the CPOC ENTRY checks in Annex I.</p>
<p>(Prior to CPOC ENTRY/RCA Interaction)</p> <p>Submission of the RCA Enrolment Form. The RCA organisation joins the EU CCMS and ECTL scheme at the CPA.</p>	<p>The RCA Enrolment Form contains the administrative data of the RCA Organisation and its AR.</p>
<p>Submission of RCA certificates to the CPOC ENTRY can only be accomplished with a valid RCA application approval form.</p> <p>RCA application approval forms can only be submitted once the RCA Enrolment form has been approved and a <CPA-ID> has been assigned.</p>	<p>A strong consistency check is needed to correlate the RCA application approval form with:</p> <ol style="list-style-type: none"> 1) the self-signed RCA EtsiTS103097Certificate and hash of the RCA certificate that is presented/uploaded to the CPOC ENTRY. 2) the RCA organization <p>The applicable procedure for approval is described in detail in the CP [1] (chapter 4.1.2).</p>
<p>The entity requesting the addition or removal of RCA information with the CPOC ENTRY is authorized to make the request associated with the indicated credentials</p>	<p>The RCA representatives making the request is the entity with the credentials specified in the CP [1] (sections 3.2.2.1 and 3.2.3.1).</p>

3.2.3 Prerequisites

1. AR authenticators: AR authenticators (defined in the C-ITS Certificate policy, sections 3.2.2.1 and 3.2.3.1) have been pre-shared (RCA Enrolment form) and the following steps are achieved:

- a) The RCA and CPA organisation and AR identification and authentication information has been conveyed to the CPA and validated.
- b) The RCA AR authenticators are known to the CPOC ENTRY. The CPA has securely shared this information with the CPOC ENTRY ahead of time and out-of-band of the RCA / CPOC ENTRY interface. The identification information of the RCA representative is defined in section 3.2.3 of the CP [1].
- c) The CPOC ENTRY AR authenticators are known to the RCA AR. The CPA has securely shared this information with the RCA AR ahead of time and out-of-band of the RCA / CPOC ENTRY interface.

Note: The management of the AR authenticators of the RCA, CPA and CPOC/TLM is addressed within the processes of the CPA and implemented with the forms RCA Enrolment / RCA Enrolment approval.

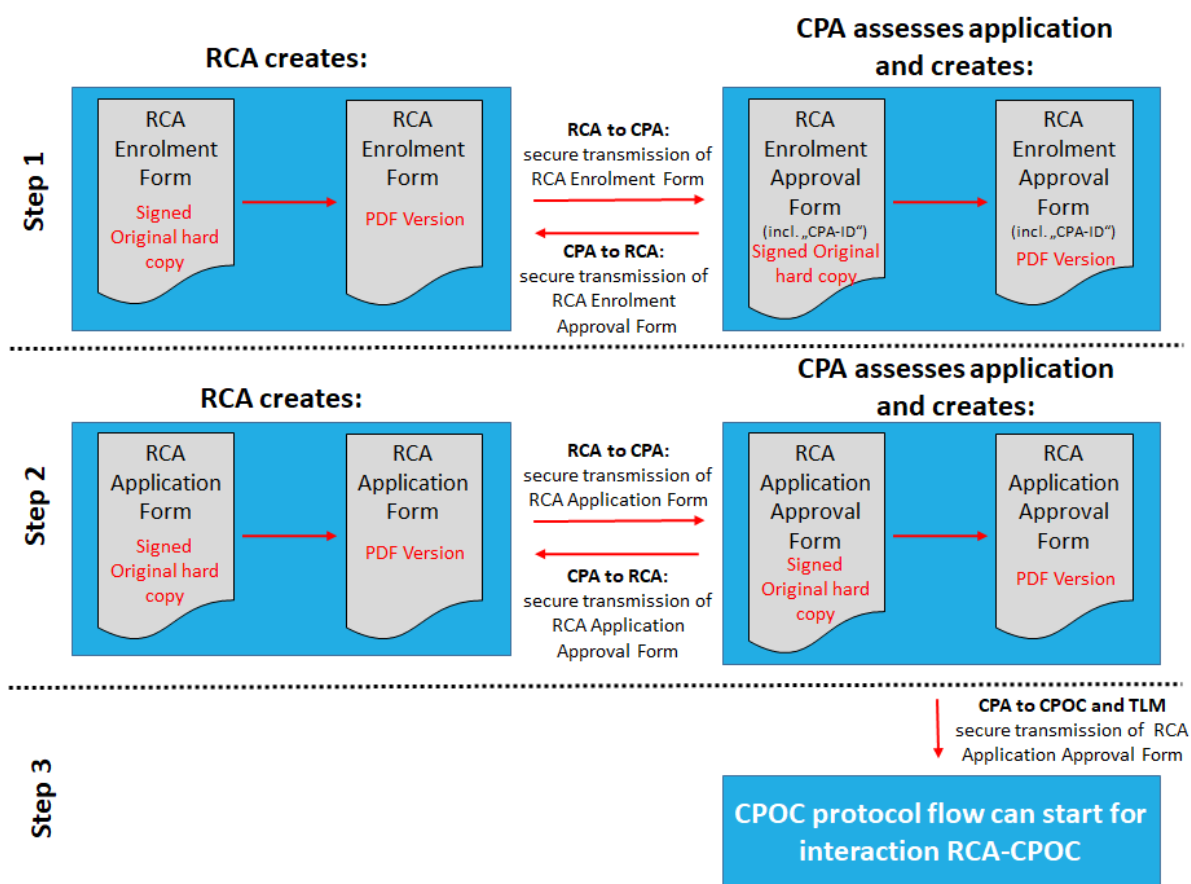
2. Audit: The RCA has been audited successfully according to the CP [1]:

- a) In addition to the audit procedure, specified in CP [1], this document also recommends (i.e., recommended steps and not mandatory step) the following: (If the new RCA Credential was already generated) there was sufficient evidence (e.g., witness documentation and verification) to validate that the audited system indeed generated the RCA certificate AND that only the audited system (and any authorized, documented backups) maintain the self-generated root private key. This could be performed via an auditor-witnessed root signing operation (over challenge data) that successfully verifies with the RCA's public key.
- b) The audit has been passed, including successful authentication of auditor's credentials.
- c) The auditor's audit report has been provided back to the applicant RCA organization.
- d) The Accredited PKI Auditor has successfully completed and submitted its Audit Report to the RCA (CP Flow 36)

3. Valid RCA Enrolment and RCA Application Form: The new (or existing) RCA organization has completed and submitted a valid RCA Enrolment Form (including the Accredited PKI Audit Report summary according to CP Flow 16) and RCA Application Form (CP Flow 14) to the CPA. In case the RCA intends to optionally make use of the remote re-key (with link certificate message) or urgent revocation (see section 3.3), the RCA organization shall also provide the necessary information to identify the RCA AR through eIDAS (e.g., identifiers, eIDAS provider) to the CPA via the RCA Application Form.

The process on the RCA Enrolment Form and RCA Application Form via an RCA-CPA-CPOC/TLM interaction is a pre-requisite for any insertion of RCA certificates into the ECTL. Figure 4 gives an overview of the practical use of the RCA Enrolment Form and RCA Application Form and RCA Enrolment Approval Form and RCA Application Approval Form (see templates in Annex) in order to achieve CPA approval of RCA enrolment & application requests to enter the ECTL. This process is a pre-requisite before any RCA certificate can be enrolled in the ECTL by the CPOC/TLM.

Figure 4. EU CCMS Process for each application approval process (RCA-CPA-CPOC interaction)



The following steps are depicted in Figure 4:

- Step 1: The RCA creates the RCA Enrolment Form (see Template in Annex II) in order to enrol the RCA organisation and its administrative information (including the authorised representative identifiers) in the EU CCMS. The RCA Enrolment Form shall also be used to deliver the latest CP Audit Report summary (which shall, if applicable, include any eventual relevant last CPS changes). The CPA processes the application and assigns a unique <CPA-ID> to the RCA Organisation.
- Step 2: In line with [1], Section 4.1.2.1., the RCA Application Form (see Template in Annex IV of the CPOC protocol) is prepared by the RCA. The RCA creates PDF versions of all the files and shall securely transmit the PDFs to the CPA AR. The CPA assesses the RCA application form and the CPA AR signs the RCA Application Approval Form hard copy version. The CPA AR creates a PDF version of the RCA Application Approval Form and shall securely transmit the PDF to the CPA AR and CPOC/TLM.
- Step 3: The work flow of the CPOC protocol to manage the insertion of RCA Certificates into the ECTL can start.

Note: The exact method of secure transmission of the RCA Enrolment Form, RCA Application Form and RCA application approval form between the RCA and CPA shall be addressed within the processes of the CPA.

3.2.4 Protocol flow

This flow is used to add:

- A new RCA certificate to the ECTL. This approach is used when either 1) the RCA certificate is new, or 2) when the RCA certificate requires no linkage to an already existing RCA certificate on the ECTL.

- A new RCA Certificate with a linkage that cryptographically binds it to a predecessor RCA Certificate. For more detailed information on RCA trust anchor exchange and technical definitions of RCA linkages in the EU CCMS please also see Annex I.

A manual protocol is defined for this interface.

The protocol is based on and will use the ASN.1 structures defined in ETSI standards [3] and [2], as well as the definitions in Annex I (e.g. describing the implementation of the concept of “Link Certificates” foreseen in [1]).

The ASN.1 encoded data structures according to the ETSI standards [3] and [2] as well as Annex I are transferred by manual delivery via a CD/DVD by the RCA AR to the CPOC ENTRY.

The following procedure applies to any interaction between RCAs and the CPOC ENTRY that want to take part in the EU CCMS. This manual protocol with the required physical presence of RCA representatives travelling to the CPOC ENTRY applies both for the initial enrolment of a root CA, as well as for all re-keying operations of root CA certificates (also see Annex I for additional information on re-keying principles of RCA certificates). The European Commission DG JRC acting as the CPOC supports this protocol at this moment in time with only two exceptions that can be processed remotely, the RCA re-key with link certificate message (cryptographic linkage) and the urgent revocation case.

In the future, this protocol may be revised to allow other methods of interaction with the CPOC ENTRY in line with the CP (e.g. via a secure communication protocol in order to perform additional actions remotely).

1. Following section 4.1.2.1 of the CP [1], **the RCA’s Trusted Courier shall:**

- (a) Travel to the CPOC, in possession of the following:
 - CD/DVD containing:
 - the self-signed RCA Certificate formatted as a `EtsiTs103097Certificate` structure according to [3].
 - In case of a re-keying of the RCA certificate, the new RCA self-signed `EtsiTs103097Certificate` and (if applicable) the double signed RCA link certificate message according to Annex I.
 - Its ID documents matching the information delivered in the RCA Enrolment Form.
 - The RCA Application Approval Form received from the CPA.
- (b) Provide his/her own Trusted Courier identification/authentication materials to the CPOC ENTRY AR corresponding to the RCA Enrolment Form.

2. The CPOC ENTRY AR shall:

- (a) Authenticate the RCA trusted courier based on its presented ID documents.
- (b) Verify that the presented RCA application approval form of the trusted courier is identical to the one that the CPOC has received from the CPA.

(If there are any mismatches, the operation is discontinued, logged and the mismatch is investigated)

- (c) On a secure, isolated system:
 - Insert the RCA’s CD/DVD and extract the information provided by the RCA for validation. This is the self-signed RCA `EtsiTs103097Certificate` and where applicable link certificate messages (as defined in Annex I).
 - Generate a hash (SHA-256 / SHA-384) over any RCA certificates (in COER binary format) being added to the ECTL. The hash of the RCA certificates is stored in the CPOC ENTRY and also used for revocation of the RCA certificate.
- (d) For any RCA certificate being added to the ECTL,

- Check that the generated Hash equals the Hash of the RCA certificate (already verified to be equal to that on the RCA AR's presented RCA application approval form). In addition all the parameters and signatures in the RCA certificate shall also be verified, taking into account all CPOC ENTRY checks defined in Annex I.
- It is recommended (but not mandatory) to validate that the upload datetime is within the 'upload window', a period of time during which the approved upload (or indicated revocation) may be performed (approvals made too far in the past should be reinvestigated by the CPA before the upload is allowed to proceed).
- In case of an update of a RCA certificate, where a link certificate message is provided: validate the RCA link certificate message as described in Annex I.

(If there are any miss-matches, the operation is discontinued, logged and the mismatch is investigated)

If all checks pass, successfully, the CPOC ENTRY shall:

- Transfer the digital copy of RCA certificate (and the link RCA certificate message in case of an update of a RCA certificate) to the TLM via interface over CP Flow 8 [1],
- Log the successful procedure and transfer to the TLM
- Provide a "Response CD/DVD" to the RCA trusted courier, including:
 - Copy of the new signed ECTL (if available)
 - Copy of the current TLM Certificate
 - Overview document including information on the date and time of the RCA certificate addition, the planned publication date in the ECTL, hash of the RCA certificate, etc.

3.3 RCA Certificate revocation from the ECTL

3.3.1 Overview on revocation scenarios and high level assurance goals

The operator of a RCA can use the mechanisms of this section to request that the RCA is revoked on the ECTL. In this interface, the RCA and CPOC ENTRY Authorized representatives mutually authenticate each other, the RCA provides the CPOC ENTRY with a hash (SHA-256 / SHA-384) of the to-be-revoked Root certificate, and the CPOC ENTRY acknowledges the removal request.

Building upon section 7.3.1 of the CP [1], for the purpose of this CPOC protocol the RCA certificate revocation are described in the following scenarios in subsequent sections:

- Revocation Scenario 1: The compromise or suspected compromise of a RCA system.
 - Revocation Scenario 1a: The incident is not considered of critical importance by the RCA management entity and/or the CPA.
 - Revocation Scenario 1b: The incident is considered of critical importance by the RCA management entity and/or the CPA. The removal of the associated RCA certificate from the ECTL shall be executed as soon as possible.
- Revocation Scenario 2: The need to upgrade an entire certificate chain's cryptographic algorithm type/strength following approval of the CPA,
- Revocation Scenario 3: Activities originating from an organizational, industry or regulatory change to the C-ITS trust model or new policies that warrant root certificate replacement.
- Revocation Scenario 4: RCA managing entity exiting the market.

Since RCA revocation may have a significant impact on the C-ITS system, if it is possible for the RCA operator to give advance notice of the revocation to the CPOC/TLM, this should be done to enable the impact to be gauged and mitigations to be planned.

The assurance goals for this component of the interface are as follows.

Table 3: RCA Revocation High Level Assurance Goals

Goal	Notes
Root revocation is performed only for the authorized party	The RCA entity making the request needs to be authorized to request revocation on the specified root certificate.
Revocation actions need to be coordinated in time with other activities.	RCAs need to be able to specify a future point in time before which the revocation will not be performed.

RCA certificate revocation is an informative process. Policy shall require notification ahead of time to the CPA so that possibly wide-ranging impacts to the C-ITS system are gauged and understood.

3.3.2 Prerequisites

1. The RCA Enrolment Form, RCA Application Form have been approved and a RCA Certificate of the RCA organisation is enrolled on the ECTL.
2. The RCA Authorized Representative has informed the CPA of the intent to revoke a root credential. This information shall include the intended revocation date, which is within the policy constraint.

3.3.3 Protocol flow for revocation scenarios 1a, 2, 3 and 4

Based on the scenarios defined in chapter 3.3.1, the following revocation flow shall apply to Scenario 1a, 2, 3 and 4:

1. The RCA trusted courier shall physically travel to the CPOC ENTRY.
2. The CPOC AR shall check the RCA trusted courier's ID according to the RCA enrolment form
3. The RCA trusted courier shall present the RCA Revocation Form (see Annex VI), populated, dated and signed by the RCA AR (see Annex). Further, the RCA trusted courier shall present the corresponding RCA application approval form.
4. The CPOC ENTRY shall validate the following:
 - The RCA certificate exists (based on its SHA-256/SHA-384 hash), is currently valid, and is published in the ECTL.
 - The requested revocation time is within the policy-constrained maximum time in the future.
 - The provided hash of the RCA Certificate within the RCA Revocation Form matches the recorded hash at the CPOC and RCA Application Approval Form.
5. If any validation checks fail, STOP and notify the CPA. Otherwise, PROCEED.
6. The CPOC AR shall provide a "Response CD/DVD" to the RCA trusted courier, including at least:
 - Copy of the newly signed ECTL (if available).
 - Copy of the current TLM Certificate.
 - Overview document including information on the date and time of the RCA certificate revocation, the planned publication date in the ECTL, hash of the RCA certificate.

The newly signed ECTL shall be published on the CPOC WEB accordingly.

3.3.4 Protocol flow for revocation scenario 1b (critical RCA certificate revocation)

According to the scenarios defined in chapter 3.3.1, the following revocation flow shall apply to Scenario 1b:

1. The RCA Authorized Representative can optionally choose to not physically travel to the CPOC ENTRY.
2. Instead, The RCA Authorized Representative shall send an email to the CPOC ENTRY (JRC-CPOC@ec.europa.eu) with the RCA Enrolment Form (see template in Annex II)

The e-mail containing the RCA revocation Form shall be signed using the eIDAS compliant digital certificate (i.e. issued by a trust service provider enrolled in the eIDAS EU Trust List) of the RCA AR. [4]

3. The RCA and CPOC ENTRY ARs shall mutually authenticate by additional remote communication. The CPOC ENTRY will contact the physical representative of the RCA AR through phone or other secure means to confirm the request and the information defined in the previous step. If authentication fails, STOP and notify the CPA; otherwise PROCEED.
4. The CPOC ENTRY shall validate the following:
 - The RCA certificate exists (based on its SHA-256/SHA-384 hash), is currently valid, and is published in the ECTL
 - The requested revocation time is within the policy-constrained maximum time in the future
 - The provided hash of the RCA Certificate within the RCA Revocation Form matches the recorded hash at the CPOC and RCA Application Approval Form.
5. If any validation checks fail, STOP and notify the CPA. Otherwise, PROCEED. The TLM shall create and sign a new ECTL with the corresponding RCA certificate removed.
6. The CPOC AR shall provide an acknowledgement e-mail containing at least the following:
 - Copy of the newly signed ECTL
 - Copy of the current TLM Certificate
 - Overview document including information on the date and time of the RCA certificate revocation, the planned publication date in the ECTL, hash of the RCA certificate, etc.

The newly signed ECTL shall be published on the CPOC WEB accordingly.

4 Conclusions

The contents of Release 3.0 of the CPOC Protocol were approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in December 2023.

The aim of this document is to lay down the processes for interaction between RCAs, CPOC and CPA as well as to define the RCA-CPOC interface. The CPOC Protocol plays an essential role within the European Union C-ITS Security Credential Management System (EU CCMS) and 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 interface specification and also clear rules and guidelines especially to all stakeholders wanting to implement and deploy RCAs within the European C-ITS trust domain.

Until a dedicated entity is appointed as C-ITS 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 protocol.

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

- [1] European Commission, "*Certificate policy for deployment and operation of European cooperative intelligent transport systems (C-ITS)*", Release 3: <https://cpoc.jrc.ec.europa.eu/>, 2023.
- [2] European Telecommunications Standards Institute, *ETSI TS 102 941 V1.4.1 (2021-01) or V2.2.1 (2022-11) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*.
- [3] European Telecommunications Standards Institute, *ETSI TS 103 097 V1.4.1 (2020-10) or V2.1.1 (2021-10) Intelligent transport systems (ITS) security; security header and certificate formats*.
- [4] "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," OJ L 257/73, 2014.
- [5] European Telecommunications Standards Institute, "ETSI TS 102 965 Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2" .
- [6] "C-ITS Day-1 Services, listed in table 3 of the C-ITS Platform Phase I final report of January 2016," 2016.
- [7] Car 2 Car Communication Consortium, "Basic System Profile," v1.6 or newer. [Online]. Available: <https://www.car-2-car.org/documents/basic-system-profile/>.
- [8] C-ROADS, "Harmonised C-ITS specifications for Europe," Release 2.0 or newer.
- [9] International Organization for Standardization, "ISO 15408-1:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security / Common Criteria," 2022.
- [10] International Telecommunication Union, *Information technology – ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)*, 2014.
- [11] "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages".*IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)* , vol., no., pp.1-240, 1 March 2016.
- [12] European Commission, "*Security policy for deployment and operation of European cooperative intelligent transport systems (C-ITS)*", Release 3: <https://cpoc.jrc.ec.europa.eu/>, 2023.

List of abbreviations

AA	Authorisation Authority
AR	Authorised Representative
CA	Certification Authority
C-ITS	Cooperative Intelligent Transport Systems
CP	Certificate Policy
CPA	Certificate Policy Authority
CPOC	C-ITS Point of Contact
CPS	Certificate Practice Statement
DC	Distribution Centre
EA	Enrolment Authority
EC	Enrolment Credential
ECTL	European Certificate Trust List
EU CCMS	European Union C-ITS Security Credential Management System
PKI	Public Key Infrastructure
PP	Protection Profile
RCA	Root Certification Authority
RCA AR	Root Certification Authority Authorised Representative
TLM	Trust List Manager
TOE	Target of Evaluation. The target of evaluation is a security-relevant part of the C-ITS station.

List of figures

Figure 1. High level view of the EU CCMS trust model (from [1])	4
Figure 2. Detailed view of the Common European Elements	5
Figure 3. RCA Certificate Management - High Level Flow (note that this is a subset of Figure 2 in the Certificate Policy [1])	7
Figure 4. <i>EU CCMS Process for each application approval process (RCA-CPA-CPOC interaction)</i>	10
Figure 5: Example timetable of TLM regular re-keying and publishing of ECTLs in the EU CCMS.....	46
Figure 6: General schematic representation of transition period using the concept of a “link certificate” (shown is the case of a RCA certificate).....	52
Figure 7: Overview of the different EU CCMS Environments and their relation to TLM/ECTL	90
Figure 8: Overview and timeline of ECTL levels	91

List of tables

Table 1: Release Versions	3
Table 2: Assurance Goals between the CPOC ENTRY and RCAs for Flow 1 and Flow 2	7
Table 3: RCA Revocation High Level Assurance Goals	13
Table 4: ITS-AID values allowed in the EU CCMS based on ETSI/ISO according to ETSI TS 102 965 [5]	41
Table 5: Specification of maximum permissions contained in a RCA certificate in the EU CCMS	42
Table 6: Consistency requirements for TLM Link Certificates	53
Table 7: Requirements on new TLM certificates to permit it to be the subject of a link certificate	54
Table 8: Single Signed RCA Link Certificate: consistency between old CA (signer) and new CA (subject)	55
Table 9: Requirements on New Root CA certificate to permit it to be the subject of a link certificate	56
Table 10: Double Signed RCA Link Certificate: consistency between new CA (signer) and old CA (subject)	57
Table 11: Requirements on Old Root CA certificate to permit it to be the subject of a double-signed link certificate	58
Table 12: CPOC ENTRY checks of the attributes of RCA Certificates	64
Table 13: CPOC ENTRY checks of other properties of RCA Certificates	67
Table 14: Treatment of L1 and L2 messages on the receiver side	92
Table 15: Overview of requirements of the three EU CCMS Levels	93
Table 16: Level 1 Exceptions	95
Table 17: Level 1 Evaluation Tasks for the TOE of the C-ITS Station and respective Developer Content (see exception item no. 1 in Table 16)	97
Table 18: Generic Security Objectives for the C-ITS Station (TOE) and the Environment (see exception item no. 1 in Table 16)	102

Annexes

Annex I. Requirements & best practices of TLM certificates, RCA certificates and the ECTL

I.1. Overview

ETSI and IEEE specifications provide detailed definitions of a RCA certificate content and ASN.1 for the RCA certificate OER encoded binary. Moreover, the European Commission has also issued a Certificate Policy [1] document to specify policies, attributes and values in the RCA certificate.

Organizations operating as a RCA register their RCA certificate to the TLM through the CPOC. The TLM then regularly publishes the ECTL containing all registered RCA certificates. Other PKI entities (EA, AA, mobile and fixed C-ITS stations...) download the ECTL, parse its content and extract RCA certificates for their own operations.

During an initial TLM testing phase operated by Gemalto on behalf of the European Commission in the course of the 6th ITS CMS C-ITS Security Plugtest, it has been observed that the content of RCA certificates received from several RCA operators in Europe for testing purposes show a lot of differences, e.g. attributes such as appPermissions and certIssuePermissions are interpreted differently from RCA certificate issuers, some values may not be optimal, and some others may result in a non-deterministic and non-expected result.

Facing this content divergence, PKI entities which consume (i.e. load and parse) RCA certificates from the ECTL will require higher development and validation effort to adjust the software behaviour for different RCA certificates' content. Moreover, from the security perspective, different RCA certificate contents mean more attack surface for the attacker, e.g. allowing unlimited permission of services could also open other attack opportunities.

The goal of this document as Annex I of the CPOC protocol is to provide binding technical requirements on RCA certificates that are delivered to the CPOC for insertion in the ECTL as well as a collection of requirements, best practices, recommendation and guidance for a more consistent RCA certificate content in the context of the EU CCMS. Following these requirements and best practices, RCA certificate issuers and consumers shall reach a better development cost and security trade-off, which is considered as the common interest to the European C-ITS ecosystem.

I.1.1. Scope of Annex I

The scope of this Annex I of the CPOC protocol is:

- To provide a list of attributes and their optimal value along with the rational of those values.
- To apply security principle on some values.
- To reach a consistent RCA certificate content in the context of the EU CCMS by means of some RCA certificate templates as example.
- To define binding technical requirements that the CPOC ENTRY is going to check based on the RCA certificate template.
- To provide clear descriptions on how re-keying works in the EU CCMS of TLM and RCA Certificates, including the requirements on Link Certificates.
- To define requirements for the TLM issuing ECTLs as well as for PKI participants in processing it.

All requirements of this Annex I of the CPOC protocol are to be seen as complementary to the existing set of policy documents and standards.

The currently applicable EU CCMS policy documents can be found on the website of the CPOC at <https://cpoc.jrc.ec.europa.eu/>

I.2. TLM Certificate and attributes

I.2.1. TLM Certificate Overview

I.2.1.1. Example TLM certificate in the EU CCMS

The following gives an example of the contents of the TLM Certificate according to [1] and [3].

```

value EtsiTs103097Certificate ::= {
  version 3,
  type explicit,
  issuer self : sha384,
  toBeSigned {
    id name : "EU-TLM",
    cracaId '000000'H,
    crlSeries 0,
    validityPeriod {
      start 499125603,
      duration years : 4
    },
    appPermissions {
      {
        psid 624,
        ssp bitmapSsp : '01C8'H
      }
    },
    verifyKeyIndicator verificationKey : ecdsaBrainpoolP384r1 : compressed-
y-1 :
'893FDE2EB186A0D63BC21E1AF2E8B661C43401A3900591AA034F0B968C4972C0E339F2'H -
- truncated --
  },
  signature ecdsaBrainpoolP384r1Signature : {
    rSig x-only :
'250FF690EB12B8BA16983FCEFACA4187D3397B8E6B686A48F8BFEAAF2C3FF874838F1E'H -
- truncated --,
    sSig
'385DAABF81C1631BB0433EA496ECAE4D32E5CADEA39FD08BF4EA0BAE9AAB52A2291BDC'H -
- truncated --
  }
}

```

Note: This TLM certificate example is taken from the ETSI plug-test of November 2019 and has been adapted (id name has been changed from “ECTL” to “EU-TLM” in line with chapter I.2.2). Hence the signature shown above (in yellow) is not valid anymore. The correct signature will be updated once available, however since it is truncated it is not possible to double check it anyway.

I.2.2. Implementation choices for the EU CCMS TLM Certificate

I.2.2.1. TLM CertificateID

Detailing the CP [1], the naming scheme of the TLM Certificate in the EU CCMS shall be able to reflect a possible level nature of its operating environment. Hence, a mandatory naming scheme for CertificateID within the TLM Certificates is introduced to provide such flexibility.

The `CertificateID` in TLM Certificates shall consist of the pre-fix “EU-TLM” and an optional `<TLM-ENVIRONMENT>` component, combined with a separator (“_”):

EU-TLM_<TLM-ENVIRONMENT>

Detailed specification of the components of the TLM `CertificateID`:

- The pre-fix shall be set to “EU-TLM”.
- `<TLM-ENVIRONMENT>`: is an optional component that can be set by the TLM to create TLM certificates which are used to sign specific ECTLs for specific RCA certificate environments (in line with the optional `<RCA_ENVIRONMENT>` fields in the RCA `CertificateID` in chapter I.3.2.2). The optional field `<TLM-ENVIRONMENT>` can be set by the TLM following instruction of the CPA with one of the following entries:
 - L0 (Level 0: indicates TLM Certificates which are used to sign ECTLs including L0 RCA Certificates)
 - L1 (Level 1: indicates TLM Certificates which are used to sign ECTLs including L1 RCA Certificates)
 - Any other specific indicators to reflect specific maturity of C-ITS service operations for C-ITS in the EU CCMS agreed on by the CPA on a case by case basis (e.g. L2 or other TLM environments if needed).

Note: The `<TLM-ENVIRONMENT>` component within the TLM `CertificateID` serves as an additional indicator to avoid any mix-up of TLM Certificates and their intended operating environment, especially in the ramp-up phase of C-ITS services in the EU. The CPOC shall in principle only publish fully CP compliant environment RCA Certificates for insertion into the ECTL, unless the CPA instructs the CPOC differently according to the given indicators and defined levels.

Examples TLM `CertificateID`:

- EU-TLM
 - The TLM can choose to not set any specific environment – this example corresponds to TLM certificates which are used to sign ECTLs containing RCA Certificates with no specific environments defined.
- EU-TLM_L0
 - This example is the TLM `CertificateID` of the L0 TLM Certificate used to sign L0 ECTLs containing L0 RCA Certificates.
- EU-TLM_L1
 - This example is the TLM `CertificateID` of the L1 TLM Certificate used to sign L1 ECTLs containing L1 RCA Certificates.
- EU-TLM_xyz
 - This example assumes a specific purpose “xyz” (or abc123, or any other) defined by the CPA. In that case, the “EU-TLM_xyz” is the TLM `CertificateID` of the “xyz” TLM Certificate used to sign “xyz” ECTLs containing “xyz” RCA Certificates.

I.2.2.2. TLM Region

According to TS 103 097 [3] the TLM Certificate (which is an `EtsiTs103097Certificate`) shall have a certificate content of type

`ToBeSignedCertificate` and may optionally include the component `region` of type `GeographicRegion`.

In the EU CCMS the TLM certificates shall comply with the following additional constraints:

The component `region` shall be absent.

Note: this implies that the TLM certificate does not further constrain the geographical validity of the ECTL and the RCA certificates contained in it.

I.3. RCA certificate and attributes

I.3.1. RCA Certificate Overview

I.3.1.1. Example RCA certificate

This section firstly provides a RCA certificate example according to [1] and [3]. The next section includes further explanations.

Note: Although the example shows duration 8 years, the maximum RCA Certificate validity has been reduced to 5 years instead of 8 years according to chapter I.3.3.

```
{
  "version": 3,
  "type": "explicit",
  "issuer": {"self": "sha256"},
  "toBeSigned": {
    "id": {"name": "A RCA name"},
    "cracald": "000000",
    "crlSeries": 0,
    "validityPeriod": {
      "start": 474103935,
      "duration": {"years": 8}
    },
  },
  "appPermissions": [
    {
      "psid": 624,                                -- 0x0270, IEEE registered Certificate Trust List Service
      "ssp": {"bitmapSsp": "0138"}
    },
    {
      "psid": 622,                                -- 0x026e, IEEE registered Certificate Revocation List Service
      "ssp": {"bitmapSsp": "01"}
    }
  ],
  "certIssuePermissions": [{
    "subjectPermissions": {"explicit": [
      {
        "psid": 36,                                -- 0x24, IEEE registered CA Basic Service
        "sspRange": {"bitmapSspRange": {
          "sspValue": "01FFFC",
          "sspBitmask": "FF0003"
        }}
      },
    ]
  },
  {
```

```

"psid": 37,                                -- 0x25, IEEE registered DEN Basic Service
"sspRange": {"bitmapSspRange": {
    "sspValue": "01FFFFFF",
    "sspBitmask": "FF000000"
}}
},
{
"psid": 137,                              -- 0x89, IEEE registered TLM (Traffic Light Manoeuver) Service
"sspRange": {"bitmapSspRange": {
    "sspValue": "01E0",
    "sspBitmask": "FF1F"
}}
},
{
"psid": 138,                              -- 0x8a, IEEE registered RLT (Road and Lane Topology) Service
"sspRange": {"bitmapSspRange": {
    "sspValue": "01C0",
    "sspBitmask": "FF3F"
}}
},
{
"psid": 139,                              -- 0x8b, IEEE registered IVI (Infrastructure to Vehicle Information) Service e
"sspRange": {"bitmapSspRange": {
    "sspValue": "01000000FFF8",
    "sspBitmask": "FF0000000007"
}}
},
{
"psid": 140,                              -- 0x8c, IEEE registered TLC (Traffic Light Controler Request Service) Service
"sspRange": {"bitmapSspRange": {
    "sspValue": "02FFFFE0",
    "sspBitmask": "FF00001F"
}}
},
{
"psid": 141,                              -- 0x8d, IEEE registered GeoNetworking Management Communication
},
{
"psid": 623,                              -- 0x026f, IEEE registered Secured Certificate Request Service
"sspRange": {"bitmapSspRange": {
    "sspValue": "01C0",
    "sspBitmask": "FF3F"
}}
}

```

```

    },
    {
      "psid": 637,
      -- 0x27d, IEEE registered TLC (Traffic Light Controller Status Service) Service
      "sspRange": {"bitmapSspRange": {
        "sspValue": "01",
        "sspBitmask": "FF"
      }}
    },
  ],
  "minChainLength": 2,
  -- minChainLength and chainLengthRange indicate how long
  -- the certificate chain from this certificate to the end-entity certificate is permitted to be,
  -- (IEEE 1609.2a-2017 sections 5.1.2.1, 6.4.30)

  "chainLengthRange": 0,
  "eeType": "C0"
  -- (app, enroll)
},
"certIssuePermissions": [{
  "subjectPermissions": {"explicit": [
    {
      "psid": 623,
      -- 0x026f, IEEE registered Secured Certificate Request Service with default value for
      minChainLength = 1 and chainLengthRange = 0 and eeType = App
      "sspRange": {"bitmapSspRange": {
        "sspValue": "013E",
        "sspBitmask": "FFC1"
      }}
    }
  ]}
}],
},
},
"verifyKeyIndicator": {"verificationKey": {"ecdsaBrainpoolP256r1": {
  "compressed-y-0": "272833C1980A51AAB624D1C032E82CB220E8B7A2814AC18C8F0E837ECB4EB112"}}
},
"signature": {"ecdsaBrainpoolP256r1Signature": {
  "rSig": {"x-only": "300E0A34A7C19015E5E1A30DA8EC2CB33C8D318D9A58BEC8FFC63ED71456CFD6"},
  "sSig": "8ACBF7809990D3AA34BC72747F2DE7EF2BD2B66DDE32F54BD1F04DFF38BD1345"
}}
}

```

I.3.1.2. Example RCA Certificate – More detailed explanations

This section contains a general RCA certificate template, which serves as example to show common values in an RCA certificate and the description of each service permission and the bit position. The permissions in this template shall be considered as example values and not as default values.

Note: Although the example shows duration 8 years, the maximum RCA Certificate validity has been reduced to 5 years instead of 8 years according to chapter I.3.3

```

{
  "version": 3,
  "type": "explicit",
  "issuer": {"self": "sha256"},

```

```

"toBeSigned": {
  "id": {"name": "RCA name"},
  "cracald": "000000",
  "crlSeries": 0,
  "validityPeriod": {
    "start": 474103935,
    "duration": {"years": 8}
  },
  "appPermissions": [
    {
      "psid": 624,                                -- 0x0270, IEEE registered CTL (Certificate Trust List) service
      "ssp": {"bitmapSsp": "0138"}                -- byte 0, 0x01, SSP version control
                                                    -- byte 1, 0x38 (binary 00111000), the RCA operates the CTL service and has the permissions
                                                    -- 0x20 (bit 2)          to sign CTL containing EA entries
                                                    -- 0x10 (bit 3)          to sign CTL containing AA entries,
                                                    -- 0x08 (bit 4)          to sign CTL containing DC entries
    },
    {
      "psid": 622,                                -- 0x026e, IEEE registered Certificate Revocation List service
      "ssp": {"bitmapSsp": "01"} -- byte 0, 0x01, SSP version control
    }
  ],
  "certIssuePermissions": [{
    "subjectPermissions": {"explicit": [
      {
        "psid": 36,                                -- 0x24, IEEE registered CA (Cooperative Awareness) service.
        "sspRange": {"bitmapSspRange": {
          "sspValue": "01FFFC", -- byte 0, 0x01, SSP version control
                                                    -- byte 1, 0xfffc (binary 11111111 11111100), the CA service permission provide the ability for
                                                    -- subordinate certificates to sign CA messages with the following specific containers:
                                                    -- 0x80 (byte 1, bit 0)      "Tolling zone",
                                                    -- 0x40 (byte 1, bit 1)      "Public transport",
                                                    -- 0x20 (byte 1, bit 2)      "Special transport",
                                                    -- 0x10 (byte 1, bit 3)      "Dangerous goods",
                                                    -- 0x08 (byte 1, bit 4)      "Road work",
                                                    -- 0x04 (byte 1, bit 5)      "Rescue",
                                                    -- 0x02 (byte 1, bit 6)      "Emergency",
                                                    -- 0x01 (byte 1, bit 7)      "Safety car",
                                                    -- 0x80 (byte 2, bit 0)      "Close lanes",
                                                    -- 0x40 (byte 2, bit 1)      "Request for right of way",
                                                    -- 0x20 (byte 2, bit 2)      "Request for free crossing at a traffic light",
                                                    -- 0x10 (byte 2, bit 3)      "No passing",
                                                    -- 0x08 (byte 2, bit 4)      "No passing fro trucks",

```



```

-- 0x04 (byte 2, bit 5)          "Speed limit",
-- 0x02 (byte 2, bit 6)          reserved for future usage,
-- 0x01 (byte 2, bit 7)          reserved for future usage.

"sspBitmask": "FF0003"          -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA
responsibility

-- to deliver or not to deliver the permission to subordinate entities

}}
},
{
"psid": 37,                    -- 0x25, IEEE registered DEN service
"sspRange": {"bitmapSspRange": {
"sspValue": "01FFFFFF",       -- byte 0, 0x01, SSP version control
                                -- byte 1 to 3, 0xffffffff (binary 11111111 11111111 11111111), the DEN service permissions
                                -- allow subordinate certificates to sign DEN messages with the following data item:
                                -- 0x80 (byte 1, bit 0)          "Traffic condition",
                                -- 0x40 (byte 1, bit 1)          "Accident",
                                -- 0x20 (byte 1, bit 2)          "Road works",
                                -- 0x10 (byte 1, bit 3)          "Adverse weather condition - adhesion",
                                -- 0x08 (byte 1, bit 4)          "Hazardous location – surface condition",
                                -- 0x04 (byte 1, bit 5)          "Hazardous location – obstacle on the road",
                                -- 0x02 (byte 1, bit 6)          "Hazardous location – animal on the road",
                                -- 0x01 (byte 1, bit 7)          "Human presence on the road",
                                -- 0x80 (byte 2, bit 0)          "Wrong way driving",
                                -- 0x40 (byte 2, bit 1)          "Rescue and recovery working in progress",
                                -- 0x20 (byte 2, bit 2)          "Adverse weather condition – extreme weather condition",
                                -- 0x10 (byte 2, bit 3)          "Adverse weather condition – visibility",
                                -- 0x08 (byte 2, bit 4)          "Adverse weather condition – precipitation",
                                -- 0x04 (byte 2, bit 5)          "Slow vehicle",
                                -- 0x02 (byte 2, bit 6)          "Dangerous end of queue",
                                -- 0x01 (byte 2, bit 7)          "Vehicle break down",
                                -- 0x80 (byte 3, bit 0)          "Post crash",
                                -- 0x40 (byte 3, bit 1)          "Human problem",
                                -- 0x20 (byte 3, bit 2)          "Stationary vehicle",
                                -- 0x10 (byte 3, bit 3)          "Emergency vehicle approaching",
                                -- 0x08 (byte 3, bit 4)          "Hazardous location – dangerous curve",
                                -- 0x04 (byte 3, bit 5)          "Collision risk",
                                -- 0x02 (byte 3, bit 6)          "Signal violation",
                                -- 0x01 (byte 3, bit 7)          "Dangerous situation".

                                "sspBitmask": "FF000000"          -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
                                to deliver

                                -- or not to deliver the permission to subordinate entities

                                }}
                                },
                                {
                                "psid": 137,                    -- 0x89, IEEE registered TLM (Traffic Light Manoeuvre) Service

```

```

"sspRange": {"bitmapSspRange": {
  "sspValue": "01e0",      -- byte 0, 0x01, SSP version control
                             -- byte 1, 0xe0, (binary 11100000), the TLM service permissions allow
                             -- subordinate certificates to sign SPATEM messages with the following data item:
                             -- 0x80 (bit 0)      "Signal Phase and Timing"
                             -- 0x40 (bit 1)      "Public transport prioritization status response"
                             -- 0x20 (bit 2)      "Maneuver assisting information"
  "sspBitmask": "FF1F"     -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

                             -- or not to deliver the permission to subordinate entities
}}
},
{
  "psid": 138,              -- 0x8a, IEEE registered RLT (Road and Lane Topology) Service
  "sspRange": {"bitmapSspRange": {
    "sspValue": "01C0",     -- byte 0, 0x01, SSP version control
                             -- byte 1, 0xc0 (binary 11000000), the RLT service permissions allow
                             -- subordinate certificates to sign MAPEM messages with the following data item:
                             -- 0x80 (bit 0)      "Intersections geometry list allowed to transmit"
                             -- 0x40 (bit 1)      "Road geometry list allowed to transmit"
    "sspBitmask": "FF3F"    -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

                             -- or not to deliver the permission to subordinate entities
}}
},
{
  "psid": 139,              -- 0x8b, IEEE registered IVI (Infrastructure to Vehicle Information) Service
  "sspRange": {"bitmapSspRange": {
    "sspValue": "01000000FFf8", -- byte 0, 0x01, SSP version control
    -- byte 1 to 3, "Identification of the Service Provider for which the R-ITS-S is allowed
    -- to send out IVIM and to which the Service-specific parameter apply"
    -- byte 4 to 5, 0xffff8 (binary 11111111 11111000), the IVI service permissions allow
    -- subordinate certificates to sign "General IVIM container" with the following data item:
    -- 0x80 (byte 4, bit 0) "Vienna Convention Code for road sign"
    -- 0x40 (byte 4, bit 1) "ISO/TS 14823 road signs with traffic sign pictogram set to Danger
warning"
    -- 0x20 (byte 4, bit 2) "ISO/TS 14823 road signs with traffic sign pictogram set to
regulatory"
    -- 0x10 (byte 4, bit 3) "ISO/TS 14823 road signs with traffic sign pictogram set to
informative"
    -- 0x08 (byte 4, bit 4) "ISO/TS 14823 road signs with public facilities pictogram"
    -- 0x04 (byte 4, bit 5) "ISO/TS 14823 road signs with ambient and road conditions set to
ambientCondition"
    -- 0x02 (byte 4, bit 6) "ISO/TS 14823 road signs with ambient and road conditions set to
ambientConditionn"
    -- 0x01 (byte 4, bit 7) "the ITIS codes"
  }
}

```

```

-- 0x80 (byte 5, bit 0) "laneStatus"
-- 0x40 (byte 5, bit 1) "Road Configuration Container"
-- 0x20 (byte 5, bit 2) "Text container"
-- 0x10 (byte 5, bit 3) "Layout Container"
-- 0x08 (byte 5, bit 4) "IVI Status (negation)"
-- 0x04 (byte 5, bit 5) not used, set to 0
-- 0x02 (byte 5, bit 6) not used, set to 0
-- 0x01 (byte 5, bit 7) not used, set to 0

"sspBitmask": "FF0000000007" -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

-- or not to deliver the permission to subordinate entities

}}
},
{
"psid": 140, -- 0x8c, IEEE registered TLC (Traffic Light Controler Request Service) Service
"sspRange": {"bitmapSspRange": {
"sspValue": "02FFFE0", -- byte 0, 0x02, SSP version control
-- byte 1 to 3, 0xffff0, (binary 11111111 11111111 11100000), the TLC request service
permissions allow

-- subordinate certificates to sign SREM messages with the following data item:
-- 0x80 (byte 1, bit 0) "Signal request"
-- 0x40 (byte 1, bit 1) "Requestor role (public transport)"
-- 0x20 (byte 1, bit 2) "Requestor role (special transport)"
-- 0x10 (byte 1, bit 3) "Requestor role (dangerousGoods)"
-- 0x08 (byte 1, bit 4) "Requestor role (roadWork)"
-- 0x04 (byte 1, bit 5) "Requestor role (roadRescue)"
-- 0x02 (byte 1, bit 6) "Requestor role (emergency)"
-- 0x01 (byte 1, bit 7) "Requestor role (safetyCar)"
-- 0x80 (byte 2, bit 0) "Requestor role (truck)"
-- 0x40 (byte 2, bit 1) "Requestor role (motorcycle)"
-- 0x20 (byte 2, bit 2) "Requestor role (police)"
-- 0x10 (byte 2, bit 3) "Requestor role (fire)"
-- 0x08 (byte 2, bit 4) "Requestor role (ambulance)"
-- 0x04 (byte 2, bit 5) "Requestor role (Department of Transport)"
-- 0x02 (byte 2, bit 6) "Requestor role (official transit)"
-- 0x01 (byte 2, bit 7) "Requestor role (slowMoving)"
-- 0x80 (byte 3, bit 0) "Requestor role (cyclist)"
-- 0x40 (byte 3, bit 1) "Requestor role (pedestrian)"
-- 0x20 (byte 3, bit 2) "Requestor role (military)"
-- 0x10 (byte 3, bit 3) not used, set to 0
-- 0x08 (byte 3, bit 4) not used, set to 0
-- 0x04 (byte 3, bit 5) not used, set to 0
-- 0x02 (byte 3, bit 6) not used, set to 0
-- 0x01 (byte 3, bit 7) not used, set to 0

```

```

"sspBitmask": "FF00001F"    -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

    -- or not to deliver the permission to subordinate entities

    }}
  },
  {
    "psid": 141,              -- 0x8d, IEEE registered GeoNetworking Management Communication
  },
  {
    "psid": 623,              -- 0x026F, IEEE registered Secured Certificate Request Service
    "sspRange": {"bitmapSspRange": {
      "sspValue": "01C0",    -- byte 0, 0x01, SSP version control
                              -- byte 1, 0xc0 (binary 00111110), the Secured Certificate Request service permissions allow
                              -- subordinate entities to sign the following request and response messages:
                                -- 0x01 (bit 7)  not used,
                                -- 0x02 (bit 6)  to issue certificate able to sign CA Certificate Request messages
                                -- 0x04 (bit 5)  to issue certificate able to sign Enrolment Response messages
                                -- 0x08 (bit 4)  to issue certificate able to sign Authorization Validation Response
messages,
                                -- 0x10 (bit 3)  to issue certificate able to sign Authorization Response messages,
                                -- 0x20 (bit 2)  to issue certificate able to sign Authorization Validation Request
messages,
                                -- 0x40 (bit 1)  to issue certificate able to sign Authorization Request messages,
                                -- 0x80 (bit 0)  to issue certificate able to sign Enrolment Request messages,
    "sspBitmask": "FF3F"    -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

    -- or not to deliver the permission to subordinate entities

    }}
  },
  {
    "psid": 637,              -- 0x27d, IEEE registered TLC (Traffic Light Controller Status Service) Service
    "sspRange": {"bitmapSspRange": {
      "sspValue": "01",      -- byte 0, 0x01, SSP version control
      "sspBitmask": "FF"    -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver

    -- or not to deliver the permission to subordinate entities

    }}
  },
  },
}],
"minChainLength": 2,        -- minChainLength is the length of the certificate chain, i.e. the number of certificates "below"
                              -- this certificate in the chain, down to and including the end-entity certificate
                              -- (IEEE 1609.2a-2017 section 5.1.2.1)

"chainLengthRange": 0,
"eeType": "C0"              -- (app, enroll)
}},
"certIssuePermissions": [{

```

```

"subjectPermissions": {"explicit": [
  {
    "ITS-AID": 623, -- 0x026f, IEEE registered Secured Certificate Request Service with default value for
minChainLength = 1 and chainLengthRange = 0 and eeType = App
    "sspRange": {"bitmapSspRange": {
      "sspValue": "013E", -- byte 0, 0x01, SSP version control
-- byte 1, 0x3e (binary 11000000), the Secured Certificate Request service permissions allow
-- subordinate entities to sign the following request and response messages:
-- 0x01 (bit 7) not used,
-- 0x02 (bit 6) to issue certificate able to sign CA Certificate Request messages
-- 0x04 (bit 5) to issue certificate able to sign Enrolment Response messages
messages,
-- 0x08 (bit 4) to issue certificate able to sign Authorization Validation Response
messages,
-- 0x10 (bit 3) to issue certificate able to sign Authorization Response messages,
-- 0x20 (bit 2) to issue certificate able to sign Authorization Validation Request
messages,
-- 0x40 (bit 1) to issue certificate able to sign Authorization Request messages,
-- 0x80 (bit 0) to issue certificate able to sign Enrolment Request messages,

"sspBitmask": "FFC1" -- the Certificate Policy Authority delegates the right to the RCA, and it's the RCA responsibility
to deliver
-- or not to deliver the permission to subordinate entities

    }}
  }
}],
}],
"verifyKeyIndicator": {"verificationKey": {"ecdsaBrainpoolP256r1": {
  "compressed-y-0": "272833C1980A51AAB624D1C032E82CB220E8B7A2814AC18C8F0E837ECB4EB112"}}
},
"signature": {"ecdsaBrainpoolP256r1Signature": {
  "rSig": {"x-only": "300E0A34A7C19015E5E1A30DA8EC2CB33C8D318D9A58BEC8FFC63ED71456CFD6"},
  "sSig": "8ACBF7809990D3AA34BC72747F2DE7EF2BD2B66DDE32F54BD1F04DFF38BD1345"
}}
}

```

I.3.2. RCA certificate name / CertificateID

According to the CP it is clearly the CPA who assigns the actual names, following the proposal of RCAs. Hence, this chapter mandates a mandatory naming scheme for such proposals, based on several considerations that are summarised in chapter I.3.2.1.

I.3.2.1. Considerations and requirements on the “CertificateID” within the RCA Certificate and RCA Link Certificates

Looking at the requirements and different implementations of RCAs so far in Europe (used e.g. at the two ETSI plugtests in 2019) it seems that there were distinct purposes/goals that had to be combined in only one available field in the RCA Certificate Format (“CertificateID”):

1. Creating and keeping a “unique name/identifier” for each RCA that participates/enrols in the ECTL and hence in the EU CCMS. Each of such RCA (that has to have a “unique name/identifier”) will have to create RCA Certificates.
2. RCAs issue RCA Certificates and can (if they decide to) re-key them with the help of RCA Link Certificates. These RCA Link Certificate shall also include the “names” that have to be chosen/assigned and shall be able to be updated in different use cases – hence there is a need to explicitly define how this shall function in the EU CCMS. It was identified that the 2019 set of ETSI standards did not fully support implementation of Link Certificates yet, which are hence being replaced by the concept of “Link Certificate Messages” in this document.

The following fictitious Examples of RCAs participating in the EU CCMS are introduced for the purpose of illustrating examples in this document: Six example Root CAs are used, for which a mandatory naming scheme is introduced in this paper (see chapter I.3.2.2):

- Root CA #1: EU-Root-CA
- Root CA #2: OEM1-Root-CA
- Root CA #3: OEM2-Root-CA
- Root CA #4: RoadOperator1-Root-CA
- Root CA #5: City1-Root-CA
- Root CA #6: MemberState1-Root-CA

Requirements to the unique name/identifier:

- All of these actors running those Root CAs seem to only exist once in the EU. Each of them will have an authorised representative and all of them have to enrol with their application form at the CPA. But what if OEM2 e.g. actually wants to run 3 different Root CAs for different vehicle models? Or MemberState1 actually has 16 different governmental Root CAs for each region? Each of them **will need a unique “name” to be identified**, since they would all have to apply separately to the CPA since they will be stand-alone RCAs listed on the ECTL.
- Such “RCA names” in EU implementations so far seem to have a “human-readable” and directly interpretable notion. While there are different pro’s and con’s regarding human-readable RCA Names in the actual certificate (i.e. it could in principle also only be a numerical identifier), the chosen way forward shall be to use human-readable RCA Names directly in the Certificate. This is mainly to ease operations when Certificates are handled in a manual way in different steps of EU CCMS enrolment and operation.
- Such human-readable “RCA names” are subject to change over time, since it is expected that the name is very close to company or country names/authority names. These are not expected to be constant variables, since companies can change names (one buys the other etc.) and also Member States may have different needs (ministries/regions/road operators etc. being involved). To accommodate this, the CertificateID shall be flexible to be changed if necessary, while at the same time the naming convention shall provide stability on the level of the CPA and CPOC to always be able to clearly identify “who is who”.
- In general, the field CertificateID is the only field that can be used at the moment inside the standardised RCA certificate format for naming purposes.
- Each CertificateID in the operational EU CCMS shall be unique, hence the CPA shall have a role in validating certain components of the CertificateID according to the mandatory naming scheme of the CPA.
- Each newly enrolled RCA shall have a unique CertificateID. In some re-keying purposes of RCA certificates the same CertificateID may in principle be re-used. However, the re-use of CertificateID is bound to certain rules, depending whether Root CA Link Certificates are used or not for re-keying:

- Case 1: The RCA re-keys its RCA Certificate, but does not make use of RCA Link Certificate Messages. Rekeying of Root CA certificates shall in any case be done before the private key usage period ends. When the validity period of the first RCA Certificate is about to expire and if the RCA wishes to continue operations within the EU CCMS, it has to apply for a new enrolment (i.e. also new “name” and consequently a new CertificateID) in an appropriate timing at the CPA. It will be treated by the CPOC like a new enrolment, which means a new application form has to be created and validated by the CPA. The CertificateID will be new, because the RCA is treated as a new Enrolment since no Link Certificate messages are used. A new application form means that the RCA certificate shall not be mixed up with the previously enrolled RCA at the level of the CPOC (since a fully new RCA certificate is placed on the ECTL that the CPOC needs to keep track of).
- Case 2: The RCA re-keys its RCA Certificates with the help of RCA Link Certificate Messages, where two sub-cases arise:
 - Case 2a: Simple case of expiry of the validity period of the RCA certificate: RCA does a “normal” re-key simply due to expiry of the old RCA certificate. No changes in the “ToBeSignedCertificate” (except validity), that means that also NO CHANGE to CertificateID shall be done.
 - **Case 2b: ANY changes in the RCA certificate ‘ToBeSignedCertificate’:** requires approval of CPA first. If granted, the CertificateID could (like all other fields) also be changed.

I.3.2.2. The mandatory naming/CertificateID format

Considering the above points and requirements, a mandatory naming scheme for CertificateID within the RCA Certificates is introduced. It includes both a mandatory <CPA assigned mandatory> component and an optional <RCA-ENVIRONMENT> component that are combined with a separator (“_”) in order to accommodate all use cases. The <CPA assigned mandatory> component shall further consist of a <CPA-ID> component and a <RCA-NAME> component:

The CertificateID in RCA Certificates shall consist of two components: <CPA assigned mandatory>_<RCA-ENVIRONMENT>, whereas only the <CPA assigned mandatory> is mandatory to be filled and <RCA-ENVIRONMENT> is an optional component.

The <CPA assigned mandatory> component shall further consist of <CPA-ID>_<RCA-NAME>.

Detailed specification of the components of CertificateID:

- The <CPA assigned mandatory> component shall be validated by the CPA and shall never be allowed to be changed, unless the CPA allows to do so in the process of a full new enrolment of the RCA (see Case 1 in chapter I.3.2.1) or “a re-keying with changes and with RCA Link Certificates” use case (see case 2b in chapter I.3.2.1).
- <CPA-ID>: shall be a numerical sequence in the format 1, 2, 3, 4, 5, 6, 7 ... (decimal) following the order of application forms received by the CPA from all RCAs participating to the EU CCMS (i.e. for each approved application form the CPA assigns a new next free unused <CPA-ID>, whereas no specific order is applied at all). The value 0 is a reserved value (e.g. to be used for LO RCA Certificates, compare with <RCA-ENVIRONMENT> below).. The assignment of the <CPA-ID> needs to happen in advance and in coordination with the CPA, prior to the formal application to the CPA and consequent later enrolment (after the application form approval by the CPA) of the created Root CA Certificate at the CPOC in Ispra.
- <RCA-NAME>: shall be a chosen name by the Root CA that can be proposed by the authorised representative of the RCA to the CPA. The <RCA-NAME> should aim to best describe its origin and governance, limited by the maximum size of the CertificateID field (32 byte according to CP) minus <CPA-ID> and <RCA-ENVIRONMENT>. Any ASCII characters may be used except “_” (underscore, ASCII code 95 (decimal) / 0x5f (hex))

- **<RCA-ENVIRONMENT>**: is an optional component. If the optional component **<RCA-ENVIRONMENT>** is not set, the RCA certificate shall be considered a fully CP compliant certificate. The optional field **<RCA-ENVIRONMENT>** can be set as one of the following entries:
 - L0 (Level 0: indicates RCAs and C-ITS stations which are not compliant to the CP, e.g. for testing purposes)
 - L1 (Level 1: indicates RCAs and C-ITS stations which are not fully compliant to the CP, but are compliant to the requirements set by the CPA, e.g. for the ramp-up phase of C-ITS)
 - Any other specific indicators for environments to reflect specific maturity of C-ITS service operations in the EU CCMS agreed on by the CPA on a case by case basis (e.g. L2 or other if needed).

Note: Since many actors manually handle RCA certificates the **<RCA ENVIRONMENT>** component serves as an additional indicator to avoid any mix-up of RCA Certificates and their intended operating environment, especially in the ramp-up phase of C-ITS services in the EU. The CPOC shall in principle only consider fully CP compliant environment RCA Certificates for insertion into the ECTL, unless the CPA instructs the CPOC differently according to the given indicators and defined levels.

- Examples of different possible **CertificateID** according to the mandatory naming scheme and example Root CAs introduced in chapter I.3.2.1. (Note: the examples do not intend to exclude any other type of stakeholder beyond the ones listed) :
 - 1_EU-Root-CA
 - 2_OEM1-Root-CA_L0
 - 3_OEM2-Root-CA_L1
 - 4_RoadOperator1-Root-CA_L0
 - 5_City1-Root-CA_L0
 - 6_MemberState1-Root-CA

I.3.2.3. Consequences on re-use of CertificateID in re-keying scenarios

Following the mandatory naming scheme, the following shall happen to **CertificateID** (and their components) in RCA certificates in the different use cases of re-keying RCA certificates introduced in chapter I.3.2.1:

Case 1: The RCA re-keys its RCA Certificate, but does not make use of RCA Link Certificate Messages: The **CertificateID** shall not be re-used in the new re-keyed RCA Certificate. A new **CertificateID** shall be assigned, where the **<CPA assigned mandatory>** component is newly assigned by the CPA and the **<RCA ENVIRONMENT>** component is (again, like the first time) chosen by the RCA. This process requires approval of the CPA via the initial application form process (like initial enrolment of a new RCA). In principle, the **<RCA-NAME>** may also change within this process, since it is a fully new enrolment.

- Example 1, the **<CPA-ID>** changes since it is a new enrolment of the RCA Certificate. The **<RCA-NAME>** and **<RCA-ENVIRONMENT>** fields could stay the same, if no change is needed:
 - CertificateID of 1st RCA Certificate (old RCA Certificate):
 - 2_OEM1-Root-CA_L0
 - CertificateID of 2nd RCA Certificate (newly enrolled RCA Certificate, the next available **<CPA-ID>** is assigned):
 - 7_OEM1-Root-CA_L0
- Example 2, the **<CPA-ID>** changes since it is a new enrolment of the RCA Certificate. The **<RCA-NAME>** and the **<RCA-ENVIRONMENT>** field may also be changed if required:

- CertificateID of 1st RCA Certificate ("old"):
 - 4_RoadOperator1-Root-CA_L0
- CertificateID of 2nd RCA Certificate ("newly enrolled"):
 - 8_RoadOperator1-~~NewName~~-Root-CA_L1

Case 2a: The RCA re-keys its RCA Certificates with the help of RCA Link Certificate Messages – but no attributes in the `ToBeSignedCertificate` are changed. The identical `CertificateID` shall be re-used (no changes allowed). This does not require CPA approval:

- Example 1:
 - CertificateID of 1st RCA Certificate (old RCA Certificate):
 - 2_OEM1-Root-CA_L0
 - CertificateID of 2nd RCA Certificate (re-keyed new RCA Certificate):
 - 2_OEM1-Root-CA_L0
- Example 2:
 - CertificateID of 1st RCA Certificate (old RCA Certificate):
 - 4_RoadOperator1-Root-CA_L0
 - CertificateID of 2nd RCA Certificate (re-keyed new RCA Certificate):
 - 4_RoadOperator1-Root-CA_L0

Case 2b: Re-key with ANY changes in the RCA certificate '`ToBeSignedCertificate`' (such as permissions, `CertificateID`, region, etc.): requires approval of CPA first. If granted, the `CertificateID` could also be changed in both the `<CPA assigned mandatory>` and `<RCA-ENVIRONMENT>` components, if needed. However, within the `<CPA assigned mandatory>` component the `<CPA-ID>` needs to stay the same and only the `<RCA-NAME>` is allowed to be changed (since no new application form was sent, this is only a new re-keyed Certificate for the very same enrolled RCA).

- Example 1: OEM1 changes its `<RCA-NAME>` from "OEM1-Root-CA" to "OEM-NewName" and its `<RCA-ENVIRONMENT>` field from "L0" to "no environment set", hence removing the optional `<RCA-ENVIRONMENT>` component.
 - CertificateID of 1st RCA Certificate ("old"):
 - 2_OEM1-Root-CA_L0
 - CertificateID of 2nd RCA Certificate ("re-keyed new"):
 - 2_OEM1-~~NewName~~-Root-CA
- Example 2: RoadOperator1 changes its `<RCA-NAME>` from "RoadOperator1-Root-CA" to "RoadOperator1-NewName". No changes of the `<RCA-ENVIRONMENT>` field.
 - CertificateID of 1st RCA Certificate ("old"):
 - 4_RoadOperator1-Root-CA_L0
 - CertificateID of 2nd RCA Certificate ("re-keyed new"):
 - 4_RoadOperator1-~~NewName~~-Root-CA_L0

I.3.2.4. Note regarding EA and AA naming and URLs

Root CAs shall ensure that EA and AA CertificateIDs follow a defined structure, allowing proper identification of the issuing Root CA.

A recommendation is described here: components from the mandatory RCA CertificateID naming structure (i.e. components from the CertificateID of the RCA described in the chapter I.3.2.2) should be re-used:

- The <CPA-ID> of the Root where the EA/AA is enrolled should be inserted at the beginning of the EA/AA CertificateID.
- Instead of the component <RCA-NAME> a chosen <EA-NAME> and <AA-NAME> of the EA or AA is inserted, with the same rules/restrictions concerning the underscore symbol “_” as separator. Further, just like for the RCA CertificateID an optional <EA-ENVIRONMENT> or <AA-ENVIRONMENT> can be added at the end of the EA/AA CertificateID.

Hence, the structure for the EA and AA CertificateID is:

- **For the EA CertificateID:** <CPA-ID>_<EA-NAME>_<EA-ENVIRONMENT>:
- **For the AA CertificateID:** <CPA-ID>_<AA-NAME>_<AA-ENVIRONMENT>:

Examples of EA and AA certificateIDs (based on the RCA CertificateID examples listed in chapter I.3.2.2):

- 1_EU-AA
- 2_OEM1-AA1_L0
- 3_OEM2-EA-xyz_L0
- 4_RoadOperator1-EA_L0
- 5_City1-AA_L0
- 6_MemberState1-AA

By derivation, URLs for EAs and AAs may have the following structure: http://CertificateID.domain, with “.” replacing “_”.

Examples:

- http://1.EU-AA.eu-rca.eu
- http://2.OEM1-AA1.L0.oem1.com
- http://3.OEM2-EA-xyz.L0.oem2-rca.fr
- http://4.RoadOperator1-EA.L0.xx.de
- http://5.City1-AA.L0.city.nl
- http://6.MemberState1-AA.MSDomain.it

I.3.3. Validity period of Certificates in the EU CCMS

The Certificate Policy mandates that a RCA certificate has a maximum private key usage equal to the validity period with a maximum validity time of 5 years (Certificate Policy, section 7.2, Table 8).

The maximum private key usage period and maximum validity time for all root CAs in the EU CCMS shall be 5 years, whereas the private key usage period shall always be equal to the chosen validity time. The value of 5 years for the RCA certificate is only the possible maximum value and thus indicates the maximum validity time of all certificates in the EU CCMS (except the TLM certificate). That means any RCA operator can choose a value equal or lower than 5 years for its RCA certificate validity. The certificates issued by the RCA and sub CAs shall not exceed a validity period of 5 years. It must be ensured that the certificates are re-keyed in good time before expiration.

Note: It is recommended that EA and AA certificates should be re-keyed within the maximum validity period chosen for the RCA Certificate by the RCA. The EA and AA certificate validity period shall not exceed the validity

period of the issuing RCA certificate. Hence, the maximum validity time of those certificates shall be equal or lower than 5 years. It is recommended to re-key RCA, EA and AA certificates with an overlap period of at least 3 months before the validity of the RCA, EA and AA certificates expire.

The ASN.1 has a single attribute to define the validity period of the RCA, limited to 65 535 (Uint16).

The validity period duration has several granularities. For instance:

- as years: 1 year equals to 31 556 952 seconds (cf. IEEE 1609.2)
- as sixtyhours: 1 “sixtyhour” equals to 216 000 seconds
- as hours: 1 hour equals to 3 600 seconds

Examples:

- With a RCA certificate issuance date time is 2010-01-01T00:00:00 and with a validityPeriod of 5 years, the certificate end date time shall be 2014-12-31T22:33:33.
Note: the end date is not 2015-01-01T00:00:00 because the duration of 1 year is fixed and especially does not depend on leap years or seconds.
- To end exactly at 2015-01-01T00:00:00 with a validity period of 438 sixtyhours, RCA certificate issuance date time shall be 2012-01-02T00:00:02.

A proper management of validity dates and durations requires an implementation using a library with an advanced date time arithmetics, such as Gregorian Calendar, time zone, daylight saving time.

In particular, this will ensure a deterministic calculation of start and end dates.

I.3.4. Omitted attributes

The following attributes shall not be present in the RCA certificate:

- encryptionKey,
 - The Certificate Policy doesn't specify encryption key for RCA certificate (section 6.1.4.2),

The following attributes shall not be present in the RCA certificate:

- certRequestPermissions, (from ASN.1 – EtsiTs103097Module)
- canRequestRollover, (from ASN.1 – EtsiTs103097Module).

I.3.5. ECC key format for an optimal over-the-air bandwidth

The verificationKey may have different formats: x-only, compressed-y-0, compressed-y-1, uncompressed.

The uncompressed format requires both the x and y values, and hence requires more octets to represent the verificationKey.

This best practice proposes to avoid using the uncompressed format in order to reduce the RCA certificate size as much as possible. This will reduce the bandwidth consumption (and hence the operation cost) when a C-ITS station downloads the ECTL over-the-air.

I.3.6. Unlimited permission and “least privilege” principle

certIssuePermissions is an attribute specifying if the RCA certificate has the permission to grant AppPermissions or CertIssuePermissions to the subordinate entity.

According to the ASN.1, one can in theory specify the permissions of a service in two ways:

- Unlimited service and unlimited permission as:
 - "certIssuePermissions": [{"subjectPermissions": {"all": null}}], this is also called “wildcards”. However, such wildcards are not allowed to be used in the EU CCMS by any RCA.
- An individual permission by turning the bit position of the permission to 1 as “allowed”, and to 0 as “disallowed”.

The permission setting is somewhat similar to firewall setting rules for controlling inbound and outbound traffic. When setting the firewall rule, one uses to apply the “least privilege” security principle by closing all routes of the firewall and by only setting the strict minimum rules for the firewall operation.

For permission of services, this best practice proposes to apply the “least privilege” principle by avoiding the use of “unlimited permission” in the certIssuePermissions and/or appPermissions attributes, and by specifying individual permission of each service. Unmanaged permission of a service shall be set as disallowed (i.e. turning the bit position in the “sspValue” to 0 and the bit position in the SSP bitmask to 1). Additionally, only a “0” in Bitmask is allowed, if the corresponding SSP value contains a “1” at the same index.

I.3.7. appPermissions with predefined values

According to the ETSI TS 102 941 [2], its sections B.2 and B.3 define two mandatory services in appPermissions content:

- appPermissions:
 - psid = 624, IEEE registered Certificate Trust List Service, (ETSI TS 102 941 [2] section B.2),
 - ssp is a bitmapSsp with “0138” as value (i.e. byte 1 is the SSP version control, byte 2 means that the RCA certificate is able to sign CTL with EA, AA and DC entries),
 - psid = 622, IEEE registered Certificate Revocation List Service, (ETSI TS 102 941 [2] section B.3),
 - ssp is a bitmapSsp with “01” as value (i.e. byte 1 is the SSP version control),

Each RCA certificate shall have this two ITS-AIDs in the appPermissions attribute.

I.3.8. certIssuePermissions with predefined values

According to the ETSI TS 102 941 [2], its sections B.4 and B.5 define the following mandatory service in certIssuePermissions content. Each RCA certificate shall have at least this following ITS-AID in the certIssuePermissions attribute.

- certIssuePermissions for permissions end in EA and AA certificates:
 - psid = 623, the IEEE registered Secured Certificate Request Service.
 - The declaration of this psid means that the RCA certificate authorizes subordinate certificates to include the Secured Certificate Request Service.
 - “sspValue” is “013E”
 - byte 1 (“01”) is the SSP version control,
 - byte 2 (“3E”) means that the RCA certificate covers a set of permissions in the Secured Certificate Request Service, each permission is materialized by a bit position in the “sspValue”. Permissions are:
 - the permission to issue subordinate certificate able sign Authorization validation request message,

- the permission to issue subordinate certificate able sign Authorization response message,
 - the permission to issue subordinate certificate able sign Authorization validation response message,
 - the permission to issue subordinate certificate able sign Enrolment response message,
 - the permission to issue subordinate certificate able sign CA certificate request message.
- “sspBitmask” is “FFC1”
- byte 1 (“FF”) is the bitmask for SSP version control byte,
- byte 2 (“C1”, all bit positions set to 0, except bit position 7 which is not used) means that the Certificate Policy Authority delegates the right to the RCA. In this case the RCA is the one which decides about the encoded permissions in the subordinate certificates.
- “eeType” not encoded because default value “app” used
- minChainLength not encoded because default value 1 used
- certIssuePermissions for permissions end in EC and AT certificates:
 - psid = 623, the IEEE registered Secured Certificate Request Service.
 - The declaration of this psid means that the RCA certificate authorizes subordinate certificates to include the Secured Certificate Request Service.
 - “sspValue” is “01C0”
 - byte 1 (“01”) is the SSP version control,
 - byte 2 (“C0”) means that the RCA certificate covers a set of permissions in the Secured Certificate Request Service, each permission is materialized by a bit position in the “sspValue”. Permissions are:
 - the permission for ITS-S to sign Enrolment request message,
 - the permission for ITS-S to sign Authorization request message,
 - “sspBitmask” is “FF3F”
 - byte 1 (“FF”) is the bitmask for SSP version control byte,
 - byte 2 (“3F”, all bit positions set to 0, except bit position 7 which is not used) means that the Certificate Policy Authority delegates the right to the RCA, and it’s the RCA responsibility to deliver or not to deliver the permissions to subordinate entities. The RCA is the one which decides about the encoded permissions in the subordinate certificates.
 - psid = 36, 37, 137, 138, 139, 140, 141 with related sspValue and sspBitmask
 - “eeType” is “CO” (app, enroll)
 - eeType indicates the type of certificates that this instance of PsidGroupPermissions in the certificate is entitled to authorize.
If this field indicates app, the chain is allowed to end in a certificate in which these permissions appear in an appPermissions field (in other words, if the field does not indicate app but the chain ends in an appPermissions field, the chain shall be considered invalid).
If this field indicates enroll, the chain is allowed to end in a certificate in which these permissions appear in a certReqPermissions or certIssuePermissions permissions field (in other words, if the field does not indicate app but the chain ends in an appPermissions field, the chain shall be considered invalid). As the sspValue and sspBitmask in the PsidGroupPermissions concern both the enrolment (i.e. EA), and authorization subordinate (i.e. AA), eeType is (app, enroll).
 - Note: Release 2 of ETSI 102 941 [2] clarifies the use of “enroll”.
 - minChainLength = 2
 - minChainLength is the length of the certificate chain, i.e. the number of certificates “below” this RCA certificate in the chain, down to and including the end-entity certificate (IEEE 1609.2a-2017 section 5.1.2.1). In the European V2X, below the RCA, there are EA and EC in one certificate hierarchy branch, and there are AA and AT in another certificate hierarchy branch.
 - chainLengthRange not encoded because default value 0 used

NOTE: With the permission (i.e. “sspValue”) in the Secured Certificate Request Service of the RCA certificate, an EA may then request the RCA to sign an EA certificate with the following app permissions in the Secured Certificate Request Service:

- the permission to sign CA certificate request message,
- the permission to sign Authorization validation response message,
- the permission to sign Enrolment response message.

An EA may then request the RCA to sign an EA certificate with the following cert issue permissions in the Secured Certificate Request Service:

- the permission to issue EC certificates able to sign Enrolment request message,
- the permission to issue EC certificates able to sign Authorization request message.

With the permission (i.e. “sspValue”) in the Secured Certificate Request Service of the RCA certificate, an AA may then request the RCA to sign an AA certificate with the following app permissions in the Secured Certificate Request Service:

- the permission to sign CA certificate request message,
- the permission to sign Authorization validation request message,
- the permission to sign Authorization response message.

The RCA will not grant any permission to the EA and AA if those permissions are not set in the certIssuePermissions in the RCA certificate (IEEE 1606.2a-2017, sections 6.4.34 and 6.4.34a).

I.3.9. Region

According to TS 103 097 [3] an `EtsiTs103097Certificate` shall be of type `ToBeSignedCertificate` and may include the component `region` of type `GeographicRegion` as defined in IEEE Std 1609.2

RCA certificates to be inserted into the ECTL shall comply with the following additional constraints:

- The component `toBeSignedCertificate.region` shall be absent if and only if the RCA certificate is to be considered globally valid.
- If the RCA certificate is not intended to be globally valid:
 - the component `toBeSignedCertificate.region` shall be present and constraint to the choice `identifiedRegion`.
 - The sequence of `IdentifiedRegion` contained in `identifiedRegion` shall be of length at least 1.
 - Each instance of `IdentifiedRegion` shall be of type `countryOnly`.
 - The RCA certificate shall be considered valid in the indicated country / countries.

The country code in `identifiedRegion` shall be assigned according to the M49 code listed in:

- United Nations Statistics Division, “Composition of Macro Geographical (Continental) Regions, Geographical Sub-Regions, and Selected Economic and Other Groupings,” revision of 31 Oct. 2013. Available from <http://unstats.un.org/unsd/methods/m49/m49regin.htm>
- For the European Union “27 countries as of 31 January 2020” the value 65535 shall be used instead of listing the individual countries.

Note: the geographic validity of the RCA certificate affects the:

- Consistency of permissions within a certificate chain as specified in clause 5.1.2.4 in IEEE 1609.2. This specifically constraints the geographic validity of the subordinate EA/AA and EC/AT certificates.
- Consistency between signed SPDU and signing certificate as specified in clause 5.2.3.2.2 in IEEE 1609.2. This specifically constraints the location generation of the SPDU (obtained from the security headers or from the payload) to be within the geographic region indicated in the signing certificate.

I.4. Supported Permissions in RCA and TLM Certificates

I.4.1. Minimum Set of Permissions:

NOTE: In general it is up to the RCA to define its permission, in line with the CP and CPA approval. However, the CPA shall also define a minimum set of permission that is absolutely mandatory to be inserted in every RCA certificate, and will hence be checked by the CPOC ENTRY. At this moment, the CPOC ENTRY shall hence check if the following set of permissions is available in all RCA certificates:

- App Permissions for CTL and CRL shall be set to 1 (hence being active)
- Certificate permissions for at least one ITS-AID according to ETSI TS 102 965 [5] shall be set to 1 (hence being active)

I.4.2. Maximum Set of Permissions:

The RCA certificate shall contain the following permissions specified in Table 4 or a subset of these permissions.

If an ITS-AID is given in the root certificate the full SSP element shall be given according to Table 5. The sppValue (binary) in Table 5 shows the maximum SSP values that are allowed according to the related standards. The root certificate may contain SSP entries with less SSP bits set to 1. The root certificate shall not contain a SSP set to 1 if this is not defined in the standards or the RCA is not allowed to have the right and therefore set to 0 in Table 5.

Table 4: ITS-AID values allowed in the EU CCMS based on ETSI/ISO according to ETSI TS 102 965 [5]

ITS application name	ITS-AID Value (decimal)	ITS-AID Value (hex)	Standard Number	Supported Versions*
CA Basic service	36	24	ETSI TS 103 900 ETSI EN 302 637-2	V2.1.1 (2023-11) V1.4.1 (2019-04)
DEN Basic service	37	25	ETSI TS 103 831 ETSI EN 302 637-3	V2.2.1 (2024-04) V1.3.1 (2019-04)
TLM service	137	89	ETSI TS 103 301	V2.1.1 (2021-03) V1.3.1 (2020-02)
RLT service	138	8a	ETSI TS 103 301	V2.1.1 (2021-03) V1.3.1 (2020-02)
IVI service	139	8b	ETSI TS 103 301	V2.1.1 (2021-03) V1.3.1 (2020-02)
TLC Request Service	140	8c	ETSI TS 103 301	V2.1.1 (2021-03) V1.3.1 (2020-02)

GeoNetworking Management Communications (GN-MGMT)	141	8d	ETSI TS 103 836-4-1 ETSI EN 302 636-4-1	V2.1.1 (2022-11) V1.4.1 (2020-01)
CRL service	622	26e	ETSI TS 102 941	V2.2.1 (2022-11) V1.4.1 (2021-01)
Secured certificate request service	623	26f	ETSI TS 102 941	V2.2.1 (2022-11) V1.4.1 (2021-01)
CTL service	624	270	ETSI TS 102 941	V2.2.1 (2022-11) V1.4.1 (2021-01)
TLC Status Service	637	27d	ETSI TS 103 301	V2.1.1 (2021-03) V1.3.1 (2020-02)
CP Service	639	27f	ETSI TS 103 324	V2.1.1 (2023-06)
POI Service	1619	653	ETSI TS 103 916	V2.1.1 (2024-01)
* The list of supported ITS-AID versions for each standard will be maintained as new versions of the indicated standard are published and accepted by the CPA in the future. All supported versions listed in this table shall be interoperable.				

Any other ITS-AID shall not be used. In particular, test ITS-AID are not authorized in RCA certificates candidating to the ECTL.

Table 5: Specification of maximum permissions contained in a RCA certificate in the EU CCMS

App Permissions		sspValue (hex)	sspBitmask (hex)	sspValue (binary)	sspBitmask (binary)
624	CTL service	0138		0000 0001 0011 1000	
622	CRL service	01		0000 0001	
Explicit cert issue permissions with minimum chain length = 1 (default), chain length range = 0 (default) and end entity type = app (default)					
ITS-AID values		sspValue (hex)	sspBitmask (hex)	sspValue (binary)	sspBitmask (binary)

623	Secured certificate request service	013E	FFC1	0000 0001 0011 1110	1111 1111 1100 0001
Explicit cert issue permissions with minimum chain length = 2, chain length range = 0 (default) and end entity type = app, enrol					
ITS-AID values		sspValue (hex)	sspBitmask (hex)	sspValue (binary)	sspBitmask (binary)
36	CA Basic service	01FFFF	FF0000	0000 0001 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000
37	DEN Basic service Rel.1 DEN Basic service Rel.2	01FFFFFF 02FFFFFFFF	FF000000 FF00000000	0000 0001 1111 1111 1111 1111 1111 1111 0000 0010 1111 1111 1111 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000 0000 0000 1111 1111 0000 0000 0000 0000 0000 0000 0000 0000
137	TLM service	01E0	FF1F	0000 0001 1110 0000	1111 1111 0001 1111
138	RLT service	01C0	FF3F	0000 0001 1100 0000	1111 1111 0011 1111
139	IVI service	01xxxxyyFFFF	FF0000000000	0000 0001 xxxx xxxx xxyy yyyy yyyy yyyy 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

140	TLC Request Service	02FFFFE0	FF00001F	0000 0010 1111 1111 1111 1110 0000	1111 1111 0000 0000 0000 0000 0001 1111
141	GN-MGMT	<i>no value</i>	<i>no value</i>		
623	Secured certificate request service	01C0	FF3F	0000 0001 1100 0000	1111 1111 0011 1111
637	TLC Status Service	01	FF	0000 0001	1111 1111
639	CP Service	01	FF	0000 0001	1111 1111
1619	POI Service	01	FF	0000 0001	1111 1111

The value 'x' in above shall contain the country code according to ISO 14816 and the value 'y' the provider ID which is defined in ETSI TS 103 301 but currently not assigned to specific values. All 'x' and 'y' values may be set to 0 to allow supporting all possible country codes and provider IDs. For these three specific SSP bytes the related bitmask value might be set to 0.

I.5. Publications of the TLM/CPOC

I.5.1. Regular publication schedule of the ECTL by the TLM/CPOC

Following the Certificate Policy, Figure 5 gives an overview of the regular publications of ECTLs of the TLM/CPOC, where the following logic applies:

Regular re-keying of TLM Certificates:

- Due to the limits of maximum validity and private key usage period of TLM Certificates defined in the CP, the TLM is going to regularly re-key its TLM Certificate. Re-keying of TLM Certificates is performed 1-2 months before the private key usage expiry (Figure 5 displays the case of "2 months before").
- The start of validity of the re-keyed new TLM Certificate is equal to the end of the private key usage period of the previous old TLM Certificate (for regular re-keying – if re-key happens earlier, the start of validity changes according to the needs). This means that the TLM will at all times only have one TLM certificate valid and active at the same time, using it to sign ECTLs.
- The re-keyed TLM Certificates and the corresponding TLM Link Certificate messages (see chapter I.6) are available on the CPOC Website. In addition the re-keyed TLM Certificates are inserted in specific versions of the ECTL(s) after the re-keying until the new TLM Certificate becomes valid, i.e. its private key usage period starts (see blue ECTLs in Figure 5).

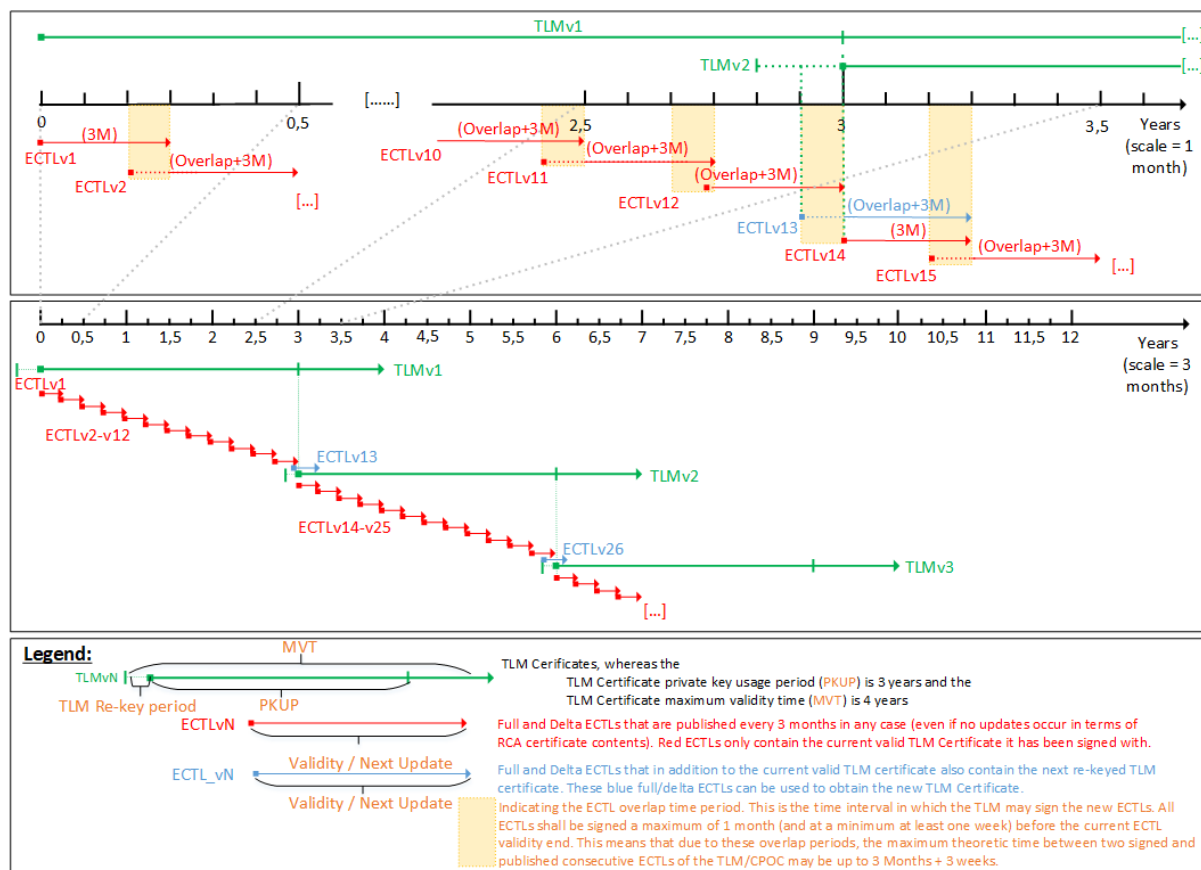
Regular publishing of ECTLs:

- The TLM signs (and hence the CPOC publishes) ECTLs about every 3 months on a regular basis. This regular publication happens in any case, no matter if actually updates of the RCA contents inside the ECTL happened or not. However, there may also be additional publications of ECTLs needed that are not foreseen in the regular schedule, e.g. in the case of revocation.
- ECTL Overlap periods:
 - All ECTLs are published with a validity (i.e. `nextUpdate` field in the ECTL) that overlaps with the previously published ECTL. The ECTL overlap period in the EU CCMS is defined as the following: All ECTLs shall be signed a maximum of 1 month, and at a minimum at least one week before the current ECTL validity end. (compare with Figure 5).

Note: Beyond the above described overlap period rule, which is according to the CP in-line with the 1-week rule of C-ITS stations having time to get any updated new ECTL on the C-ITS station, the following shall apply for regular operations: The TLM/CPOC shall under normal operating conditions not wait with the signing and publishing of new ECTLs until the described “minimum last week” of validity of the current ECTL has been reached. Instead, the TLM/CPOC shall publish the new ECTLs already around 3-4 weeks before the end of the validity period of the previous ECTL in order to allow more time in case any issue should occur.

- In order to facilitate the update of TLM Certificates in C-ITS stations via the ECTL, the TLM includes the new TLM certificate on specific versions of the ECTL following the same overlap principles (compare with blue ECTLs v13 or v26 in Figure 5).
 - ECTLs, which are signed with the initial or a new (re-keyed) TLM Certificate shall have a validity of 3 months to (re-)start the regular ECTL publication cycle and shall be published by the CPOC at the latest when the (new) TLM Certificate has become valid (compare with ECTLv14 in Figure 5).
 - All C-ITS stations shall update their ECTLs always based on the currently valid TLM Certificate, i.e. until the (re-keyed) new TLM certificate becomes valid. In any case, each C-ITS station has to have the newest published ECTL on board the station after a maximum of one week after its publication by the CPOC.
- To further clarify, the following details apply for the example ECTLs in Figure 5:
 - ECTL v1-v13 is signed by TLMv1, whereas
 - v1-v12 contain only TLMv1 and
 - v13 contains TLMv1 and TLMv2 (and all RCA certificates too, it is a normal full ECTL)
 - ECTL v14-v26 is signed by the TLM Certificate “TLMv2”, whereas
 - v14-v25 contain only TLMv2 and
 - v26 contains TLMv2 and TLMv3 (and all RCA certificates too, it is a normal full ECTL)

Figure 5: Example timetable of TLM regular re-keying and publishing of ECTLs in the EU CCMS



I.5.2. Machine-readable access of TLM Certificates, TLM Link Certificate Messages, ECTLs and delta ECTLs

In order to provide a machine-readable interface, the distribution of TLM certificates, TLM Link certificate messages, ECTLs and delta ECTLs shall be done via a defined web-endpoint distribution centre of the CPOC. The URL-scheme is based on the definitions for RCA-CTLs of ETSI TS 102 941 [2].

The definition of <HOST> shall be done once and shall ideally not change during the lifetime of the CPOC.

I.5.2.1. CPOC HOST URL Definition

<HOST> in the EU CCMS is defined as `http(s)://cpoc.jrc.ec.europa.eu`

<HOST> may be complemented by an optional <subpath>, for example "L0", "L1" or any other defined value in order to enable the CPOC to provide different sets of TLM Certificates and ECTLs in the EU CCMS. Some possible examples are listed here, the CPA shall instruct the TLM/CPOC with the exact needs for the EU CCMS:

- `http(s)://cpoc.jrc.ec.europa.eu/L0`
- `http(s)://cpoc.jrc.ec.europa.eu/L1`
- any other, based on the needs of the CPA, e.g. `https://cpoc.jrc.ec.europa.eu/xyz`

If the <subpath> is omitted, the CPOC shall either return:

- the TLM Certificate and ECTL used to sign ECTLs for RCA certificates where no specific RCA environment is set (Note: what is currently provided as such “default ECTL” in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly) or
- no file at all.

All end-points are available both as `https` and plain `http`, whereas the CPOC strongly advises to use the TLS `https` secured end-point.

I.5.2.2. Request of TLM certificate

```
GET http(s)://<HOST>/[<subpath>]/gettlmcertificate/[<HashedId8>]
```

- Parameters :
 - `<HOST>`: The fixed hostname as described in chapter I.5.2.1
 - `<subpath>`: Optional as described in chapter I.5.2.1
 - `<HashedId8>`: Optional: The HashedId8 of the requested TLM certificate. If omitted, the latest valid TLM certificate will be returned.
- Return value:
- Content-type: `application/octet-stream`
- Content: The requested TLM certificate, COER-encoded of type `EtsiTs103097Certificate`.

I.5.2.3. Request of TLM link certificate message

```
GET http(s)://<HOST>/[<subpath>]/gettlmlinkcertificate/[<HashedId8>]
```

- Parameters:
 - `<HOST>` : The fixed hostname as described in chapter I.5.2.1
 - `<subpath>`: Optional as described in chapter I.5.2.1
 - `<HashedId8>`: Optional: The HashedId8 of the TLM certificate to which the TLM link certificate message links to. If omitted, the link certificate message linking to the latest issued and valid TLM certificate (“current valid TLM Certificate”) will be returned.
- Return value:
- Content-type: `application/octet-stream`
- Content: The requested TLM link certificate message (as defined in [2]).

I.5.2.4. Request of full ECTL

```
GET http(s)://<HOST>/[<subpath>]/getectl/HashedId8
```

- Parameters:
 - `<HOST>`: The fixed hostname as described in chapter I.5.2.1
 - `<subpath>`: Optional as described in chapter I.5.2.1
 - `<HashedId8>`: The HashedId8 of the signing TLM certificate which will return the last ECTL signed by that TLM certificate.
- Return value:
- Content-type: `application/octet-stream`
- Content: The requested full ECTL, COER-encoded of type `TlmCertificateTrustListMessage`.

Note: even if the TLM has already re-keyed its TLM Certificate, the TLM continues to provide the last ECTL signed with the specific (old) TLM Certificate through the above GET command.

I.5.2.5. Request of delta ECTL

```
GET http(s)://<HOST>/[<subpath>]/getdeltaectl/<HashedId8>/[<EctlSequenceNumber>]
```

- o Parameters:
- o <HOST>: The fixed hostname as described in chapter I.5.2.1
- o <subpath>: Optional as described in chapter I.5.2.1
- o <HashedId8>: The HashedId8 of the signing TLM certificate.
- o <EctlSequenceNumber>: Optional: The sequence number of the requested delta ECTL. If omitted, the latest delta ECTL will be returned.
- o Return value:
- o Content-type: application/octet-stream
- o Content: The requested delta ECTL, COER-encoded of type `TlmCertificateTrustListMessage`.

The `EctlSequenceNumber` of range `[0 . . 255]` in (delta) ECTLs is reset to 0 with every new signing TLM certificate (i.e. with each TLM re-key and the first signing of a new ECTL making use of the new re-keyed TLM certificate). This is done in order to reduce the chance of overruns of `EctlSequenceNumber` during the lifetime of each used TLM certificate. In case the TLM has to sign more than 255 (delta) ECTLs during the validity period of a TLM certificate, the TLM shall re-key its TLM certificate before it reaches 255.

Note on delta ECTLs: In the initial phase of the EU CCMS deployment in Europe, delta ECTLs are not yet considered to be a fully mandatory requirement for publication by the CPOC. This is due to the fact that some open issues on delta ECTLs exist (such as the full availability of standards on exchange protocols of delta ECTLs, the confirmed availability and commitment of European C-ITS station operators to actually broadcast such delta ECTLs, agreements how to manage the size constraints of delta ECTLs, etc.).

However, this Annex I already defines all necessary interfaces and processes to be ready to make use of delta ECTLs, for those that intend to use them in the future. The publishing of delta ECTLs by the CPOC is hence considered of test nature at this moment in time, until the CPA instructs the CPOC otherwise, taking the solutions of the above mentioned points into account.

I.5.3. Delivery of Root CA Distribution Centre URLs via the CPOC

The distribution centres (DC) URL of the Root Certificate Authorities (RCA)s are needed to distribute the Certificate Trust Lists (CTL) and the Certificate Revocation List (CRL) (see ETSI TS 102 941 [2]).

It is mandatory that the entity setting up and managing the RCA will make this information public via a distribution centre URL.

This requires that the delivery of the URL to the CPOC becomes part of the RCA enrolment process (CPOC Protocol). An update of the URL means either a new enrolment of the RCA certificate or a re-key procedure with RCA link certificate messages at the CPOC.

The TLM shall include one `DcEntry` for each RCA Certificate on the ECTL. Each of these entries shall include the `HashedId8` of the concerned RCA certificate as well as the corresponding RCA DC URL which was delivered by the RCA to the CPOC at its enrolment or re-key. If two RCA Certificates use the same DC URL, the ECTL shall include only one `DcEntry` entry with the URL and the 2 corresponding `HashedId8` of the RCA Certificates.

At least the following requests shall be accessible at the URLs of the CPOC and RCAs distribution centres:

CPOC requests:

- `cpoc.jrc.ec.europa.eu/gettlmcertificate`
 - o **plus optional** `<subpath>` **and** `<HashedId8>`
- `cpoc.jrc.ec.europa.eu/gettlmlinkcertificate`
 - o **plus optional** `<subpath>` **and** `<HashedId8>`
- `cpoc.jrc.ec.europa.eu/getectl/HashedId8`

- plus optional <subpath>
- cpoc.jrc.ec.europa.eu/getdeltaectl
 - **plus optional** <EctlSequenceNumber>
 - initially for testing purposes only

RCA requests, where $U \pm 1$ is the URL of the respective RCA:

- Url/getctrl
- Url/getctl

I.6. Link Certificates

I.6.1. Introduction

This chapter was compiled by EC JRC on the basis of different inputs of stakeholders after the November 2019 ETSI Plug-Test. It serves to support a structured way forward and definition on Link Certificates.

The main objective of link certificates are the update of trust anchors (RCA, TLM) in all C-ITS entities: Link certificates are used to change trust anchors certificates in an integrity/authenticated protected way.

Main focus on needed clarifications:

- What are the main objectives of Link Certificates for RCA/TLM in C-ITS?
- How to exactly create/specify link certificates for operational C-ITS deployment (based on the same ASN.1 Structure as defined in ETSI and IEEE standards)?
 - Issue raised at Plug-Test on possible unclarity how to specify the Link Certificates lifespan (starting time and validity period)
 - Issue raised at Plug-Test on the validation process for Link Certificates, i.e. how to exactly check the validity of the Link Cert up to a trusted Root CA or TLM Certificate in the PKI participants including C-ITS stations.
- Definition of the main use cases to be supported in the design of ETSI security architecture and evaluation if any specifications are missing in ETSI base standards or Certificate Policy for the processing of the Link Certificates or the other PKI artefacts in general.
- While the issuing of TLM Link Certificates is mandatory for the TLM, and hence the verification of TLM Link Certificate is mandatory for all PKI participants, is this also the case for RCA Link Certificates? What exactly does the C-ITS station need to support in terms of verification of RCA Link Certificates?

This chapter answers all the points above and adds extensive clarifications.

Note: All mentionings of “TLM Link Certificate” and “RCA Link Certificate” are technically implemented by “TLM Link Certificate Messages” and “RCA Link Certificate Messages” as described in chapter I.6.4.

I.6.2. Trust Anchor exchange on TLM Level (TLM Certificate)

According to the CPOC protocol³ each RCA operator will receive the initial (or current, if already re-keyed) TLM Certificate out-of-band at its enrolment on Commission premises in Ispra, which is the starting point of the chain of trust of TLM Certificates.

The TLM regularly re-keys its TLM Certificate following the rules of the CP. For the TLM it is mandatory to issue a TLM Link Certificate for every re-keyed TLM certificate. The TLM hence always supplies “the pair” of re-keyed (new certificate) TLM Certificate and corresponding TLM Link Certificate via the CPOC.

³ Compare with page 8, Footnote 2: <https://ec.europa.eu/jrc/en/publication/c-its-point-contact-cpoc-protocol>

The TLM/CPOC in the EU CCMS will provide different options to PKI participants to facilitate the update of their TLM Trust Anchors, i.e. the TLM Certificate. These are described in the following subchapters. There are three different options on how these files can be obtained, which are described below in detail. Depending on the option chosen, it may or may not be mandatory to verify the re-keyed TLM Certificates via the corresponding TLM Link Certificates for all PKI participants (RCA, EA/AA, C-ITS Stations).

I.6.2.1. TLM Certificate Update Option 1 – Out of band delivery of TLM Certificate & TLM Link Certificate:

The PKI participants can physically travel to Ispra and receive the current version of the TLM Certificate and corresponding TLM Link Certificate out of band directly from the CPOC. In any case, all PKI participants (including the C-ITS Station) shall verify the TLM Link Certificate using their current TLM Certificate before they actually change/update their trust anchor (TLM Certificate).

Note: In terms of the C-ITS station, the default is clearly that the C-ITS station itself shall check the validity of the TLM link certificate against the current TLM Certificate on board the C-ITS station. In the EU CCMS it is only possible to deviate from such validity check before exchanging the trust anchor TLM Certificate on the C-ITS station (e.g. checking the validity of the new TLM certificate only in a backend prior to submission to the C-ITS station), if such alternative process is covered and certified in the protection profile of the C-ITS station. Such protection profile of the C-ITS station shall be in line with the C-ITS security policy, section 1.6.2.2. (30).

I.6.2.2. TLM Certificate Update Option 2 – TLM Certificate & TLM Link Certificate available on the CPOC Website:

The PKI participants can access the CPOC Website and download the current version of the TLM Certificate and corresponding TLM Link Certificate (i.e. 2 separate binary .oer files) on the CPOC Website / CPOC Distribution Centre). All PKI participants (including the C-ITS Station) shall in any case verify the TLM Link Certificate using their current TLM Certificate before they actually change/update their trust anchor (TLM Certificate) with the new TLM Certificate.

The exact method of how the CPOC provides the TLM Certificate and TLM Link Certificate on the CPOC Website in a machine readable form is described in chapter I.5.2.

Note to further clarify: Irrespective of where the downloading/obtaining of the TLM Certificate and TLM Link Certificate from the CPOC website is actually done, the following applies in any case as the default:

- If e.g. the TLM Certificate and TLM Link Certificate is downloaded directly by the C-ITS station from the CPOC Website, then the C-ITS stations shall verify the TLM Link Certificate before it actually changes its trust anchor.
- If e.g. the TLM Certificate and TLM Link Certificate is downloaded first in a C-ITS Station backend environment, and then only forwarded to the actual C-ITS Station (e.g. in a proprietary secure way), then the C-ITS Station shall still verify the TLM Link Certificate before it actually changes its trust anchor. This means that the TLM Link Certificate needs to end up in the actual station and shall also be verified there.

In the EU CCMS it is only possible to deviate from such validity check before exchanging the trust anchor TLM Certificate on the C-ITS station (e.g. checking the validity of the new TLM certificate only in a backend prior to submission to the C-ITS station), if such alternative process is covered and certified in the protection profile of the C-ITS station. Such protection profile of the C-ITS station shall be in line with the C-ITS security policy, section 1.6.2.2. (30).

I.6.2.3. TLM Certificate Update Option 3 – new TLM Certificates available on specific versions of the ECTL:

The PKI participants can use specific published versions of the ECTL that include the new TLM Certificates to update their TLM Certificates. ECTLs are published by the CPOC. The ECTL versions, which can be used for TLM Certificate updates, are signed by the TLM with the currently still active TLM Certificate (compare with blue ECTLs in Figure 5), before the new re-keyed TLM Certificate becomes valid. These ECTLs can be received either directly from the CPOC Website or via other channels, such as ITS-G5 (from other PKI participants).

The exact method of how the CPOC provides the ECTLs on the CPOC Website is described in I.5.

Following the ETSI Standards, these published versions of the ECTL (and delta ECTLs) may also be obtained via other channels than the CPOC Website, such as for instance via ITS-G5 from other PKI participants.

However, no matter by which method the ECTLs are received by the PKI participants, it is important on where the ECTLs are actually processed and validated. The following rules shall apply:

- If the ECTL is processed directly on the C-ITS station then the successful verification of the signature of the ECTL using the station's current TLM Certificate is sufficient to trust the new TLM certificate inside the ECTL. After successful signature verification of the ECTL the new TLM Certificate can be extracted from the ECTL and can be exchanged with the old TLM Certificate on the C-ITS Station. This is the case, because the ECTL itself provides a sufficient cryptographic link to the previous trust anchor embedded in the C-ITS Station.
- If the ECTL is processed in a C-ITS Station backend, and the new TLM Certificate is after successful verification of the ECTL signature extracted out of the ECTL and only forwarded to the actual C-ITS Station (e.g. in a proprietary secure way), then the C-ITS Station shall still verify the TLM Link Certificate Message (available on the CPOC Website) before it actually changes its trust anchor.

Note: In the EU CCMS it is only possible to deviate from such validity check before exchanging the trust anchor TLM Certificate on the C-ITS station (e.g. checking the validity of the new TLM certificate only in a backend prior to submission to the C-ITS station), if such alternative process is covered and certified in the protection profile of the C-ITS station. Such protection profile of the C-ITS station shall be in line with the C-ITS security policy, section 1.6.2.2. (30).

I.6.3. Trust Anchor exchange on RCA level (RCA Certificate):

The issuing of RCA Link Certificates is not mandatory for Root CAs for re-keying. In such case where re-keying (e.g. after the end of validity of the RCA Certificate) is done without RCA Link Certificates and hence no RCA Link Certificate is delivered to the CPOC, the RCA will have to undergo a full new enrolment procedure at the CPA/CPOC. Full new enrolment means that the administrative process (e.g. CPA approval of application form, etc.) is more cumbersome when approaching the CPOC (for more information compare with the use cases in section I.6.3.1).

Root CAs may re-key also with RCA Link Certificates according to the CP. With RCA Link Certificates the process of processing the re-keyed RCA Certificate at the CPOC is associated with less administrative burden, since the update of the RCA Certificate does not have to be treated like a new enrolment from the administrative point of view (including steps like CPA approval of the application form like in an initial enrolment, etc.).

At this moment there is no use case to perform a verification of the RCA Link Certificates for any PKI Participant, except the CPOC ENTRY before handing over the RCA Certificate to the TLM for the re-keying use cases (e.g. also to double check if the CPA has actually approved changes in permissions of the RCA, etc.).

I.6.3.1. Example use cases of RCA link certificates

This chapter lists examples of use cases where link certificates are needed for re-keyed RCA certificates, in order to avoid a full new enrolment of the RCA in the EU CCMS. A full new enrolment means that from an

administrative point of view, the CPOC will treat the RCA like a new RCA at its first initial enrolment in the EU CCMS – including all the checks of the CPA and administrative burden. A new enrolment does not mean that the old RCA certificate is necessarily removed from the ECTL.

1. Expiry of the validity period of the RCA certificate: the RCA link certificate serves for the transition period of validity between the old RCA Certificate and the new self-signed RCA Certificate. The provided RCA Link certificate eases the process at the CPOC when the re-keyed RCA Certificate is delivered by the RCA authorized representative, since a cryptographic link is demonstrated between the old RCA certificate and the new, proving the origin of the new self-signed RCA Certificate with the new validity period.

Note: If no link RCA certificate is delivered to the CPOC, the new self-signed RCA certificate (with the new validity period) will have to undergo the same administrative process like an initial new RCA enrolment (i.e. more administrative burden like approval of the application form at the CPA, etc.).

2. ANY changes in the RCA certificate 'ToBeSignedCertificate', such as permissions, CertificateID or region prior to the expiry of validity period of the certificate: any change in permissions, CertificateID or region requires prior approval of the CPA. In case of positive approval of the CPA, a new self-signed RCA certificate with the updated permissions, CertificateID or region (based on CPA approval) as well as a corresponding link RCA certificate has to be delivered to the CPOC in addition to the current RCA certificate.

Note: Without the use of link RCA certificate this operation of changing contents (such as the permissions, CertificateID or region) of existing RCA certificates on the ECTL is not allowed by the CPOC/TLM. It will only be possible to insert a completely new self-signed RCA certificate, where the process follows the initial first enrolment process of a RCA (i.e. CPA approval of the new RCA, application form approval, etc.).

I.6.3.2. Example use cases where RCA link certificates are NOT needed

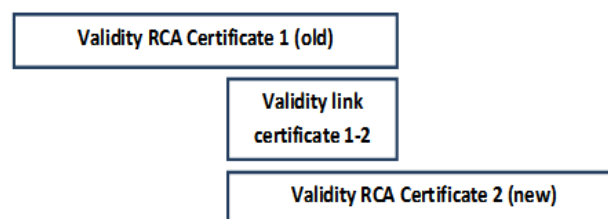
To give a full picture, this chapter lists example use cases where RCA link certificates are NOT needed.

1. Initial first enrolment of a root CA on the ECTL.
2. A root CA stops operation (it was not compromised): In this case the exiting root CA certificate is removed from the ECTL.
3. A root CA is compromised (disaster recovery / revocation situation). In this case, no re-keying with a compromised root CA and compromised private key shall be done. The compromised root CA certificate is removed from the ECTL. A new RCA certificate should be created and enrolled.

I.6.4. Construction and verification of RCA and TLM Link Certificates:

The concept of link certificates are used to ensure trust migration from a current valid self-signed certificate (denoted in Figure 6 as the “old” certificate) to the “new” self-signed one.

Figure 6: General schematic representation of transition period using the concept of a “link certificate”
(shown is the case of a RCA certificate)



ETSI TS 102 941 [2] supports the concept of TLM Link Certificates and RCA Link Certificates as foreseen in the (current version) of the European C-ITS Certificate Policy via Link Certificate Messages, both for RCAs and the TLM. In the EU CCMS the TLM is not going to include the TLM Link Certificate Messages and RCA Link Certificate Messages inside the ECTL.

I.6.4.1. Construction of Link Certificates

A “link certificate” is a message signed by the “old” CA and containing the certificate of the “new” CA. (“CA” in this section also encompasses the TLM). The format is defined in ETSI TS 102 941 [2] as follows:

- TlmLinkCertificateMessage for TLM link certificates,
- singleSignedLinkCertificateRca for single signed RCA link certificates,
- doubleSignedlinkCertificateRca for double signed RCA link certificates.

I.6.4.2. Verification of Link Certificates

The following two sections describe the verification of RCA and TLM link certificates. It is important to note that this verification is only one part of the processing that a receiver carries out to determine whether a link certificate is valid. In order for a link certificate to be valid:

- The old certificate shall be valid (by rules established by the CPA)
- The new certificate shall be valid (by rules established by the CPA)
- The old certificate shall be permitted to issue the link certificate (by the rules provided below).

The rules provided below are deliberately narrowly scoped and only address the conditions that establish that old certificate A was entitled to link to new certificate B. The rules below do not address the validity conditions for old certificate A and new certificate B separately.

I.6.4.2.1. Verification of TLM Link Certificates:

A TLM Link Certificate is valid if the following properties hold.

Table 6: Consistency requirements for TLM Link Certificates

ieee1609Dot2Data field	Requirements
protocolVersion	Shall be set to 3 (Uint8)
Content	signedData
SignedData field	Requirements
hashId	Consistent with signing key: sha384
tbsData	ToBeSignedData – described later in this table
Signer	Indicates the old TLM
Signature	Generated with the private key of the old TLM and in accordance with the 1609.2 signing specification
ToBeSignedData field	Requirements

Payload	Contains an ieee1609Dot2Data of type unsecured, containing a COER-encoded <u>ToBeSignedLinkCertificate</u> containing the sha384 hash of the new TLM certificate. See the following table for requirements on that certificate.
HeaderInfo	HeaderInfo – described later in this table
HeaderInfo field	Requirements
ITS-AID	Certificate Trust List service (0x02 70 / decimal 624) (see ETSI TS 102 965 [5])
generationTime	Present (required per ETSI TS 103 097 [3])
expiryTime	Absent
generationLocation	Absent
p2pcdLearningrequest	Absent
missingCrlIdentifier	Absent
encryptionKey	Absent
inlineP2pcdRequest	Absent
requestedCertificate	Absent
pduFunctionalType	Absent ⁴

Table 7: Requirements on new TLM certificates to permit it to be the subject of a link certificate

Certificate fields	Requirements
version	3
type	Explicit
Issuer	Self
ToBeSignedCertificate fields	Requirements
id	No constraints (allows ID to change in the event of a change of ownership)
cracaId	0 (per 103 097 [3])

⁴ In 1609.2b but not currently in 103 097 [3]

crlSeries	0 (per 103 097 [3])
validityPeriod	No constraints imposed by consistency. In most cases the certificate lifetime will begin during the lifetime of the previous certificate and end after it but this is not required by this document.
region	No constraints (TLM is trusted and TLM region of responsibility may change)
assuranceLevel	Absent
appPermissions	Shall contain CTL Service ITS-AID (0x02 70 / decimal 624) and the TLM CTL SSPs (bit at position 0 (80h) set to 1). Other appPermissions fields may be present without constraint (TLM is trusted to determine its own appPermissions).
certIssuePermissions	Absent (TLM does not issue certs)
certRequestPermissions	Absent
canRequestRollover	Absent
encryptionKey	Absent
verifyKeyIndicator	Of type verificationKey

I.6.4.2.2. Verification of Single Signed RCA Link Certificates:

A Single Signed RCA Link Certificate is valid if the following properties hold.

Table 8: Single Signed RCA Link Certificate: consistency between old CA (signer) and new CA (subject)

ieee1609Dot2Data field	Requirements
protocolVersion	Shall be set to 3 (UInt8)
Content	signedData
SignedData field	Requirements
hashId	Consistent with signing key: sha256 or sha384
tbsData	ToBeSignedData – described later in this table
Signer	Indicates the old RCA. Is always of type digest, i.e. is a HashedId8.
signature	Generated with the private key of the old RCA and in accordance with the 1609.2 signing specification
ToBeSignedData field	Requirements

Payload	Contains an IEEE1609Dot2Data of type unsecured, containing a COER-encoded EtsiTs102941Data with content of type ToBeSignedLinkCertificateRca containing the hash of the new Root CA certificate.
HeaderInfo	HeaderInfo – described later in this table
HeaderInfo field	Requirements
ITS-AID	Certificate Trust List service (0x02 70 / decimal 624) (see ETSI TS 102 965 [5])
generationTime	Present (as required by TS 103 097 [3])
expiryTime	Absent
generationLocation	Absent
p2pcdLearningrequest	Absent
missingCrlIdentifier	Absent
encryptionKey	Absent
inlineP2pcdRequest	Absent
requestedCertificate	Absent
pduFunctionalType	Absent ⁵

Table 9: Requirements on New Root CA certificate to permit it to be the subject of a link certificate

Certificate fields	Requirements
version	3
type	Explicit
issuer	Self
tobeSigned	ToBeSignedCertificate (see below)
signature	Generated with the private key corresponding to the public key in the certificate and in accordance with the 1609.2 signing specification.

⁵ In 1609.2b but not currently in 103 097 [3]

ToBeSignedCertificate fields	Requirements
id	No consistency constraints to be directly enforced (allows ID to change in the event of name change events, for example a change of ownership) but it shall follow the rules established by, and be approved by, the CPOC/CPA/TLM.
cracaId	0 (per 103 097 [3])
crlSeries	0 (per 103 097 [3])
validityPeriod	No constraints imposed by consistency. In most cases the certificate lifetime will begin during the lifetime of the previous certificate and end after it but this is not required by this document.
region	No constraints
assuranceLevel	Absent
appPermissions	For a root CA cert, shall contain CTL Service ITS-AID (0x02 70 / decimal 624) with the root CA CTL SSPs (bit at position 2 (20h) or position 3 (10h) set to 1). Other appPermissions fields may be present without constraint (CPA is in charge of authorizing the appPermissions).
certIssuePermissions	No constraints (CPA is in charge of authorizing the certIssuePermissions)
certRequestPermissions	Absent
canRequestRollover	Absent
encryptionKey	Optional
verifyKeyIndicator	Of type verificationKey

I.6.4.2.3. Verification of Double Signed RCA Link Certificate Message:

A Double Signed RCA Link Certificate Message is valid if the following properties hold.

Table 10: Double Signed RCA Link Certificate: consistency between new CA (signer) and old CA (subject)

ieee1609Dot2Data field	Requirements
protocolVersion	Shall be set to 3 (UInt8)
Content	signedData
SignedData field	Requirements
hashId	Consistent with signing key: sha256 or sha384

tbsData	ToBeSignedData – described later in this table
Signer	Indicates the new RCA. Is always of type digest, i.e. is a HashedId8.
signature	Generated with the private key of the new RCA and in accordance with the 1609.2 signing specification
ToBeSignedData field	Requirements
Payload	Contains an Ieee1609Dot2Data of type unsecured, containing a C-OER encoded EtsiTs102941Data with the content of type RcaSingleSignedLinkCertificateMessage containing the Single Signed RCA Link Certificate Message.
HeaderInfo	HeaderInfo – described later in this table
HeaderInfo field	Requirements
ITS-AID	Certificate Trust List service (0x02 70 / decimal 624) (see ETSI TS 102 965 [5])
generationTime	Present (as required by TS 103 097 [3])
expiryTime	Absent
generationLocation	Absent
p2pcdLearningrequest	Absent
missingCrlIdentifier	Absent
encryptionKey	Absent
inlineP2pcdRequest	Absent
requestedCertificate	Absent
pduFunctionalType	Absent ⁶

Table 11: Requirements on Old Root CA certificate to permit it to be the subject of a double-signed link certificate

Certificate fields	Requirements
version	3
type	Explicit

⁶ In 1609.2b but not currently in 103 097 [3]

issuer	Self
tobeSigned	ToBeSignedCertificate (see below)
signature	Generated with the private key corresponding to the public key in the certificate and in accordance with the 1609.2 signing specification.
ToBeSignedCertificate fields	Requirements
id	No consistency constraints to be directly enforced (allows ID to change in the event of name change events, for example a change of ownership) but id shall follow the rules established by, and be approved by, the CPOC/CPA/TLM.
cracaId	0 (per 103 097 [3])
crlSeries	0 (per 103 097 [3])
validityPeriod	No constraints imposed by consistency ⁷ .
region	No constraints
assuranceLevel	Absent
appPermissions	For a root CA cert, shall contain CTL Service ITS-AID (0x02 70 / decimal 624) with the root CA CTL SSPs (bit at position 2 (20h) or position 3 (10h) set to 1). Other appPermissions fields may be present without constraint (CPA is in charge of authorizing the appPermissions).
certIssuePermissions	No constraints (CPA is in charge of authorizing the certIssuePermissions)
certRequestPermissions	Absent
canRequestRollover	Absent
encryptionKey	Optional
verifyKeyIndicator	Of type verificationKey

I.6.4.3. Requirements on SSPs

According to TS 102 941 [2] to sign a RCA link certificate message, a Root CA certificate shall contain CTL Service ITS-AID (0x02 70 / decimal 624) with one of the associated SSPs bits at position 2 (20h) or position 3 (10h) set to 1. The receiver shall enforce an OR condition on these two bits position 2-3 to accept RCA link cert messages.

⁷ Consider the case where an old root CA operator goes out of business six months into operation and wants to designate an already-existing new root CA as its successor. In this case the "new" root CA will have a certificate with an earlier validity period than the "old" root CA. For this reason, and because the RCA link certificate will be used only by the CPOC ENTRY which is capable of managing subtle cases like this, there is no consistency requirement that the "new" root CA is "newer" than the "old" one.

I.6.5. Linkage of Certificates inside the ECTL

It is possible to implement linkages of certificates directly inside the ECTL based on ETSI 102 941 [2] and ETSI 103 097 [3].

I.6.5.1. Linkage of TLM certificates

The TLM in the EU CCMS will always omit the `linkTLMCertificate` in the `TlmEntry`, since the TLM Link Certificate Message will be used outside of the ECTL instead. This has no impact on the process of TLM Certificate updates that may also require the use of TLM Link Certificate Messages instead. More details can be found in section I.6.2.

I.6.5.2. Linkage of RCA certificates

In case a RCA re-keys with the help of RCA Link Certificate Messages at the CPOC and passes all checks, the TLM shall insert the new RCA Certificate in the ECTL. In addition the TLM shall also fill the field `successorTo` in the ECTL with the `EtsiTs103097Certificate` of the old RCA Certificate (that is still valid). Through this insertion in the ECTL a clear link between the old and the new re-keyed RCA Certificate shall be directly established inside the ECTL. C-ITS stations at this moment do not need to be able to validate the newly defined RCA Link Certificate Messages (see chapter I.6.4.1), since all information on RCA linkages are available directly in the ECTL via the `successorTo` entries.

To summarise, in the new logic of the `RootCaEntry` in the ECTL the following applies:

- `selfSignedRootCa` shall be the indication that the root CA `EtsiTs103097Certificate` is trusted
- `successorTo` shall be a pointer to the previous trusted RCA `EtsiTs103097Certificate`, indicating that these two certificates hence have a linkage

Note 1: This change in naming (and intent of using the fields) of the standard is not interfering with existing implementations, since only the name changes and not the type of the entry (i.e. the type stays `EtsiTs103097Certificate`). Interpretation of the `successorTo` entries on the ECTL is an optional feature for C-ITS stations depending on their needs. There may be relevant use-cases for C-ITS stations to make use of the interpretation of linkages of RCA certificates on the ECTL, such as the management of its own “home” PKI enrolment, in order to identify if its own root CA has re-keyed its certificate, and hence the station requires updates accordingly. However, such use-cases are out of scope of this document at this moment and may need to be further defined by standardisation activities.

Note 2: In case multiple Root CAs re-key to the same new RCA Certificate an identical `selfsignedRootCa` entry may appear multiple times in different `RootCaEntry` fields on the ECTL.

Note 3: After the expiry of validity of RCA Certificates on the ECTL the TLM shall “clean” their entries in newly published versions of the ECTL. However, the TLM shall only remove the `RootCaEntry` of the actual expired certificates. `successorTo` entries of `RootCaEntry` of RCA Certificates that are still valid (and where `successorTo` may hence point to already expired RCA Certificates) stay on the ECTL until the corresponding successor RCA Certificate has also expired.

Note 4: In case of a compromised RCA and the consequently necessary revocation of its RCA certificate, the TLM shall delete the `RootCaEntry` of this RCA certificate. Depending on the exact nature of the compromise situation and the decision of the CPA/TLM the `successorTo` entries pointing to this RCA may

also have to be deleted, and potentially all new RCA rekeyed certificate appearing in the deleted RootCaEntries may be removed.

I.6.5.3. Example of a RCA re-key scenario and its impact on the ECTL for further illustration

An example is explained below, where a RCA1 wants to re-key towards its next certificate RCA2. RCA2 is hence the successor of RCA1. In a last step, also RCA2 is then re-keyed in the example to RCA3. RCA3 is the successor of RCA2. This example shows how this is reflected in the ECTL.

I.6.5.3.1. Step 1: Creation of the RCA Link Certificate

RCA1 creates a Double Signed RCA Link Certificate Message “RCA1-->RCA2”, following the new format defined in chapter I.6.4.1. This Message is only used at the level of the CPOC. In the EU CCMS it is not foreseen to publish Root CA Link Certificates anywhere at this moment, since they are only used at the level of the CPOC when RCAs wish to re-key their RCA Certificates with the help of Link Certificates. Hence, RCA Link Certificates are not inserted in the ECTL and also not inserted in the CTL of Root CAs.

I.6.5.3.2. Step 2: What happens at the CPOC ENTRY?

RCA2 presents its new certificate “RCA2” as well as the “RCA1-->RCA2” Link Certificate message to the CPOC in Ispra (physical attendance of the authorized representative) for re-keying.

The CPOC then validates the RCA Link Certificate Message (the CPOC is hence at this moment the only PKI participant in the EU CCMS that SHALL be able to validate RCA Link Certificate Messages):

- The CPOC validates with the help of the cryptographically signed RCA Link Certificate Message “RCA1-->RCA2” the following:
 1. Through the validation of the InnerLinkCert the CPOC validates that RCA1 has designated RCA2 as its successor – RCA2 has been signed with the private key of RCA1.
 2. Through the validation of the OuterLinkCert the CPOC validates that RCA2 has accepted to be the successor of RCA1.

The same process applies for any following re-key, e.g. to RCA3, RCA4, etc.

I.6.5.3.3. Step 3: What is published in the ECTL by the TLM?

Version 1 of the full ECTL

Version 1 of the full ECTL only contains the original RCA1 certificate in the RootCAEntry:

```
RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA1
    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
    RCA1)
}
```

Version 2 - FULL ECTL:

After re-key of RCA1 and the successful validation process of RCA2 and the Link Certificate “RCA1→RCA” at the CPOC (see Step 2), the TLM inserts a new RootCAEntry in the ECTL. Version 2 of the full ECTL looks like this:

```
RootCaEntry ::= SEQUENCE { // this is still the RootCAEntry of RCA1
```

```

    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
RCA1)
}

```

```

RootCaEntry ::= SEQUENCE { // this is the new RootCAEntry of RCA2
    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
RCA2)
    successorTo           EtsiTs103097Certificate OPTIONAL, //(RCA
Certificate of RCA1)
}

```

NOTE: The `successorTo` entry shall contain the same RCA certificate (RCA1) as in the Link Certificate message “RCA1→RCA2” that is presented to the CPOC.

Version 2 – DELTA ECTL

The corresponding DELTA ECTL looks like this:

ADD 1 RootCaEntry:

```

RootCaEntry ::= SEQUENCE { // this is the new RootCAEntry of RCA2
    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
RCA2)
    successorTo           EtsiTs103097Certificate OPTIONAL //(RCA Certificate
of RCA1)
}

```

Version 3 - FULL ECTL:

This version shows what happens if RCA1 has expired. The TLM only removes the RootCAEntry of the expired certificates. The RootCAEntry of RCA2 stays, since RCA2 is still valid (and hence the reference in the RCA2 field “successorTo” to RCA1 also stays, until RCA2 expires). Hence, after expiry of RCA1 the next published Version 3 of the full ECTL will look like this below.

```

RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA2
    selfsignedRootCa      EtsiTs103097Certificate, //(RCA2)
    successorTo           EtsiTs103097Certificate OPTIONAL //(RCA1)
}

```

Version 3 – DELTA ECTL

The corresponding DELTA ECTL of Version 3 would look like this:

DELETE 1 RootCaEntry:

```

RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA1
selfsignedRootCa EtsiTs103097Certificate, //(RCA Certificate of
RCA1)
}

```

I.6.5.3.4. Step 4: Next re-keys of RCA – what happens to linkages?

In any further re-keying of RCA Certificates the same principles apply of updates of the full and delta ECTLs to indicate the linkages of RCAs. New RootCaEntry are added, and old ones are kept until the RCA certificates expire. For instance, for the example in the previous chapters, the FULL ECTL would look like the following in case of two re-keys of the initial RCA certificate (and if RCA1 and all rekeyed certificates RCA2 and RCA3 are not expired yet):

```

RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA1, if not
expired yet. This entry does not have a successorTo field, since it is the
first RCA Certificate of this RCA.

    selfsignedRootCa      EtsiTs103097Certificate, // RCA Certificate of RCA1
}

```

```

RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA2, having a
linkage to RCA1. The successorTo field indicates that RCA2 is the successor
of RCA1

    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
RCA2)

    successorTo           EtsiTs103097Certificate OPTIONAL, //(RCA
Certificate of RCA1)
}

```

```

RootCaEntry ::= SEQUENCE { // this is the RootCAEntry of RCA3, having a
linkage to RCA2. The successorTo field indicates that RCA3 is the successor
of RCA2

    selfsignedRootCa      EtsiTs103097Certificate, //(RCA Certificate of
RCA3)

    successorTo           EtsiTs103097Certificate OPTIONAL, //(RCA
Certificate of RCA2)
}

```

Note: In the example above the C-ITS-Station shall be able to interpret the following out of the three RootCaEntry entries on the ECTL:

- RootCaEntry of RCA1:
 - RCA1 is a trusted RCA certificate. The C-ITS station shall check for CRLs of RCA1 at the DC of RCA1.
 - RCA1 is not a successor RCA certificate, it is an initial RCA certificate that has not been re-keyed yet.
- RootCaEntry of RCA2:
 - RCA2 is a trusted RCA certificate. The C-ITS station shall check for CRLs of RCA2 at the DC of RCA2.

- RCA2 is a successor RCA certificate (of RCA1)
- RootCaEntry of RCA3:
 - RCA3 is a trusted RCA certificate. The C-ITS station shall check for CRLs of RCA3 at the DC of RCA3.
 - RCA3 is a successor RCA certificate (of RCA2)
 - The RCA2 certificate in the successorTo field is a successor RCA certificate of RCA1

I.7. CPOC ENTRY checks on RCA Certificates

This chapter defines the checks that the CPOC ENTRY will perform on any RCA Certificates in the context of the EU CCMS. The following tables are based on the RCA certificate template provided in chapter I.3.1.

If one of the checks listed in Table 12 and Table 13 fails, the RCA certificate shall be rejected by the CPOC.

Table 12: CPOC ENTRY checks of the attributes of RCA Certificates

Attributes	Values	Requirements (mandatory)	Recommendations (best practices)
version	3	ETSI TS 103 097, section A.2	
type	explicit	ETSI TS 103 097, section 6	
issuer	"self": "sha256" or "sha384"	For RCA certificate. ETSI TS 103 097, section 7.2.3, ETSI TS 103 097, section A.2	
	sha256AndDigest or sha384AndDigest	For RCA link certificate. IEEE1609.2a-2017 section 6.4.7	
toBeSigned.id.name	See I.3.2	Requirements of CertificateID according to chapter I.3.2.2 shall be checked. Appropriateness of RCA Certificate extension (e.g. TEST etc.) shall be checked.	
cracald	000000	ETSI TS 103 097, section 6	
crlSeries	0	ETSI TS 103 097, section 6	
validityPeriod.start		Check if a valid start date is included. Check if that validity start date combined with duration is in line with the CP requirements.	Recommend to set a value in a relevant range, e.g. between 01-01-2015 and 31-12-2040
validityPeriod.duration	years, sixtyhours, hours	Whatever the granularity, sub-CAs and C-ITS stations shall use Gregorian calendar to compute a deterministic end date of the RCA certificate. The RCA certificate validity duration resulting from the computation of validityPeriod.start and validityPeriod.duration shall be compliant to the CP section 7.2.	
assuranceLevel		Shall not be present.	

region		If present, check if it is in line with the requirements of chapter I.3.9.	
appPermissions	psid=624 (CTL), ssp="0138", psid=622 (CRL), ssp="01"	ETSI TS 103 097, section 7.2.3 - One PsidSsp entry shall contain psid=624 (CTL), ssp="0138". The other PsidSsp entry shall contain psid=622 (CRL), ssp="01". IEEE1609-2a-2017 section 6.4.8 - appPermissions is a critical information, and shall be present. A valid instance of appPermissions contains any particular ITS-AID value in at most one entry.	
appPermissions.ssp	"bitmapSsp": XXX See section I.4	One valid entry shall be inserted. If the ITS-AID defines a table of bitmap permissions, e.g. TLM in ETSI 103 301 v1.3.1, Table 6, BitmapSsp shall be used.	Recommend the use of bitmapSsp rather than opaque. Convergence to simplify C-ITS station implementation for cost effectiveness. Reminder: - opaque OCTET STRING (SIZE(0..MAX)), - BitmapSsp ::= OCTET STRING (SIZE(0..31))
certRequestPermissions		ETSI TS 103 097, section A.1 certRequestPermissions shall not be presented in ExplicitCertificate,	
certIssuePermissions		IEEE1609-2a-2017 section 6.4.8 - certIssuePermissions is a critical information, and shall be present. .) certIssuePermissions for at least one ITS-AID shall be set to 1 (hence being active). .) For certIssuePermissions the aid, ssp and bitmask shall match the certIssuePermissions in the application form, for the initial request. .) For root CA re-keying with linkages to previous root CA certificates it shall be verified that the certIssuePermissions of the new certificate matches the certIssuePermissions of the old RCA certificate. Any change in certIssuePermissions have to first be approved by the CPA. In case such approval exists, the CPOC ENTRY shall check and compare all changes against this approval. .) for each RCA certificate, if a bit in the sspBitmask is set to 0, the corresponding bit in the sspValue shall be set to 1.	

certIssuePermissions.subjectPermissions	explicit	<p>Shall use “explicit” rather than “all”.</p> <p>“explicit” requires the certIssuePermissions specifying each ITS-AID and its permissions, hence avoiding to grant all ITS-AIDs and their permissions not indicated by other PsidGroupPermissions in the same certIssuePermissions field.</p>	
certIssuePermissions.subjectPermissions.explicit.psid		The “explicit” attribute shall contain at least one element, i.e. at least one of the IEEE registered ITS-AIDs listed in chapter I.4.2. No other elements shall be used than the one listed in chapter I.4.2.	
certIssuePermissions.subjectPermissions.explicit.sspRange	bitmapSspRange	If the ITS-AID defines a table of bitmap permissions, e.g. TLM in ETSI 103 301 v1.3.1, Table 6, BitmapSsp shall be used.	<p>Recommend to use bitmapSspRange rather than opaque choice.</p> <p>Reminder:</p> <ul style="list-style-type: none"> - opaque SequenceOfOctetString, - BitmapSspRange ::= SEQUENCE { sspValue OCTET STRING (SIZE(1..32)), sspBitmask OCTET STRING (SIZE(1..32)) } <p>Convergence to simplify C-ITS station implementation for cost effectiveness. Avoiding structure conversion and multiple certificate validation logic implementations due to different types of structure.</p>
certIssuePermissions.subjectPermissions.explicit.psid	141 (decimal)	There shall be no SSP value specified according to the GeoNet standard ETSI EN 302 636-4-1 V1.3.1. See table 24 in that document: permissions_length = 0, permissions = void.	
certIssuePermissions.subjectPermissions.explicit.minChainLength	2	If the subjectPermissions is for EC and AT	
	1	If the subjectPermissions is for EA and AA	<p>ETSI TS 103 097, section A.1 - minChainLength has a default value of 1.</p> <p>Recommend to omit the minChainLength attribute if it contains the default value.</p>
certIssuePermissions.subjectPermissions.explicit.chainLengthRange	0		<p>ETSI TS 103 097, section A.1 - chainLengthRange has a default value of 0.</p> <p>Recommend to omit the chainLengthRange attribute if it contains the default value.</p>
certIssuePermissions.subjectPermissions.explicit.eeType	CO (app, enroll)		

	80 (app)		<p>If the subjectPermissions is for EA and AA.</p> <p>ETSI TS 103 097, section A.1 - eeType has a default value of 80 (app).</p> <p>Recommend to omit the eeType attribute if it contains the default value.</p>
verificationKeyIndicator		<p>ETSI TS 103 097 v1.4.1, section 6 –</p> <p>The component verifyKeyIndicator of type VerificationKeyIndicator as defined in IEEE Std 1609.2 [1], present and constrained to the choice verificationKey.</p>	
encryptionKey		<p>ETSI TS 103 097 v1.4.1, section 7.2.3 - encryptionKey shall not be present.</p>	
signature		<p>Verifies with the public key included in toBeSigned.verifyKeyIndicator.verificationKey</p>	

Table 13: CPOC ENTRY checks of other properties of RCA Certificates

<i>Property</i>	<i>Values</i>	<i>Requirements (mandatory)</i>	<i>Recommendations (best practices)</i>
HashedId8		The HashedId8 of the Root certificate is unique among all certificates on the ECTL.	

Annex II. RCA Enrolment Form

The RCA Enrolment form template shall be filled-in by RCAs to enrol at the CPA. This is the first step needed in order to inform the CPA on the administrative details and authorised representative information of the RCA. After submission of the RCA Enrolment Form the CPA is going to assign the RCA a unique CPA-ID. The RCA Enrolment form shall be printed and signed by the RCA authorised representative and sent to the CPA.

How to use this template:

Please fill in all fields that are marked with *<instructions>*:

- *<insert>* text fields: please directly enter text and delete all blue instructions. Fill with "n/a" if not applicable.
- Checkboxes ☐: please replace ☐ with X to "select" them. Leave ☐ if checkbox is not applicable.
- No part of the form (tables, fields to be filled, etc.) is allowed to be changed by the applicant – should you experience problems, contact the CPA first.

II.1. Type of enrolment application

<Please fill in the following table.>

Type of enrolment application	<i><Please select the type of the intended RCA enrolment application below.</i> First initial enrolment of RCA Organisation information Update of information of already enrolled RCA Organisation <i>Note: In case of "update of information" please only fill the chapters and fields that need to be updated in this RCA Enrolment Form, i.e. all fields that remain unchanged can be left blank. Any updates of attachments of the Enrolment Form, such as Updates of the CP Audit Report summary shall be included in the update.</i>
-------------------------------	--

II.2. Information on the RCA organisation

<Please fill in the following table. >

RCA Organisation Name	<i><please insert the full name of the associated legal person or other organisational entity responsible for the RCA operation here></i>
RCA Organisation legal status information	<i><please insert the legal status of the associated legal person or other organisational entity responsible for the RCA operation here.</i> <i>Further, please attach copies of any relevant registration information (e.g. company registration) of the associated legal person or other organisational entity to this Enrolment form.></i>

Postal Address of the RCA Organisation (reaching the authorised representative)	<i><please insert the full postal address of the RCA organisation here, including street, number, city, postal code, country and/or any other relevant information for postal mail></i>
---	---

II.3. Information on the RCA authorised representative (AR)

II.3.1. RCA Authorised Representative 1

<Please fill in the following table. Please duplicate the table if there is more than one Authorised Representative of the RCA Organisation. RCA Authorised representatives are responsible for signing the RCA enrolment Form and RCA application form on behalf of the RCA organisation. Usually, there is only one RCA Authorised Representative assigned.>

Full name of the physical contact person / authorised representative (AR) in the RCA organisation	<i><please insert the full name of the physical contact person of the RCA organisation here, who will sign this form and any following RCA application forms, revocation forms (etc.) on behalf of the RCA. This person acts as the physical contact person and hence authorised representative of the RCA organisation towards the CPA and CPOC.></i>
Date and place of birth of the physical contact person / authorised representative (AR) in the RCA organisation	<i><please insert the date and place of birth of the physical contact person / authorised representative in the RCA organisation here></i>
Reference to a nationally recognised identity document of the authorised representative (AR)	<i>please insert the reference (e.g. passport ID) here and attach a copy of the document to this RCA Enrolment form></i>
Certificate of Authorisation / documentation that the authorised representative works for the RCA organisation.	<i>Please attach evidence/documentation to this Enrolment form that the authorised representative is associated with the legal entity of the RCA Organisation.</i>
e-mail address of the contact person in the RCA organisation	<i><please insert the e-mail address of the physical contact person here. Note that only corporate email addresses matching the organization domain name will be accepted. No private/personal addresses shall be used></i>
Telephone number of the authorised representative of the RCA organisation	<i><please insert the business telephone number of the RCA authorised representative person here></i>

--	--

II.4. Identity and registration information of RCA trusted couriers

<Please fill in the following table. Please duplicate the table if there is more than one trusted courier of the RCA organisation.>

Trusted Couriers are the persons of the RCA organisations that will physically travel to European Commission premises in Ispra (Italy) to deliver RCA Certificates to the CPOC for inclusion in the ECTL.>

II.4.1. RCA Trusted Courier 1

Full name of the RCA trusted courier	<i><please insert the full name of the trusted courier person here></i>
Date and place of birth	<i><please insert the date and place of birth of the trusted courier person></i>
Reference to a nationally recognised identity document	<i><please insert the reference (e.g. passport ID) here and attach a copy of the document to this RCA Enrolment form></i>
Certificate of Authorisation / documentation that the RCA trusted courier works for the RCA organisation.	<i>Please attach evidence/documentation to this Enrolment form that the RCA trusted courier is associated with the legal entity of the RCA Organisation.</i>
e-mail address of the RCA trusted courier	<i><please insert the e-mail address of the physical contact person here. Note that only corporate email addresses matching the organization domain name will be accepted. No private/personal addresses shall be used></i>
Telephone number of the RCA trusted courier	<i><please insert the business telephone number (preferably a phone number that is reachable while travelling to EC premises) of the RCA trusted courier person here></i>

II.5. Personal data processing

The processing of the personal data provided in this form and its attachments is covered by a declaration of confidentiality on the protection of personal data. These declarations can be found here:

- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00744>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-01239.2>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00406>

Please consult these declarations before filling, signing and submitting the form.

II.6. Date and Signature

Date and Place:

Signature of RCA authorized representative:

Stamp (optional):

II.7. Attachments to the RCA Enrolment Form

The enrolling RCA organisation shall attach a copy of the following documents to the RCA Enrolment Form:

- CP Audit Report: Copy of the last RCA audit report summary against the CP provided by the accredited PKI auditor, including, if applicable, copies of any audited changes in the CPS of the RCA.
- Documents regarding the RCA Organisation & Authorised Representative(s):
 - Copy of relevant RCA organisation legal status / registration information
 - Copy of nationally recognised identity document of the authorised representative of the RCA organisation
 - Certificate of Authorisation / documentation that the authorised representative is associated with the legal entity of the RCA organisation.
- Documents regarding the RCA Trusted Courier(s):
 - Copy of nationally recognised identity document of the RCA trusted courier(s)
 - Certificate of Authorisation / documentation that the RCA trusted courier(s) are associated with the legal entity of the RCA organisation.

Comments/Explanations on attachments:

<If any, please insert further comments/explanations regarding attachments>

Annex III. RCA Enrolment Approval Form

This RCA Enrolment Approval form shall be filled-in by the CPA after receiving the RCA Enrolment Form. The RCA Enrolment Approval form shall be printed and signed (digitally or on paper) by the CPA authorised representative. If the form is signed on paper, it shall be scanned and turned into a PDF by the CPA. The form shall be securely submitted back to the RCA and CPOC-ENTRY/TLM.

For each received RCA Enrolment Form (and updates thereof) an own RCA Enrolment Approval Form shall be filled-in, signed and submitted.

III.1. Summary of the received RCA Enrolment Form

The CPA has received an RCA Enrolment Form on *<insert date>* by the identified organization *<insert organisation>*.

III.2. CPA assessment of the received RCA Enrolment Form

The CPA has assessed the RCA Enrolment form and its attachments.

<insert CPA process, short summary of date of meeting, comments, etc. >

III.3. CPA approval of the RCA Enrolment form

Based on the receipt of the RCA Enrolment form and the conducted CPA assessment, the CPA

<mark relevant box >

☐ herewith approves the RCA Enrolment Form and will inform the applicant RCA and the CPOC/TLM accordingly. The following unique <CPA-ID> is assigned to the RCA applicant:

<Insert unique <CPA-ID>

☐ rejects the RCA Enrolment Form and will inform the applicant RCA organisation and the CPOC/TLM accordingly.

Comments / Recommendations:

<add any comments or recommendations>

Date and Place:

Name of CPA authorized representative:

Signature of CPA representative:

Stamp (only if applicable):

Annex IV. RCA Application Form

The RCA application form template shall be filled-in by RCAs to apply at the CPA for insertion of their RCA certificate in the ECTL. The RCA application form shall be printed and signed by its contact point / authorised representative and sent to the CPA.

For each RCA certificate that shall be added to the ECTL an own RCA Application Form shall be filled-in, signed and submitted.

How to use this template:

Please fill in all fields that are marked with *<instructions>*:

- *<insert>* text fields: please directly enter text and delete all blue instructions. Fill with "n/a" if not applicable.
- Checkboxes ☐: please replace ☐ with X to "select" them. Leave ☐ if checkbox is not applicable.
- No part of the form (tables, fields to be filled, etc.) is allowed to be changed by the applicant – should you experience problems, contact the CPA first.

IV.1. Identity of the organisation and registration information

<Please fill in the following table:>

RCA Application Form ID	<p><i><please insert the RCA Application Form ID here></i></p> <p><i>Note: The RCA Application Form ID is based on two components:</i></p> <ul style="list-style-type: none">• <i><CPA-ID></i>, which is a unique identifier assigned by the CPA to each RCA organisation (and also used in the RCA CertificateID, as defined in the CPOC Protocol, Annex I). This CPA-ID shall be requested by the RCA applicant before submission of this RCA application Form by the CPA via the RCA Enrolment Form – please contact the CPA if you have not done that yet.• <i><RCA Application Identifier></i>, which consists out of the prefix "RCA-Application-Form_" plus an assigned consecutive number, starting with 1. The RCA Application Identifier increases for every new RCA Application Form submitted and shall be assigned by the RCA.• <i><CPA-ID> and <RCA Application Identifier> shall be combined using a "_" as a separator.</i> <p><i>Example 1</i></p> <p><i>The assigned unique <CPA-ID> of this RCA example is "2".</i></p> <ul style="list-style-type: none">• <i>Hence, the first RCA Application Form ID submitted of this RCA would be: 2_RCA-Application-Form_1</i>• <i>The second RCA Application form ID submitted of this RCA would be: 2_RCA-Application-Form_2</i>• <i>The third: 2_RCA-Application-Form_3 ... etc.</i> <p><i>Example 2</i></p>
-------------------------	--

	<p><i>The assigned <CPA-ID> of this RCA example is "5".</i></p> <ul style="list-style-type: none"> • Hence, the first RCA Application Form ID submitted of this RCA would be: <i>5_RCA-Application-Form_1</i> • The second RCA Application form ID submitted of this RCA would be: <i>5_RCA-Application-Form_2</i> • The third: <i>5_RCA-Application-Form_3... etc.</i> <p><i>In case of any doubt, please contact the CPA AR prior to submission of this RCA Application Form stating your intent to assign a new RCA Application Form ID.</i></p>
--	--

RCA Organisation Name	<i><please insert the legal entity name responsible for the RCA operation here, matching the approved RCA Enrolment Form.></i>
Name of the physical contact person / authorised representative in the organisation	<i><please insert the name of the physical contact person of the RCA organisation here, who signs this RCA Application Form. This information shall match the contents of the approved RCA Enrolment Form.></i>
e-mail address of the contact person in the RCA organisation	<i><please insert the e-mail address of the physical contact person here. Note that only corporate email addresses matching the organization domain name will be accepted. No private/personal addresses shall be used></i>
Telephone number of the contact person in the RCA organisation	<i><please insert the business telephone number of the RCA authorised representative here></i>

IV.2. Type of RCA Application

<Please select the type of RCA Certificate application>

Type of RCA Application	<p><input type="checkbox"/> First enrolment of a new RCA Certificate in the EU CCMS, hence requiring CPA approval. → <i>proceed with section IV.3</i></p> <p><input type="checkbox"/> Re-key of an existing RCA Certificate in the EU CCMS without using RCA Link Certificate Messages, hence requiring CPA approval. → <i>proceed with section IV.3</i></p> <p><input type="checkbox"/> Re-key of an existing RCA Certificate in the EU CCMS with using RCA Link Certificate Messages → <i>proceed with section IV.4</i></p>
-------------------------	---

--	--

IV.3. RCA Certificate Information of the applicant self-signed RCA ETSI103097Certificate

<Please fill in the following table for the RCA CertificateID, Digital fingerprint, cryptographic information and DC URL of the RCA Certificate:>

RCA CertificateID	<p><i><please insert the RCA CertificateID here, in-line with the definitions of the CPOC Protocol, Annex I, chapter 9.2.2.></i></p> <p><i>Note: In case you do not know your <CPA-ID> component of the CertificateID, you have to please notify the CPA of your intended <RCA-NAME> before you are able to create your RCA Certificate and send this form.</i></p>
Digital fingerprint (i.e. hashvalue) of the RCA certificate	<p> <input type="checkbox"/> SHA-256 of RCA Certificate <input type="checkbox"/> SHA-384 of RCA Certificate <i><please select the applicable checkbox ></i> </p> <p><i><please insert the hashvalue (HEX) of the RCA self-signed ETSI 103 097Certificate here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.></i></p>
Cryptographic information	<p><i><please select which cryptographic algorithm and key length was used in the RCA certificate></i></p> <p> <input type="checkbox"/> ECDSA_nistP256_with_SHA 256 <input type="checkbox"/> ECDSA_brainpoolP256r1_with_SHA 256 <input type="checkbox"/> ECDSA_brainpoolP384r1_with_SHA 384 </p>
DC URL of the RCA	<p><i><please insert the DC URL of the RCA></i></p>

<Please use the following template tables to list all permissions according to the definitions in the tables in CPOC Annex I, chapter I.4.>

<Please select the following check-boxes in the table and list all set app permissions below.>

App Permissions				
ITS-AID	Value (decimal)	Value (hex)	Included in RCA certificate: <please select>	SSPValue (Hex) <please add the requested values accordingly>
CRL service	622	26e	<input type="checkbox"/>	
CTL service	624	270	<input type="checkbox"/>	
<p><insert any comments here></p>				

<Please select the following check-boxes in the tables and list all set cert issue permissions below. Please document the minimum chain length, chain length range and entity type used in the cert issue permission element. In case multiple cert issue permission elements with different chain length values are used please indicate in the tables below accordingly.>

Explicit cert issue permissions with minimum chain length = 1 (default), chain length range = 0 (default) and end entity type = app (default)					
ITS-AID	Value (decimal)	Value (hex)	Included in RCA certificate: <please select>	SSPValue (Hex) <please add the requested values accordingly>	Bitmask (Hex) <please add the requested values accordingly>
Secured certificate request service	623	26f	<input type="checkbox"/>		
<p><insert any comments here></p>					

Explicit cert issue permissions with minimum chain length = 2, chain length range = 0 (default) and end entity type = app, enrol

ITS-AID	Value (decimal)	Value (hex)	Included in RCA certificate: <please select>	SSPValue (Hex) <please add the requested values accordingly>	Bitmask (Hex) <please add the requested values accordingly>
CA Basic service	36	24	<input type="checkbox"/>		
DEN Basic service	37	25	<input type="checkbox"/>		
TLM service	137	89	<input type="checkbox"/>		
RLT service	138	8a	<input type="checkbox"/>		
IVI service	139	8b	<input type="checkbox"/>		
TLC Request Service	140	8c	<input type="checkbox"/>		
GeoNetworking Management Communications (GN-MGMT)	141	8d	<input type="checkbox"/>		
Secured certificate request service	623	26f	<input type="checkbox"/>		
TLC Status Service	637	27d	<input type="checkbox"/>		
CP Service	639	27f	<input type="checkbox"/>		
POI Service	1619	653	<input type="checkbox"/>		
<insert any comments here>					

<Please tick the additional check boxes below>.

☐ I confirm that no other ITS-AID is used in this RCA Certificate.

☐ I confirm that under this RCA Certificate only C-ITS service ITS-AIDs are operated that are in compliance with the versions of standards listed in the CPOC Protocol, Annex I, Table 4.

☐ I confirm that this RCA Certificate complies with the rules set out in the CPOC protocol Annex I, and in particular that none of the ITS-AID permissions exceeds the maximum permissions defined in CPOC Protocol, Annex I, Table 5.

IV.4. RCA Link Certificate Message Information

This chapter is only to be filled in case RCA Link Certificate Messages are used.

<Please fill in the following table:>

Type of intended RCA Re-key operation RCA	<p><i><Please select the type of the intended RCA certificate re-key operation.</i></p> <p><i>Re-key Option 1 refers to the simple case of expiry of the validity period of the RCA certificate: the RCA does a re-key simply due to expiry of the old RCA certificate. No changes in the "ToBeSignedCertificate" (except validity), that means that also no change to CertificateID shall be done.</i></p> <p><i>Re-key Option 2 refers to ANY intended change beyond the validity of the 'ToBeSignedCertificate' of the re-keyed new self-signed RCA Certificate, compared to the previous RCA Certificate. Any such change requires CPA approval, and hence the filling in of this table. If granted, e.g. the CertificateID could (like all other fields) also be changed.></i></p> <p>Re-key Option 1: No change in RCA Certificate, except validity period. No CPA approval needed.</p> <p>Re-key Option 2: Request for changes in the RCA certificate, hence requiring CPA approval.</p>	
CertificateIDs	Existing RCA certificate	New RCA certificate
	<p><i><please insert here the RCA CertificateID of the already existing RCA Certificate in the EU CCMS to which the linkage shall be created>.</i></p>	<p><i><please select if the CertificateID has changed in the new RCA CertificateID></i></p> <p>No change, same as existing RCA CertificateID.</p> <p>Changed CertificateID:</p> <p><i><if the RCA CertificateID has changed, please insert the new Certificate ID here></i></p> <p><i>In case you intend to change the RCA CertificateID, and you do not know your <CPA-ID> component of the CertificateID, you have to please notify</i></p>

		<i>the CPA of your intended new <RCA-NAME> before you are able to finalise and send this form.></i>
Digital fingerprints (i.e. SHA-256 / SHA-384 Hash) of the existing and new RCA certificate	Existing RCA certificate	New RCA certificate
	<i><please insert here the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate here that is already on the ECTL. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384></i>	<input type="checkbox"/> SHA-256 of RCA Certificate <input type="checkbox"/> SHA-384 of RCA Certificate <i><please select the applicable checkbox ></i> <i><please insert here the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.></i>
Cryptographic information	<i><please select which cryptographic algorithm and key length was used in the new RCA certificate></i> <input type="checkbox"/> ECDSA_nistP256_with_SHA 256 <input type="checkbox"/> ECDSA_brainpoolP256r1_with_SHA 256 <input type="checkbox"/> ECDSA_brainpoolP384r1_with_SHA 384	
DC URL	<i><please insert the DC URL of the new RCA certificate></i>	

<Please use the following template tables to indicate the permissions of the new RCA certificate that is linked to an existing RCA Certificate according to the definitions in the tables in CPOC Annex I, chapter I.4.

Please select the column "is different" if the permission is different than in the already existing RCA Certificate that it links to. For any differences or new permissions, please list the SSPvalue and Bitmask.>

<Please select the following check-boxes and list all set app permissions below.>

App Permissions					
ITS-AID	Value (decimal)	Value (hex)	Is different <i><please select></i>	Included in new RCA certificate: <i><please select></i>	SSPValue (Hex) <i><please add the requested values accordingly></i>
CRL service	622	26e	<input type="checkbox"/>	<input type="checkbox"/>	

CTL service	624	270	<input type="checkbox"/>	<input type="checkbox"/>	
<p><insert any comments here></p>					

<Please select the following check-boxes and list all set cert issue permissions of the new RCA certificate that is linked to an existing RCA Certificate. Please document the minimum chain length, chain length range and entity type used in the cert issue permission element. In case multiple cert issue permission elements with different chain length values are used please indicate in the tables below accordingly.>

Explicit cert issue permissions with minimum chain length = 1 (default), chain length range = 0 (default) and end entity type = app (default)						
ITS-AID	Value (decimal)	Value (hex)	Is different <please select>	Included in new RCA certificate: <please select>	SSPValue (Hex) <please add the requested values accordingly>	Bitmask (Hex) <please add the requested values accordingly>
Secured certificate request service	623	26f	<input type="checkbox"/>	<input type="checkbox"/>		
<p><insert any comments here></p>						

Explicit cert issue permissions with minimum chain length = 2, chain length range = 0 (default) and end entity type = app, enrol						
ITS-AID	Value (decimal)	Value (hex)	Is different <please select>	Included in new RCA certificate: <please select>	SSPValue (Hex) <please add the requested values accordingly>	Bitmask (Hex) <please add the requested values accordingly>
CA Basic service	36	24	<input type="checkbox"/>	<input type="checkbox"/>		
DEN Basic service	37	25	<input type="checkbox"/>	<input type="checkbox"/>		

TLM service	137	89	<input type="checkbox"/>	<input type="checkbox"/>		
RLT service	138	8a	<input type="checkbox"/>	<input type="checkbox"/>		
IVI service	139	8b	<input type="checkbox"/>	<input type="checkbox"/>		
TLC Request Service	140	8c	<input type="checkbox"/>	<input type="checkbox"/>		
GeoNetworking Management Communications (GN-MGMT)	141	8d	<input type="checkbox"/>	<input type="checkbox"/>		
Secured certificate request service	623	26f	<input type="checkbox"/>	<input type="checkbox"/>		
TLC Status Service	637	27d	<input type="checkbox"/>	<input type="checkbox"/>		
CP Service	639	27f	<input type="checkbox"/>	<input type="checkbox"/>		
POI Service	1619	653	<input type="checkbox"/>	<input type="checkbox"/>		
<i><insert any comments here></i>						

<Please tick the additional check boxes below>.

- ☐ I confirm that no other ITS-AID is used in this RCA Certificate.
- ☐ I confirm that under this RCA Certificate only C-ITS service ITS-AIDs are operated that are in compliance with the versions of standards listed in the CPOC Protocol, Annex I, Table 4.
- ☐ I confirm that this RCA Certificate complies with the rules set out in the CPOC protocol Annex I, and in particular that none of the ITS-AID permissions exceeds the maximum permissions defined in CPOC Protocol, Annex I, Table 5.

IV.5. Optional: eIDAS Information

In line with the CPOC Protocol the RCA has the possibility to inform the CPA and the CPOC/TLM on eIDAS related information in case the RCA wants to make use of the respective revocation flow possibilities in case of urgencies (i.e. revoking RCA certificates without physical presence to Commission premises in Ispra, Italy).

RCA AR eIDAS compliant Digital Certificate(s)	<p><i><please select the purpose/capabilities of the RCA AR eIDAS compliant Digital Certificate(s)></i></p> <p><input type="checkbox"/> PDF Digital Signature</p> <p><input type="checkbox"/> E-mail (s/mime) Signature</p> <p><i><please insert the details on the eIDAS compliant Digital Certificate(s) of the AR to be used for PDF/E-mail Security></i></p> <p><i><the eIDAS compliant Digital Certificate(s) of the AR to be used shall at least contain the Company name, the AR name and AR company e-mail address used in the enrolment form.></i></p>
RCA AR eIDAS compliant Digital Certificate(s) provider:	<p><i><please insert the details on the eIDAS compliant Trust Services provider. This provider shall be listed in one of the eIDAS trusted lists.></i></p>

IV.6. Personal data processing

The processing of the personal data provided in this form and its attachments is covered by a declaration of confidentiality on the protection of personal data. These declarations can be found here:

- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00744>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-01239.2>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00406>

Please consult these declarations before filling, signing and submitting the form.

IV.7. Date and Signature

RCA Application Form ID	<p><i><please insert the RCA Application ID></i></p>
-------------------------	--

I, *<insert name>* as the RCA authorised representative of *<insert RCA organisation name>* request to add the RCA Certificate with the following hashvalue to the ECTL:

<p><i><please insert the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.></i></p>
--

Date and Place:

Signature of RCA authorized representative:

Stamp (optional):

IV.8. Attachments to the RCA Application Form

The RCA organisation shall attach a copy of the following documents to the RCA Application Form:

- Documents that describe the type(s) of supported C-ITS Stations, the related services and use cases and the corresponding messages profiles according to Annex I - section I.4 that justify the request for each type of permissions, including the description of permissions management by the PKI service provider.

Annex V. RCA Application Approval Form

This RCA Application Approval form shall be filled-in by the CPA after receiving the RCA Application Form. The RCA Application Approval form shall be printed and signed (digitally or on paper) by the CPA authorised representative. If the form is signed on paper, it shall be scanned and turned into a PDF by the CPA. The form shall be securely submitted back to the RCA and CPOC-ENTRY/TLM.

For each received RCA Application Form an own RCA Application Approval Form shall be filled-in, signed and submitted.

V.1. Summary of the received RCA Application Form

The CPA has received an RCA Application Form on *<insert date>* by the identified organization *<insert organisation>*. The received RCA application form had the RCA Application Form ID *<insert corresponding RCA Application Form ID>*.

V.2. CPA assessment of the received RCA Application Form

The CPA has assessed the RCA application form with the Application Form ID *<insert corresponding RCA Application Form ID>* and its attachments.

<insert CPA process, short summary of date of meeting, comments, etc. >

V.3. CPA approval of the RCA application form

Based on the receipt of the RCA application form with the ID *<insert corresponding RCA Application Form ID>* and the conducted CPA assessment, the CPA

<mark relevant box >

☐ herewith approves the RCA application form and will inform the applicant RCA and the CPOC/TLM accordingly.

☐ rejects the RCA application form and will inform the applicant RCA and the CPOC/TLM accordingly.

Comments / Recommendations:

<add any comments or recommendations>

Date and Place:

Name of CPA authorized representative:

Signature of CPA representative:

Stamp (only if applicable):

Annex VI. RCA Revocation Form

This RCA revocation form shall be filled-in by the RCA to request revocation of an RCA Certificate that is part of the EU CCMS. The RCA revocation form shall be digitally signed or printed and signed on paper by the RCA authorised representative. If signed on paper, it shall be scanned and turned into a PDF by the RCA before its transmission to the CPA and CPOC.

For each RCA Certificate that shall be revoked from the ECTL an own RCA Revocation Form shall be filled-in, signed and submitted.

How to use this template:

Please fill in all fields that are marked with *<instructions>*:

- *<insert>* text fields: please directly enter text and delete all blue instructions. Fill with “n/a” if not applicable.
- Checkboxes ☐: please replace ☐ with X to “select” them. Leave ☐ if checkbox is not applicable.
- No part of the form (tables, fields to be filled, etc.) is allowed to be changed by the applicant – should you experience problems, contact the CPA first.

VI.1. Identity of the organisation and registration information

<Please fill in the following table:>

RCA Revocation Form ID	<i><please insert the RCA Revocation Form ID here></i> <i>Note: The RCA Revocation Form ID shall match the approved RCA Application Form ID corresponding to the certificate that has to be revoked and removed from the ECTL. Only the term “Application” shall be replaced by “Revocation” to create the corresponding RCA Revocation Form ID.</i> <i>Example 1</i> <i>If the RCA Application Form ID of the RCA certificate that is to be revoked was “2_RCA-Application-Form_1” the corresponding RCA Revocation Form ID shall be:</i> 2_RCA-Revocation-Form_1 <i>Example 2</i> <i>If the RCA Application Form ID of the RCA certificate that is to be revoked was “5_RCA-Application-Form_2” the corresponding RCA Revocation Form ID shall be:</i> 5_RCA-Revocation-Form_2
------------------------	---

<Please fill in the following table:>

RCA Organisation Name	<please insert the legal entity name responsible for the RCA operation here>
Postal Address	<please insert the full postal address of the RCA organisation here, including street, number, city, postal code, country and/or any other relevant information for postal mail>
Name of the authorised representative in the RCA organisation	<please insert the name of the physical contact person of the RCA organisation here, who signs this RCA application>
e-mail address of the AR in the RCA organisation	<please insert the e-mail address of the physical contact person here>
Telephone number of the contact person in the RCA organisation	<please insert the telephone number of the physical contact person here>

VI.2. Selection of the applicable RCA Revocation Scenario

<Please select the appropriate type of RCA revocation scenario >

Type of RCA Application	<p><In case of a compromise or suspected compromise of a RCA system please select either revocation scenario 1a or 1b.</p> <p>In case the revocation is not due to a compromise or suspected compromise: please select either revocation scenario 2, 3 or 4></p> <p><input type="checkbox"/> Revocation Scenario 1a: The incident is not considered of critical importance by the RCA management entity and/or the CPA. → <i>proceed with chapter 0 and VI.6</i></p> <p><input type="checkbox"/> Revocation Scenario 1b : If the incident the compromise or suspected compromise is considered of <u>critical importance</u> by the RCA management entity and/or the CPA , the removal of the associated RCA certificate from the ECTL should shall be executed as soon as possible. → <i>proceed with chapter VI.4 and VI.6</i></p> <p><input type="checkbox"/> Revocation Scenario 2: The need to upgrade an entire certificate chain's cryptographic algorithm type/strength → <i>proceed with chapter 0 and VI.6</i></p>
-------------------------	--

	<input type="checkbox"/> Revocation Scenario 3: Activities originating from an organizational, industry or regulatory change to the C-ITS trust model or new policies that warrant root certificate replacement. → <i>proceed with chapter 0 and VI.6</i> <input type="checkbox"/> Revocation Scenario 4: RCA managing entity exiting the market. → <i>proceed with chapter 0 and VI.6</i> <input type="checkbox"/> other: <i>first contact the CPA</i>
--	--

VI.3. Revocation Scenario 1a, 2, 3 and 4

VI.3.1. RCA Certificate Information of the self-signed RCA ETSI103097Certificate that is to be revoked

<Please fill in the following table:>

Digital fingerprint (i.e. hashvalue) of the RCA certificate	<i><please insert the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate that is to be revoked here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.></i>
RCA CertificateID	<i><please insert here the RCA CertificateID, in-line with the definitions of the CPOC Protocol, Annex I, chapter business telephone number of the RCA authorised representative . of the RCA certificate that is to be revoked></i>
Indicate date and time of intended revocation of RCA certificate	<i><please choose one of the options and indicate the earliest requested datetime when the RootCA Cert may be removed from the ECTL></i> <input type="checkbox"/> The RCA certificate shall be revoked at the next regular scheduled ECTL signing session of the TLM. <input type="checkbox"/> The RCA certificate shall be revoked at one of the next regular scheduled ECTL signing session of the TLM, but not earlier than <i><insert date and time here></i> and not later than <i><insert date and time here></i> .

VI.4. Revocation Scenario 1b (critical importance)

VI.4.1. RCA Certificate Information of the self-signed RCA ETSI103097Certificate that is to be revoked

<Please fill in the following table:>

Digital fingerprint (i.e. hashvalue) of the RCA certificate	<i><please insert the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate that is to be revoked here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.></i>
---	---

RCA CertificateID	<please insert here the RCA CertificateID, in-line with the definitions of the CPOC Protocol, Annex I, chapter I.3.2.2. of the RCA certificate that is to be revoked>
Indicate date and time of intended revocation of RCA certificate	<please tick the box below and confirm> <input type="checkbox"/> I confirm that the RCA Certificate revocation is of critical nature and shall hence be revoked by the TLM from the ECTL as soon as possible and without undue delay.

VI.5. Personal data processing

The processing of the personal data provided in this form and its attachments is covered by a declaration of confidentiality on the protection of personal data. These declarations can be found here:

- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00744>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-01239.2>
- <https://ec.europa.eu/dpo-register/detail/DPR-EC-00406>

Please consult these declarations before filling, signing and submitting the form.

VI.6. Date and Signature

RCA Revocation Form ID	<please insert the RCA Revocation Form ID>
------------------------	--

I, <insert name> as the RCA authorised representative of <insert RCA organisation name> request to remove the RCA Certificate with the following hashvalue off the ECTL:

<please insert the hashvalue (HEX) of the RCA self-signed ETSI103097Certificate here. If the certificate has a 256-bit key, the hash shall be generated with SHA-256. If the certificate has a 384-bit key, the hash shall be generated with SHA-384.> .

Date and Place:

Signature of RCA authorized representative:

Stamp (optional):

VI.6.1. IN ADDITION ONLY IN CASE OF Revocation Scenario 1b (critical importance): eIDAS signature

The Form needs to be signed using eIDAS according to the information that was provided in the RCA Application Form of the relevant RCA certificates that are subject to revocation.

RCA AR eIDAS compliant Digital Certificate(s)	<p><i><please select the purpose/capabilities of the RCA AR eIDAS compliant Digital Certificate(s)></i></p> <p><input type="checkbox"/> PDF Digital Signature</p> <p><input type="checkbox"/> E-mail (s/mime) Signature</p> <p><i><please insert the details on the eIDAS compliant Digital Certificate(s) of the AR to be used for PDF/E-mail Security></i></p> <p><i><the eIDAS compliant Digital Certificate(s) of the AR to be used shall at least contain the Company name, the AR name and AR company e-mail address used in the enrolment form.></i></p>
RCA AR eIDAS compliant Digital Certificate(s) provider:	<p><i><please insert the details on the eIDAS compliant Trust Services provider .This provider shall be listed in one of the eIDAS trusted lists ></i></p>

Annex VII. RCA Revocation Approval Form

This RCA revocation approval form shall be filled-in by the CPA to approve RCA revocation forms sent by RCAs. The RCA revocation approval form shall be printed and signed by the CPA authorised representative. It shall be scanned and turned into a PDF by the CPA and transmitted to the RCA and CPOC.

For each RCA Revocation Form an own RCA Revocation Application Form shall be filled-in, signed and submitted.

VII.1. Summary of the received RCA Revocation Form

The CPA has received an RCA Revocation Form on *<insert date>* by the identified organization *<insert organisation>*. The received RCA application form had the RCA Revocation Form ID *<insert corresponding RCA Revocation Form ID>*.

VII.2. CPA assessment of the received RCA Revocation Form

The CPA has assessed the RCA revocation form with the RCA Revocation Form ID *<insert corresponding RCA Revocation Form ID>* and its attachments.

<insert CPA process, short summary of date of meeting, comments, etc. >

VII.3. CPA approval of the RCA revocation form

Based on the receipt of the RCA revocation form with the ID *<insert corresponding RCA Revocation Form ID>* and the conducted CPA assessment, the CPA

<mark relevant box >

☐ herewith approves the RCA revocation form and will inform the applicant RCA and the CPOC/TLM accordingly.

☐ rejects the RCA revocation form and will inform the applicant RCA and the CPOC/TLM accordingly.

Comments / Recommendations:

<add any comments or recommendations>

Date and Place:

Name of CPA authorized representative:

Signature of RCA CPA representative:

Stamp (only if applicable):

Annex VIII. EU CCMS Levels & Requirements

VIII.1. Scope

This annex is an outcome of the work of the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941).

In order to support deployment of C-ITS services in Europe, three different environments (i.e. Levels) for the EU CCMS are defined. These levels are hierarchically ordered from L0 up to L2 and enable a secure deployment of C-ITS services that should guarantee a smooth rollover to a fully CP compliant EU CCMS (from a testing phase L0, to a near compliant L1 up to a full CP compliant system L2). As deployment shall move to the final and CP/SP compliant operation environment (L2), the other two environments (L0 and L1) are limited in time.

This report aims to describe these different EU CCMS Levels and their requirements that shall be followed by all C-ITS participants in the EU CCMS in order to support the initial setup phase and future regular operations of C-ITS in Europe. Hereby the basis of the securely operating C-ITS stations is their general adherence to the defined and agreed system profiles for the respective C-ITS stations.

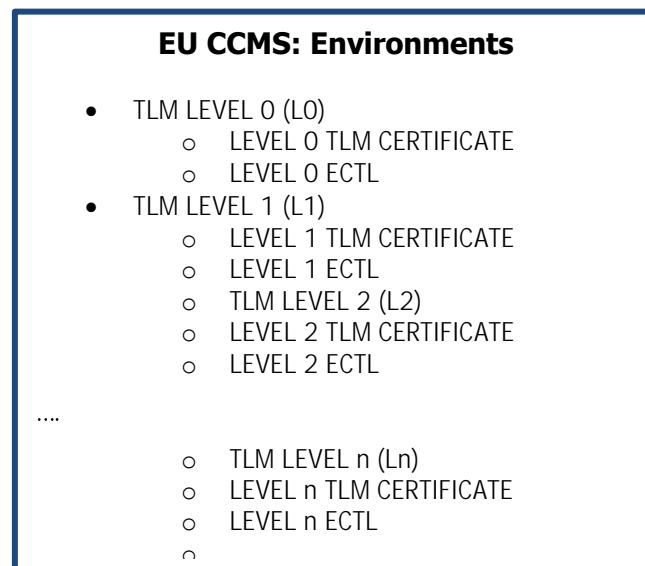
This Annex does not intend to specify, e.g. by replacing or extending, requirements that are already provided in the CP/SP, and does not define technical requirements for C-ITS stations or system functionalities, which are contained in protection profiles or system profile documents of C-ITS stations.

VIII.2. Definition of EU CCMS Levels

VIII.2.1. Overview of the Levels

This Annex describes three different Levels of trust in the EU CCMS that shall be useable for different purposes in the EU CCMS. These three levels, which sequentially follow on the way from testing single C-ITS stations to regular operations of large and distributed C-ITS networks, and respective TLM Environments are described in this section as shown in Figure 7.

Figure 7: Overview of the different EU CCMS Environments and their relation to TLM/ECTL



The different ECTLs will contain corresponding L0, L1 or L2 RCA certificates, i.e. it shall be ensured that for each EU CCMS level the corresponding TLM certificates, ECTLs and RCA certificates are used (see Figure 7). The number of levels is extensible and additional levels Ln (with $n > 2$) can be added in future.

Future level(s) Ln (with $n > 2$) can be added in the EU CCMS and used for certified production operation of C-ITS stations and PKI implementations fulfilling stricter requirements than L(n-1). Any additional Ln (with $n > 2$) is expected to be based on the level of trust in the (n-1) environment, plus additional added

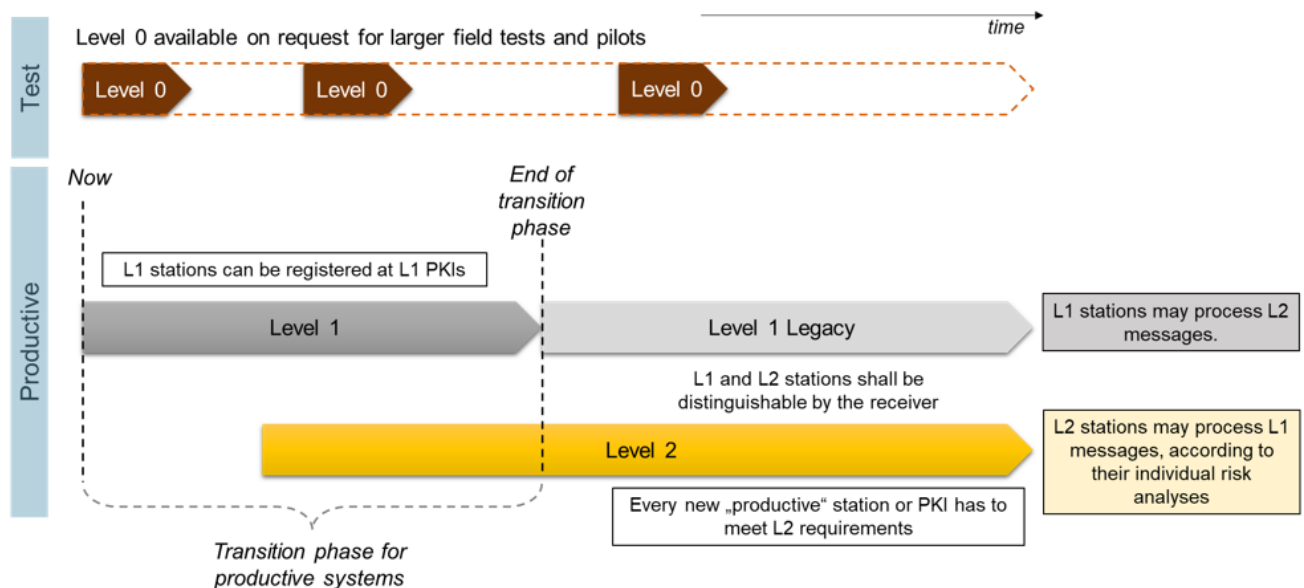
requirements. These levels may be for example needed in future to address the requirements for trust in cooperative automated driving systems.

Before additional levels L_n (with $n > 2$) can be introduced, the required process to do so as well as the additional requirements for L_n (with $n > 2$) shall be assessed by the CPA, e.g. with respect to the impact on existing PKI and station implementations.

L_0 is intended for testing C-ITS stations, L_1 is an interim environment for the ramp-up phase of C-ITS deployment and L_2 provide the environment for production C-ITS stations. Though not mandatory, it is recommended that operators of C-ITS stations aiming to deploy C-ITS Day 1 services within the EU CCMS should follow a sequential enrolment in testing and later production environments. That means they should first enrol a set of test C-ITS stations in an L_0 environment for testing purposes and only after successful testing on L_0 , the next step should be to enrol them on L_1 or L_2 . It should be noted, that general testing of C-ITS stations does not require L_0 enrolment, and the L_0 environment targets interoperability tests between C-ITS stations enrolled at different PKIs. Thus, the L_0 trust list will be made available for larger field tests and pilots.

L_1 and L_2 (and future L_n with $n > 2$) provide production environments. L_1 is intended for C-ITS stations which are not fully compliant to the CP yet in a ramp-up phase of C-ITS service deployment in the EU CCMS. These C-ITS stations types can be enrolled to L_1 within a transition phase. After the end of the transition phase, L_1 stations either move on to the full production environment L_2 once their full compliance to the CP is certified. If the required full compliance to the CP is not met, then the L_1 stations stay on the L_1 level and form the “ L_1 legacy” track. L_1 Legacy is only intended to enrol stations of types/models placed on the market before the end of the transition phase. After the end of the transition phase, the testing on L_0 and then directly moving to L_2 may be sufficient for the purpose of C-ITS Day 1 services. Any future revisions of the scope of the Levels shall be defined by the CPA.

Figure 8: Overview and timeline of ECTL levels



Note: Due to the parallel operation of L_1 (incl. L_1 legacy) and L_2 , there will be the situation that C-ITS messages are sent by L_1 -enrolled C-ITS stations or L_2 -enrolled C-ITS stations, which differ in their security level.

A receiver can filter for or distinguish between L_1 and L_2 message sources in the following way:

- 1) import only wanted trust list (L_1 or L_2 or L_1+L_2). If only one trust list is imported, then the further distinction between L_1 and L_2 message is not needed.
- 2) distinguish by certificate chain (certificate in received message belongs to L_1 or L_2 hierarchy).

Table 14: Treatment of L1 and L2 messages on the receiver side

Receiving Level 1 messages	Receiving Level 2 messages
<ul style="list-style-type: none"> For stations processing Level 1 messages, the risk analysis shall consider the exceptions for Level 1, which may have an impact on message integrity and message authentication. 	<ul style="list-style-type: none"> Received Level 2 messages are processed as defined in Certificate and Security Policy. Risk management as defined in the Security Policy.
<ul style="list-style-type: none"> Example: Level 1 messages could be used for information only or for statistics, while Level 2 messages could directly trigger traffic management actions, such as speed limit reduction etc. Note: A mere display to the driver is not considered a safety risk according to ISO 26262 Note: There could always be wrong sensor information, independent of the cybersecurity requirements. Plausibility checks might be required in any case. 	

VIII.2.2. Level 0 (LO)

The LO environment in the EU CCMS shall be used for competence-building towards C-ITS security standards and technical requirements conformity of C-ITS station and PKI implementations.

LO is offered by the TLM/CPOC on the basis of requests for interoperability testing sessions to the TLM by single stakeholders or groups of stakeholders participating in a specific test session (e.g. C-Roads interoperability test sessions, etc.).

LO shall be offered for short testing intervals, limited in time as agreed upon registration of any PKI participants.

In order to test interoperability, the TLM shall include all such test LO RCA certificates in a "LEVEL 0 ECTL (LO ECTL)", signed by a "Level 0 TLM Certificate (LO TLM Certificate)".

In the beginning of C-ITS deployment in the EU, the LO ECTL will be used for the scope of C-ITS Day 1 services and tested according to selected and agreed single use cases and basic C-ITS messages. In the future, when operators have "moved on" to higher levels (L1, L2), the LO ECTL process could be used for specific other future purposes, such as future C-ITS services (e.g. Day 2 services, other permissions, etc.) or cross-certification tests of the EU CCMS with other trust domains, subject to future revision of this Annex by the CPA.

The administration process for the LO ECTL shall be simplified and centralized at CPOC/TLM level without CPA intervention. Hence, the CPOC/TLM will define the scope of each LO TLM/ECTL signing session with the testing stakeholders on a case by case basis of C-ITS Day 1 services. The CPOC/TLM shall regularly report to the CPA on the status and achievements (i.e. learnings of the TLM/CPOC in operations, list of Root CAs enrolled, etc.) of the LO level.

VIII.2.3. Level 1 (L1) (including L1 Legacy)

The L1 environment in the EU CCMS shall be used to align C-ITS implementation to the CP/SP and CPOC protocol processes and approach full compliance. The requirements and processes in order to access L1 and L1 legacy are intermediate steps towards compliance against the CP/SP. The limited exceptions and operation scope are governed by the CPA and defined in detail in chapter VIII.3.2.

If RCAs are listed on L1, the Sub-CAs and C-ITS stations shall meet the L1 requirements and operate C-ITS Day 1 services and perform their functionalities in regular and well defined operation periods. The CPA instructs the TLM to operate such L1 environment based on these requirements and scope of such operations.

L1 for the support of C-ITS Day 1 services is intended for a transition phase up until the end of the year 2025. The transition phase is intended to allow 2 years product development and certification. After the end of the transition phase all production C-ITS Day 1 service deployments shall move to L2. Those stations formerly enrolled on L1 that fulfil L2 requirements should whenever possible migrate to L2. Those C-ITS stations which cannot fulfil L2 requirements remain as legacy equipment on L1 and form the "L1 legacy" track if they meet all L1 legacy requirements as specified in chapter 3.2. All stations of types/models placed on the market after

the end of the transition phase, shall not be enrolled on L1, but only on L2, where full compliance to the certificate policy is required.

The TLM includes all such L1 certificates on a "Level 1 ECTL (L1 ECTL)", signed by a "Level 1 TLM Certificate (L1 TLM Certificate)", if the requirements of L1 mentioned in chapter VIII.3.2 are fulfilled. There shall only be one such L1 TLM Certificate and corresponding L1 ECTL valid in the EU at the same time.

Note: In the ramp-up phase of C-ITS service deployment in the EU CCMS the L1 ECTL will be used predominantly for the scope of C-ITS Day 1 services [6] and station functionalities following the definitions of the CP, SP and CPOC Protocol Annexes. The scope, timing, requirements and exceptions granted for L1 may be revised at any time by the CPA by instructing the CPOC to update this Annex, whereas a revision shall happen in any case towards the end of the transition phase (end of 2025).

VIII.2.4. Level 2 (L2)

The L2 environment in the EU CCMS shall be used for certified production operation of C-ITS station and PKI implementations according to [7] and [8]. The L2 environment is hence equivalent to compliance to all EU CCMS requirements, based on the CP, SP and CPOC. The requirements to access are detailed in chapter VIII.3.3.

The TLM includes all such L2 RCA certificates using a "Level 2 ECTL (L2 ECTL)", signed by a "Level 2 TLM certificate (L2 TLM Certificate)", if the requirements of L2 mentioned in chapter VIII.3.3 are fulfilled. There is only one such L2 TLM Certificate and corresponding L2 ECTL valid in the EU CCMS at the same time.

VIII.3. Access criteria, needed achievements & other considerations on Levels

The following table gives an overview of the access criteria, needed achievements and other considerations of the three defined Levels in the EU CCMS, which are then for some aspects further detailed in the consecutive sections.

Table 15: Overview of requirements of the three EU CCMS Levels

Level	Goal	Access criteria (organizational criteria)	Achievement needed (technical criteria)
L0	Competence-building towards standard and technical requirements conformity based on publicly available system profiles	<ul style="list-style-type: none"> <u>RCA access to TLM</u>: Legal existence of RCA operator (proof of registration according to CP Section 3.2.2.1) <u>Sub-CAs access to RCA</u>: Legal existence <u>Stations access to Sub-CAs</u>: Legal existence of station operator, declaration of standards conformity 	<p><u>CAs</u>: Full conformity with all relevant standards (self-declaration)</p> <p><u>Stations</u>: Full conformity with all relevant standards for interoperability and respective system profiles of stations (self-declaration).</p> <p>Note: Exceptions from conformity to standards and profiles can be made on Level 0 only to allow testing of new message types (facilities layer).</p>
L1	Alignment to CP/SP processes and approach towards full station certification. L1 legacy to allow operation where L2	<ul style="list-style-type: none"> See L2 access criteria and exceptions for Level 1 (see Table 16 for necessary deliverables) 	<p><u>CAs</u>: Compliance to CP with exceptions defined in the Level 1 table of exceptions (see Table 16T).</p> <p><u>Stations</u>:</p> <ul style="list-style-type: none"> Full conformity with all relevant standards for interoperability and respective system profiles of stations (self-declaration)

	cannot be reached, but L1 fulfilled.		<ul style="list-style-type: none"> Compliance to CP, SP with the exceptions defined in the Level 1 table of exceptions (see Table 16).
L2	Certified production operation	<ul style="list-style-type: none"> <u>RCA access to TLM</u>: according to CP <u>Sub-CAs access to RCA</u>: according to CP <u>Stations access to Sub-CAs</u>: certification of compliance to SP, declaration of standards conformity 	<p><u>CAs</u>: Full compliance to CP</p> <p><u>Stations</u>:</p> <ul style="list-style-type: none"> Full conformity with all relevant standards for interoperability and respective system profiles of stations (self-declaration) Compliance to all specific L2 CP, SP and PP requirements defined by the CPA

For all stations, an active service contribution is expected, and interaction among stations requires interoperability for the implemented use cases. Those interoperability requirements are specified in profiles. Thus, the standards conformance needed shall be declared based on relevant profiles, i.e. Car 2 Car Communication Consortium - Basic System Profile [7], or C-ROADS Harmonised C-ITS specifications for Europe [8]. Further profiles can be agreed on by the CPA.

The authorization to access and operate solutions in the L1 trust domain is granted against the user's commitment to comply with the rules defined in the present document. In case of misuse evidences, the user's authorization can be withdrawn. The CPA may review and decide to modify, cancel or add any Level 1 exception. Such modifications will be applicable to all Level 1 users without derogations.

VIII.3.1. Details of L0 access criteria & achievements needed

Basis of the access criteria are publicly available and well documented system profiles for the participating stations, which make it possible to compare the implemented security elements at this level. The services or functions used to demonstrate these can be selected and agreed day 1 services implemented in road side or vehicle stations complying with the full set of involved standards.

No CP/SP audit and certification is needed for CAs/C-ITS stations to access the L0 Environment. No specific checks on permissions are performed by the CPOC when receiving LO RCA Certificates, hence no full compliance to the CP/SP and CPOC protocol is needed. However, the syntactical and logical correctness (e.g. validity) of the certificates and service specific permissions is in principle checked. (Note: the level of detail of checks may vary in the setup-phase of the L0 and L1 Environment and is expected to gradually increase over time, i.e. once the defined L1 Environment checks are fully implemented by the CPOC, they may also be applied for L0 to inform PKI participants with feedback on the quality of their L0 Certificates).

VIII.3.2. Details of L1 access criteria & achievements needed

Level 1 aims at real C-ITS stations using the service through active C-ITS vehicles and road infrastructure. PKI security and privacy must be fully guaranteed. Active C-ITS service contributions are needed, i.e. sending and receiving of standard day 1 C-ITS messages.

In order to be granted access to the EU CCMS L1 environment all C-ITS stations and PKI related entities need on the basis of the L0 requirements also to comply with the set of requirements of the CP, SP and CPOC protocol for C-ITS Day 1 service deployment. However, since the purpose of the L1 environment is to help bridge C-ITS implementations which are not yet fully compliant towards full compliance in the ramp-up phase of C-ITS Day 1 Services, not necessarily all requirements of the CP, SP and CPOC protocol apply at L1. The following exceptions to access criteria and requirements shall apply for L1:

Table 16: Level 1 Exceptions

Item	Scope	Reference	Level 1 Exception during transition phase	Level 1 Legacy after transition phase
1	C-ITS station, CC certification	Security Policy, Requirement (25)	<p>An evaluation of the C-ITS station shall be performed by a SOG-IS recognized test lab.</p> <p>The test lab shall evaluate that the C-ITS station is protected against an attacker with basic attack potential and therefore perform at least the Level 1 Evaluation Tasks in Section VIII.3.2.1. A positive evaluation report shall be provided by the station operator to the EA for registration.</p>	Same exception, only for the stations of types/models placed on the market before the end of the transition phase.
2a	C-ITS station, Secure Element (Option a)	Certificate Policy, Requirement (324)	<p>The manufacturer of the secure element shall be certified according to ISO 27001.</p> <p>The hardware platform of the secure element shall have achieved Common Criteria certification.</p> <p>According to certified protection profiles of at least EAL level 4. This comprises the hardware as well as the on-chip software (firmware). Additional software (on top of the certified scope) and/or modifications in the software part from the certified state shall be developed following the same processes as other comparable Common Criteria certified products of the same manufacturer.</p>	Same exception, only for the secure elements of stations of types/models placed on the market before the end of the transition phase.
2b	C-ITS station, Secure Element (Option b)	Certificate Policy, Requirement (324)	<p>A SOG-IS MRA accredited certification lab was contracted. A declaration from the certification lab shall be provided by the manufacturer/operator that the corresponding Secure element certification process shall be completed before end of transition phase.</p> <p>During transition phase, periodic (at least six-monthly) progress reports from the accredited lab shall be submitted and assessed by the CPA in order to maintain L1 enrolment of the Secure element.</p>	No exception

Item	Scope	Reference	Level 1 Exception during transition phase	Level 1 Legacy after transition phase
3	C-ITS station, Validation of ECTL	CPOC Protocol, Chapter I.6.2	The update of the TLM Certificate in C-ITS stations may deviate from the process specified in Section I.6.2.1 of the CPOC protocol if the validation is done by a backend service and the submission to the C-ITS station is performed through a secured channel.	Same exception
4	C-ITS station, Protocol	Certificate Policy, References to ETSI TS 102 941 [2]	<p>Exceptions on the implemented protocol for enrolment and authorization management for C-ITS stations as well as authorization validation may be granted if the following is ensured:</p> <ul style="list-style-type: none"> - The same level of security and privacy has been certified by an accredited auditor. The certificate has to be presented to the CPA. - The interoperability with other PKIs and C-ITS stations is ensured by adhering to the certificate profiles specified for RCA, AA, and AT certificates in ETSI TS 103 097 [3]. 	Same exception
5	C-ITS station operator, ISMS	Security Policy, Requirement (1)	If a security management system according to requirement (1) of the Security Policy is not available, a comparable security management process shall be operated (e.g. national standard or equivalent to ISO 27001).	No exception
6	C-ITS station operator, Compliance Audit	Security Policy, Requirement (31), (32), (33)	The compliance audit for the Security Policy may be conducted internally by the C-ITS station operator which shall be confirmed by a self-issued statement of compliance. This statement does not shift responsibility from C-ITS station operator to the PKI operator.	No exception
7	PKI, Compliance Audit	Certificate Policy, Chapter 8	In general, it is sufficient for the access to L1, if the full compliance to the CP has been certified by an accredited auditor. A compliance audit report summary shall be provided along with the application form.	No exception, except for item 4 scope

Item	Scope	Reference	Level 1 Exception during transition phase	Level 1 Legacy after transition phase
			In case such report summary cannot be presented, a documentation along the guidelines for L1 PKIs in Section VIII.3.2.2 is required. Based on the content provided, the CPA may request additional information to grant access to L1.	
8	PKI, Root CA naming convention	CPOC Protocol, Chapter I.3.2.2	The naming convention for the CertificateID in RCA certificates as specified by the CPOC protocol is not enforced.	No exception

VIII.3.2.1. Level 1 Evaluation Tasks for the C-ITS Station

Table 17 states the Level 1 Evaluation Tasks based on Common Criteria assurance components [9] that shall be evaluated by the test lab (see Table 16, Item 1, column 3), which shall ensure that the C-ITS station is protected against an attacker with basic attack potential (cf. Section 17.1, AVA_VAN.2 in Common Criteria Part 3). The secure element that is included in the C-ITS station is not subject of this evaluation as the secure element is subject of its own evaluation (see Table 16, Item 2a and 2b). The content, which has to be delivered by the developer to the test lab for the respective Level 1 Evaluation Tasks, is stated in column 3 of Table 17. As required by the developer content for Level 1 Evaluation Task No. 32, the product-specific security functional requirements (SFRs) shall be defined by the developer to enable the security level required by the generic security objectives (SOs) for the TOE (Target of Evaluation) in Table 18. An evaluation report shall be handed out by the test lab to the developer that should at least comprise the identification of the tested product(s), the involved persons or institutions, the Level 1 evaluation tasks, and the final verdict (pass or fail). The enrolment to a Level 1 PKI requires a positive verdict (pass). In case of major releases with new security functionality of the evaluated version of the TOE, the test lab shall evaluate if the verdicts from the previous evaluation can still be assured.

Table 17: Level 1 Evaluation Tasks for the TOE of the C-ITS Station and respective Developer Content (see exception item no. 1 in Table 16)

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
1	Secure initialisation process of the TOE (e.g. Secure Boot, Runtime-Level) is sufficient	Short description of implemented mechanisms (table overview, flowchart, ...)	ADV_ARC.1.3C / 1.1E
2	Self-Protection of the TOE (physical protection, integrity protection mechanisms, ...) is sufficient	Table overview of mechanism. Tasks 2 and 3 can be analysed in conjunction	ADV_ARC.1.4C / 1.1E
3	Security Functionality cannot be bypassed (e.g. by exploiting debug		ADV_ARC.1.5C / 1.1E

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
	interfaces, causing buffer-overflows, altering boot-order, ...)		
4	Method of use and purpose of each external logical interface is described sufficiently.	Purpose and method of use for each logical interface shall be defined. Incl. Protocols, standards (RFCs etc.)	ADV_FSP.2.2C / 2.1E
5	All parameters for each external logical interface shall be described sufficiently.	External entities interact with the TOE via external logical interfaces. All parameters which might be used have to be defined.	ADV_FSP.2.3C / 2.1E
6	All actions related to the security relevant behaviour of the TOE are defined sufficiently. (e.g., access rights, used cryptographic algorithms, managed security functionality...)	For all possible actions via external logical interfaces, list all possible actions which might influence the security-relevant behaviour of the TOE.	ADV_FSP.2.4C / 2.1E
7	All possible error messages, a TOE might reply on the defined actions above are documented sufficiently and are understandable.	List all possible error messages for all actions mentioned above.	ADV_FSP.2.5C / 2.1E
8	The given developer documentation is an accurate and complete instantiation of the SFRs defined at Level 1 evaluation task no. 32.	No additional documentation necessary. Additional information is provided on request to the evaluation body	ADV_FSP.2.2E
9	For each role and interface, all accessible functions and privileges including corresponding warnings and error messages are defined.	Existing user guidance might be used. References to the corresponding sections is necessary.	AGD_OPE.1.1C / 1.1E
10	The use of all available interfaces for each user role is defined sufficiently.		AGD_OPE.1.2C / 1.1E
11	All available functions and the corresponding interface for each user role is documented sufficiently.		AGD_OPE.1.3C / 1.1E
12	All events/actions that are necessary for the security functionality are clearly defined for each user-role.		AGD_OPE.1.4C / 1.1E

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
13	All modes of operation of the TOE are defined clearly and understandably, including their consequences (e.g. secure mode, normal operation...)		AGD_OPE.1.5C / 1.1E
14	All necessary security measures defined at Level 1 evaluation task no. 31 are documented for each user role to fulfil the security objectives for the environment.		AGD_OPE.1.6C / 1.1E
15	The user guidance is clear and reasonable.		AGD_OPE.1.7C / 1.1E
16	All steps for the secure acceptance of the delivered TOE in accordance with line 25 are defined.	List of necessary steps.	AGD_PRE.1.1C / 1.1E
17	All steps for secure installation of the TOE and for the secure preparation of the environment are defined sufficiently.		AGD_PRE.1.2C / 1.1E
18	The TOE can be prepared securely for operation with the defined methods.	None	AGD_PRE.1.2E
19	The TOE is labelled with a unique reference	Unique reference for the TOE (HW+SW)	ALC_CMC.2.1C / 2.1E
20	All configuration items shall be uniquely defined.	List of all configuration items in a configuration list. Additional questions from the evaluation body possible.	ALC_CMC.2.2C (partially) / 2.1E ALC_CMC.2.3C (partially) / 2.1E
21	The configuration list includes the TOE itself, and all parts the TOE is comprised of.		ALC_CMS.2.1C (partially) / 2.1E
22	The configuration list shall uniquely identify all configuration items.		ALC_CMS.2.2C / 2.1E
23	The configuration list shall indicate the developer of the item.		ALC_CMS.2.3C / 2.1E
24	The delivery procedure (from production side until start of normal operation of the TOE) shall maintain security of the TOE. (e.g.,	List the delivery procedure.	ALC_DEL.1.1C / 1.1E

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
	seal, personal hand-over, fix transportation time...)		
25	A unique reference of the developer deliverables and the TOE itself is given.	Clear and consistent versioning of TOE and documentation for the Level 1 Evaluation Tasks.	ASE_INT.1.1C (partially) / 1.1E
26	The developer deliverables clearly identify the TOE		ASE_INT.1.3C / 1.1E
27	The developer deliverables clearly identify any necessary non-TOE hardware/software/firmware	A list of all necessary non-TOE parts with a short explanation about their objectives/tasks	ASE_INT.1.6C / 1.1E
28	All physical external interfaces are defined	Listing of all external logical interfaces	ASE_INT.1.7C (partially) / 1.1E
29	All external logical interfaces are defined	Listing of all external physical interfaces	ASE_INT.1.8C (partially) / 1.1E
30	Versioning and naming is consistent through all developer documentations	None	ASE_INT.1.2E
31	Statement of security objectives for the TOE and for the operation environment	Claim conformance to Table 18	ASE_OBJ.2.1C / 2.1E
32	All SFRs within the TOE and all SARs are defined.	Define product-specific security functionality in the TOE to realize the SOs for the TOE defined on Table 18. All SARs are defined through the Level 1 Evaluation Tasks.	ASE_REQ.2.1C / 2.1E
33	All SOs for the TOE are covered by SFRs.	Mapping of SFRs to SOs for the TOE in Table 18	ASE_REQ.2.6C / 2.1E
34	The defined SFRs sufficiently cover the SOs for the TOE defined in Table 18.	Potential questions from the evaluation body.	ASE_REQ.2.7C / 2.1E
35	The necessary SARs are clearly defined including the reason why those are chosen.	Given by the Level 1 Evaluation Tasks.	ASE_REQ.2.8C / 2.1E
36	All statements in security requirement definition is internally consistent	None	ASE_REQ.2.9C / 2.1E

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
37	All assets are clearly defined.	List of all assets	ASE_SPD.1.2C (partially) / 1.1E
38	All security objectives for the TOE from Table 18 are implemented in the TOE.	Mapping of security objectives for the TOE from Table 18 to implemented SFRs in the TOE	ASE_TSS.1.1C (partially) / 1.1E
39	All external logical interfaces are tested by the developer	Evidence that the test coverage is suitable to test all external available logical interfaces (e.g. mapping of test-cases to external interfaces)	ATE_COV.1.1C / 1.1E
40	The developer provided a developer test suite and a corresponding documentation including Test plans, expected results and actual results.	Corresponding test documentation	ATE_FUN.1.1C / 1.1E
41	The provided developer test plan identifies the tests and the scenario for performing each tests.		ATE_FUN.1.2C / 1.1E
42	The expected results show the anticipated output from a successful execution of the tests.		ATE_FUN.1.3C / 1.1E
43	All actual results are consistent with the expected ones, or an appropriate explanation for the deviations is given.		ATE_FUN.1.4C (with exception) / 1.1E
44	A TOE suitable for testing and access (physical or remote) to the test environment necessary to perform developer tests is provided to the evaluation body	Corresponding TOE and environment.	ATE_IND.2.1C / 2.1E, ATE_IND.2.2C / 2.1E
45	The evaluation body repeats a subset of developer tests	None	ATE_IND.2.2E
46	The evaluation body performs some independent tests to the TOE	None	ATE_IND.2.3E
47	The TOE does not contain any soft- or hardware parts which include relevant critical CVEs (critical according to CVSS:3.0).	Developer driven CVE analysis for all soft- and hardware parts. Commented list of known CVEs in the TOE at time of submitting the TOE to the evaluation body.	AVA_VAN.2.2E

No.	Level 1 Evaluation Tasks (E)	Developer Content (C)	Based on CC Part 3 Assurance Components (C: Content, E: Evaluation Task)
48	The evaluation body performed an independent vulnerability analysis of the TOE based on the knowledge of the TOE derived by all aspects given above.	None	AVA_VAN.2.3E
49	The evaluation body conducted penetration testing to the TOE based on identified potential vulnerabilities.	None	AVA_VAN.2.4E

Table 18: Generic Security Objectives for the C-ITS Station (TOE) and the Environment (see exception item no. 1 in Table 16)

Generic Security Objectives for the TOE	
Security Objective	Description
O.Secure_Association	<p>The TOE shall be able to establish a Secure Association (SA), i.e. a communication channel, between itself and another ITS station or certification authorities such that they can exchange messages according to set up security parameters (security configuration).</p> <p>As defined by ETSI 102 940, SA is mandatory for communication with the PKI.</p> <p>The TOE shall protect, if available, a remote administration flow, e.g. to an operator or a Traffic Control Centre, over the respective interface(s), by establishing a trusted channel.</p>
O.Message_&_Replay_Protection	<p>The TOE shall provide the following functionality:</p> <ul style="list-style-type: none"> - Authentication and integrity protection of the communication and data to external entities - Encryption of the communication is required for interfaces other than those used for C-ITS message communication between C-ITS stations. Such interfaces include Wide Area Network interfaces as well as local/remote interfaces for maintenance, if available. - Replay detection for every communication with external entities. When detecting replays, the TOE shall respond by discarding the message. <p>External entities are considered as any communication partner outside the installation environment, e.g. the vehicle or trailer.</p>

O.Function_Protection	<p>The TOE shall implement functionality to protect its security functions against malfunctions and tampering. Specifically, the TOE shall:</p> <ul style="list-style-type: none"> - implement a self-test on a regular basis, i.e. secure boot and/or checks to verify the correct operation of its components - be able to protect the V2X HSM interface from spoofing and manipulation either by physical or logical methods - perform plausibility checks of data imported from external sources (where applicable), especially for sensor data for time and position - ensure that the TOE fails into a secure state in case of a security relevant malfunction
O.Secure_Access	The TOE shall provide an authentication mechanism for access control to its services with different level of privileges (e.g. administrators, users, other).
O.Secure_Update	The TOE shall implement functionality for a secure firmware update. The TOE shall accept firmware updates only if their authenticity and integrity can be verified.
Generic Security Objectives for the Environment	
Security Objective	Description
OE.Secure_Initialization	The TOE should correctly and securely import or generate its V2X-relevant initial cryptographic data.
OE.TOE_Protection	It shall be ensured that the TOE is correctly mounted. Appropriate measures against theft protection and/or intervention shall be in place.
OE.Data_Reliability	All TOE operational environment data provided to the TOE for the ITS applications have to be reliable. This at least includes a reliable time and position.
OE.HSM	<p>The environment shall provide a secure element for:</p> <ul style="list-style-type: none"> - Generation of random numbers, digital signatures, and keys. - Storage of keys. - Secure deletion of private keys. <p>The secure element shall fulfil the requirements according to the corresponding ECTL Level requirements defined in this document.</p>

* The generic security objectives were derived from the Car 2 Car Communication Consortium Vehicle C-ITS Station PP [7] as of 16.04.2021 (working status) and BSI-CC-PP-0106.

VIII.3.2.2. Guidelines on Documentation for Level 1 C-ITS PKIs

The PKI operator shall at least provide the following documentation and an explanation how the documentation covers the overall C-ITS PKI service:

1. Access to L1 ECTL is only granted to RCA certificates of PKI serving well-identified European production C-ITS services. Therefore, the PKI operator shall demonstrate a sufficient level of security to guarantee that valid certificates cannot be delivered to unauthorized entities by fulfilling points 2 and 3 below.
2. The PKI operator shall present ISO 27001 certificates relevant for the C-ITS PKI service. These certificates (A CP audit report for a C-ITS PKI service is also valid) may have been obtained for other

similar services but must be applicable to the C-ITS PKI considered (e.g. involved infrastructure, key management procedures and service operation processes & team).

3. The PKI operator shall demonstrate the security of the PKI itself:
 - (a) Key management shall be compliant to the CP [1] with a relevant third-party compliance audit report by an accredited auditor. This includes in particular: key generation process (CP Section 6.1.1), private keys physical storage (CP Section 5.1, especially Section 5.1.1.1 and 5.1.2.1), segregation of duties and number of persons required per task (CP Section 5.2.2 to 5.2.4), trusted roles procedural controls (CP Section 5.2.1, CP Section 5.3), cryptographic modules used (CP Section 6.1.5.1).
 - (b) The Enrolment Authority shall have a process defined to authenticate and authorize organisations and subscribers.
 - (c) Verification of the compliance of stations to the present document's requirements shall be part of the authorization process.

VIII.3.3. Details of L2 access criteria & achievements needed

L2 represents the final level of C-ITS Day 1 Service deployment. Thus, L2 shall only be accessible if full compliance to all EU CCMS requirements, based on the CP, SP and CPOC protocol is given, including the requirements of L0.

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).

Open data from the EU

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



@EU_ScienceHub



EU Science Hub – Joint Research Centre



EU Science, Research and Innovation



EU Science Hub



@eu_science