JRC TECHNICAL REPORTS

C-ITS Point of Contact (CPOC) Protocol

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

Release 1, January 2019

EUR 29634 EN

E.3 – Cyber & Digital Citizens' Security Unit
Gianmarco Baldini, Gerhard Menzel

Joint
Research
Centre

Contact information
European Commission Joint Research Centre
E.3 – Cyber & Digital Citizens' Security Unit
Name: Gianmarco Baldini, Gerhard Menzel
Address: Via Enrico Fermi 2749
Email:
MOVE-JRC-C-ITS-POLICY-AUTHORITY@ec.europa.eu
gianmarco.baldini@ec.europa.eu
gerhard.menzel@ec.europa.eu

Tel.: +39 0332 78 6618

EU Science Hub
https://ec.europa.eu/jrc

JRC114086

EUR 29634 EN

PDF ISBN 978-92-79-99079-3 ISSN 1831-9424 doi:10.2760/77171

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: European Commission, C-ITS Point of Contact (CPOC) Protocol, JRC114086, ISBN 978-92-79-99079-3.

Contents

Acknowledgements

This technical report is based on the technical deliverable produced by OnBoard Security with the Service Contract 756189. The technical deliverable has been modified on the basis of the needs of the European Commission and the input of the stakeholders and experts, who participated to a workshop on the 15th of November 2018 in Brussels organized by DG MOVE and DG JRC, where the technical report was presented for feedback.

Executive Summary

This report describes one of the key elements of the European Union C-ITS Security Credential Management System (EU CCMS), which is going to support 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 Europe level. One of the components of the central elements is the CPOC protocol, which collects the RCAs certificates and provides them to the Trust List Manager (TLM) to create the European Certificate Trust List (ECTL). The CPOC protocol was mentioned in the C-ITS certificate policy as an item that was to be defined by the CPOC. This report has the objective to cover the definition of the CPOC protocol.

The content provided in this report is based on the technical deliverable provided by OnBoardSecurity on the basis of JRC Service Contract 756189. The technical deliverable has been assessed by various stakeholders and discussed in a workshop of 15th of November 2018 in Brussels, Belgium. The technical report also summarizes the key comments provided by the stakeholders. The scope of this report is the definition of the CPOC protocol between the RCAs and the CPOC Entry.

This report may be revised in the implementation process of the EU CCMS based on the needs of the C-ITS stakeholders.

Acronyms and 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
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
RCA	Root Certification Authority
RCA AR	Root Certification Authority Authorised Representative
TLM	Trust List Manager

1 Introduction

On 30th of November 2016 the Commission adopted a Commission Communication: "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" (COM (2016) 766). Regarding C-ITS security the communication has foreseen a number of important actions to enable deployment of C-ITS services in Europe by 2019.

One of the key actions of the strategy is the design and implementation of a European Union C-ITS Security Credential Management System (EU CCMS) for C-ITS messages. The implementation of an EU CCMS is urgently needed for European C-ITS deployments, both in a first learning and testing phase as well as for any commercial large-scale market introduction.

An important milestone in 2017, was the publication of the C-ITS certificate policy and security policy[1], which define 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 first phase of the deployment of the EU CCMS will focus on the development of a working prototype of the EU CCMS at European level. In this first phase, the JRC will work on the design of the so called "central elements" defined in the C-ITS certificate policy.

The work will be carried on by unit DG.JRC.E3 to support DG MOVE B.4. and it will consist in the development, implementation and deployment of the central elements of the EU CCMS, which include (the exact details can be found in the Certificate & Security Policy documents):

- *The C-ITS Point of Contact (CPOC), which is a role designed to collect the RCA certificates from other European CAs, transmitting them to the TLM and publication of the European Certificate Trust List (ECTL).*
- *The Trust List Manager (TLM) element, which is the unique entity in the trust model that signs and manages the ECTL. The TLM is composed of a secure server to sign sets of certificates and other management functionalities.*
- *An EU root Certification Authority.*

The scope of this report is to define the Central Point of Contact protocol between the RCAs and the CPOC Entry.

The content provided in this report is based on a technical deliverable provided by the company 'OnBoardSecurity' on the basis of JRC Service Contract 756189 and the subsequent comments by the stakeholders in a workshop organized by DG MOVE and DG JRC on 15th of November 2018.

Two options were investigated in the definition of the CPOC protocol: a manual protocol where RCA representatives would come physically to the CPOC Entry facilities (hosted in on European Commission premises, Joint Research Centre offices in Ispra, Italy) and an automatic protocol based on a secure network, with no physical presence needed of the RCA representatives. Both the feedback from the OnBoardSecuriy contractor and the JRC administration was strongly positive for the manual protocol, i.e. not going for an automated process. While the Commission has also received some feedback that after an

[1] C-ITS Certificate & Security Policy is published and maintained on: https://ec.europa.eu/transport/themes/its/c-its_en

initial enrolment of a RCA via the described manual procedure, it should be possible to re-key/update RCA certificates remotely without continued physical presences during normal operation, this option is currently not possible to be implemented by the Commission. Consequently, the manual protocol is hence the only option described in this technical report to deliver/update root CA certificates to the CPOC, besides a 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 choice of allowed protocol may be revised in the future.

The structure of this report is following:

Section 2 provides an overall view of the EU CCMS architecture.

Section 3 is the main part of the report and it describes the CPOC protocol.

Section 4 provides the conclusions of this report.

The Annex contains message structures defined in ASN.1 format for potential future use.

2 Overall view of the EU C-ITS Security Credential Management system architecture (EU-CCMS)

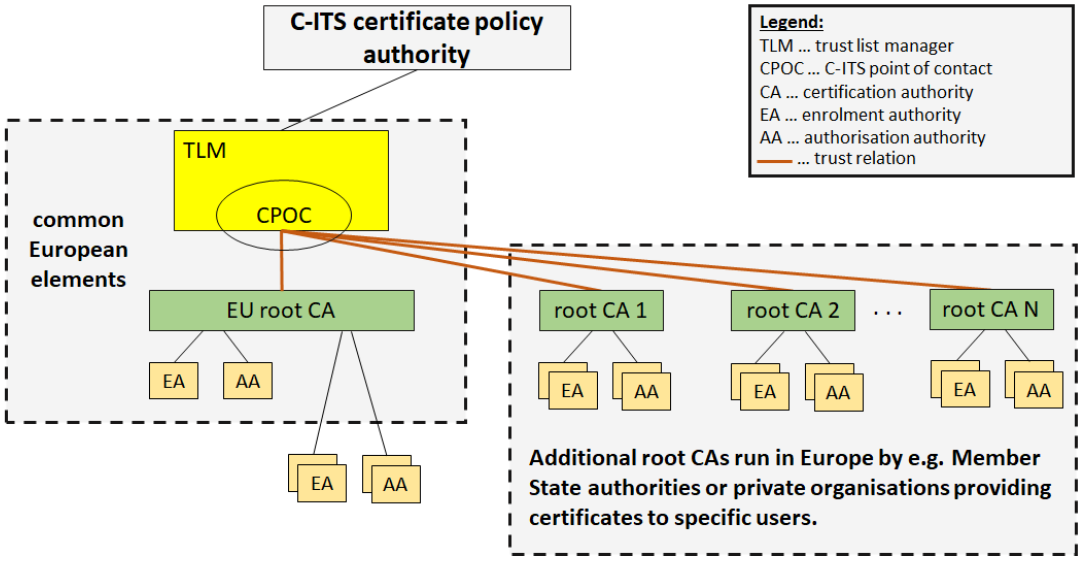

Figure 1 High level view of the EU CCMS trust model (from [2])

The high level functional view of the EU CCMS is provided in Figure 1. The main entities and roles are described in [2] and they are briefly reported here:

Trust List Manager

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

The Trust List Manager is responsible for:

- *issuing of the ECTL according to the common valid CP and regular activity reporting to the policy authority for the overall secure operation of C-ITS trust model,*
- *reception of RCA certificates from the CPOC Entry,*
- *the inclusion/exclusion of RCA certificates in ECTL upon notification by the Policy Authority,*
- *the removal of a RCA certificate from an ECTL, when it is expired, so that it can be replaced by a new RCA certificate of the same RCA,*
- *Signing of the ECTL,*
- *Distribution of the ECTL on the public CPOC Web site.*

C-ITS Point of Contact (CPOC)

The CPOC is a unique entity appointed by the C-ITS Certificate Policy Authority. As described in Figure 2, the CPOC is divided in 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.

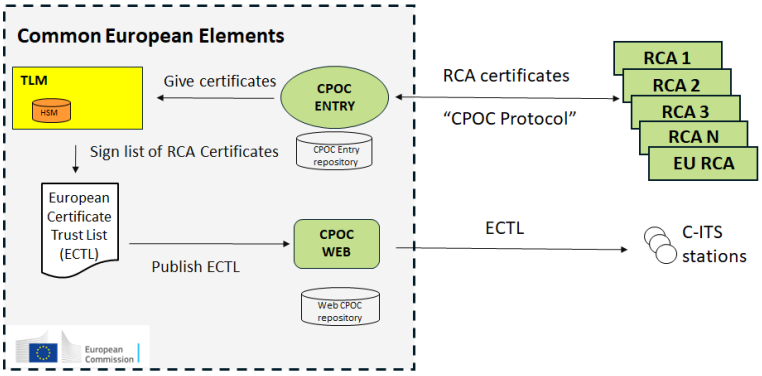

Figure 2 Detailed view of the Common European Elements

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 all entities of the C-ITS trust model,*
- *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 website maintained by the JRC administration that publishes the ECTL 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 Trust List Manager containing its public key, as well as any associated link certificates) following the structure[2] foreseen in [5],*
- *publication of the ECTL following the structure[3] foreseen in [5],*
- *publication of other information related to the deployment of the C-ITS*

This report is focused on the CPOC protocol between **the CPOC ENTRY and the RCAs**.

A more detailed view of the central element structure is provided in Figure 2.

[2] Note: To establish the initial trust between TLM and manufacturer, an additional out of band delivery of the TLM certificate to the manufacturer will be performed (to be defined by the TLM). The ECTL is signed as described in [5]. In case a new TLM certificate is created by the TLM (re-keying), the new self-signed TLM certificate (`selfSignedTLMCertificate` of type EtsiTS103097Certificate) will be inserted inside the ECTL. In addition, a `linkTLMCertificate` of type EtsiTS103097Certificate is going to be inserted in the ECTL (in accordance to the definitions of `TlmEntry` in section A.2.7. of [5], and the text of Section 5.6.1 of the CP [2]). This `linkTLMCertificate` will as well be published outside of the ECTL on the CPOC website.

[3] Note: Following the definitions of `RootCaEntry` in section A.2.7. of [5], and Section 5.6.2 of the CP [2], the ECTL will contain the self signed RCA certificates (`selfsignedRootCa` of type EtsiTS103097Certificate) and all RCA link certificates (`linkRootCaCertificate` of type EtsiTS103097Certificate) that have been received via the CPOC ENTRY interface from RCAs, in case the re-keying of the RCA certificates has been performed by the RCAs.

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 is expected to be implemented and operated on European Commission premises at DG Joint Research Centre, Via Enrico Fermi, 2749, 21027 Ispra (VA), Italy.

3 CPOC protocol

3.1 Conventions and Definitions

All message structures are defined in ASN.1 and encoded using the Canonical Octet Encoding Rules (C-OER) [1]. This means that that all messages structure are defined in ASN.1 using the same Canonical Octet Encoding Rules (C-OER) as defined in [4]. However, the Annex of this document is currently only for potential future use, as a manual protocol will be used for the delivery of root CA certificates.

The definitions of [2] apply. Further, the following definitions apply in this document:

- application form: the 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 [2], the application form includes a hash of the RCA certificate.
- application approval: the application approval is a paper-based document that originates from the CPA and is transmitted to RCA applicants. This document can be digitalised by e.g. creating a PDF of the document. Once digitalised, a hash of the signed application approval can be created and is used in the workflow of this document.

3.2 Main flows

The following three main flows are defined for the CPOC-RCA protocol:

1. ***Add a new Root Certificate.*** *This flow is used to add a new RCA certificate. This approach is used when either 1) the RCA certificate is new, or 2) when the RCA certificate requires no linkage to a prior RCA certificate*[4]*.*
2. ***Add a new Root Certificate with linkage to previous root.*** *In this case, the new RCA Certificate is added in conjunction with a link Certificate (see [2]) that cryptographically binds it to the current/valid trustable RCA Certificate.*
3. ***RCA Certificate Revocation****. In this case, the operator of a RCA can use the mechanisms of this section to request that the RCA is revoked from the ECTL.*

Each of these flows are described in the following subsections. The first two flows are described in section 3.3 below. The third flow is described in subsection 3.4.

3.3 RCA-CPOC: Addition of a new RCA

This section provides the protocol steps between a RCA organization and CPOC to securely support both scenarios to add a new root Certificate: **Add a new RCA Certificate** and **Add a new RCA Certificate with linkage to previous RCA Certificate.**

3.3.1 Assurance Goals

The following assurance goals need to be satisfied.

Note that the following sections and table do also incorporate elements of the Certificate Policy [2]. The related sections of the Certificate Policy are described accordingly.

[4] This case is not defined at this moment at writing the report, but it is inserted for future reference.

Table 1: Assurance Goals between the CPOC Entry and RCAs: 'Root Certificate Addition' and 'Add a new Root Certificate with linkage to previous root'

Goal	Notes
(Prior to CPOC ENTRY/RCA Interaction) The audited[5] system is the system that generated the self-signed RCA certificate	
(Prior to CPOC ENTRY/RCA Interaction) The RCA Certificate is valid	Minimally, the hash of the RCA certificate and any metadata (internal certificate fields such as validity period, issuance permissions (PSID-SSPs), etc. as specified in the CP [2]) associated with the RCA certificate needs to be provided to the CPA in the application form (in fact the hash of the Root-CA certificate is part of the application form as described in [2]). The process to validate the RCA Certificate is described in the CP in section 4.1.2.1.
(Prior to CPOC ENTRY/RCA Interaction) The RCA certificate is bound to a valid Application (for adding it to the ECTL)	While there is limited need for this capability today, a future updated European C-ITS trust model may need to constrain the applications and permissions issuance rights of a RCA certificate[6]. In terms of the European CPA, this is simply an additional (future) check that may need to be performed by the CPA when reviewing the application form and validating the RCA certificate according to CP [2].
(Prior to CPOC ENTRY/Root Interaction) Validation Checks are performed and verified for the RCA certificates as specified in the CP [2].	Validation checks as specified in the CP [2]. See description of the detailed flow in section 3.3.
Submission of the new RCA certificate via the CPOC ENTRY (to the TLM) can only be accomplished with a valid application approval	A strong consistency check is needed to correlate the application approval with: 1) the self-signed RCA certificate and hash of the RCA certificate[7] 2) the RCA organization

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

[6] Informative note: For example, at the time of writing this report, the US Proof of Concept Security Credential Management System (SCMS) includes no issuance constraints on application (Provider Service Identifier – PSID) or Security Specific Permissions (SSP). This will likely change, however, as the governance model matures and root certificates (and their operators) are constrained into specific application and/or permissions issuance domains. Certain types of credentials related to police, fire and other first responders may require special issuance entitlements.

[7] It is important that the hash of the RCA certificate is not disclosed to parties external to the organization responsible for the root CA.

Goal	Notes
	3) the self-signed RCA certificate that is presented/uploaded to the CPOC ENTRY. The applicable procedure for approval is described in detail in the CP [2] (chapter 4.1.2). 4) the CPOC Entry will also check the hash of the digitized form (e.g., PDF file) of the application approval.
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	The RCA representatives making the request is the entity with the credentials specified in the CP [2] (sections 3.2.2.1 and 3.2.3.1).

3.3.2 High Level Flow

The high-level flow is depicted below:

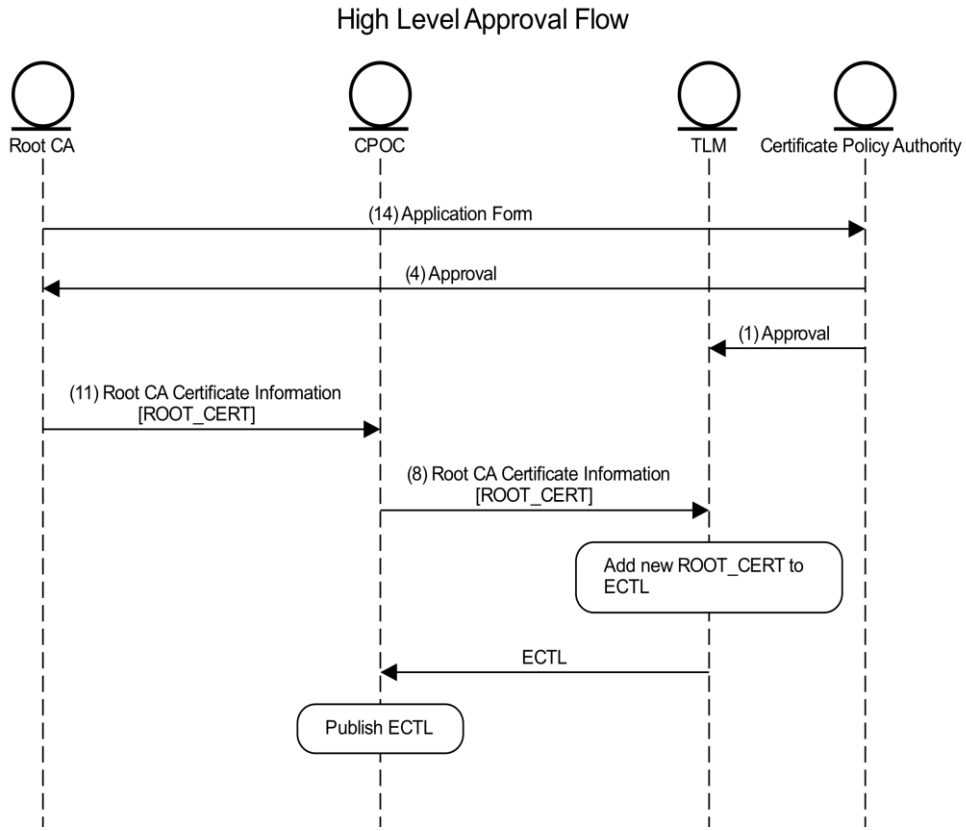

Figure 3: Root Certificate Management - High Level Flow (note that this is a subset of Figure 2 in the Certificate Policy [2]))

New RCA certificates – whether to be trusted explicitly within the TLM-signed ECTL, or additionally trusted via a linkage to a previous Root Certificate – may be added only after the RCA organization has successfully applied and received approval from the CPA for the addition of a Root Certificate.

NOTE: The process for the approval of a RCA by the CPA is described in the Certificate Policy [2]. In addition, the cryptographic material (i.e., RCA certificate) is validated following the procedure described in this document. In addition, the CPA provides the application approval to the CPOC Entry, which calculates the hash of the digital form of the application approval for each approved root CA and stores it for future use.

Any operation on the CPOC protocol will also be logged and recorded in the DG JRC administration files. The DG JRC administration can also record the identifier for the approval, which is an IA5String containing this official identifying number.

3.3.3 Protocol Description

A manual protocol is defined for this interface.

The protocol is based on and will use the ASN.1 structures defined in ETSI standards [4] and [5]. The format of the RCA certificate and the linkCertificate is defined as EtsiTs103097Certificate defined in [4].

3.3.3.1 Prerequisites

1. (Authenticators) Authorized Representative authenticators (defined in the C-ITS Certificate policy, sections 3.2.2.1 and 3.2.3.1) have been pre-shared:
    a. The RCA organization and Authorized Representative identification and authentication information been conveyed to the Certificate Policy Authority (CPA) and validated.
    b. The RCA Authorized Representative 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.
    c. CPOC ENTRY Authorized Representative authenticators are known to the RCA Authorized Representative. The CPA has securely shared this information with the RCA Authorized Representative 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 [2].
2. The RCA has been audited successfully according to the CP [2]:
    a. In addition to the audit procedure, specified in CP [2], 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-signed 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. The new (or existing) RCA organization has completed and submitted a valid application form (CP Flow 14) in conjunction with the Accredited PKI Audit Report (CP Flow 16) to the Certificate Policy Authority (CPA). In case the RCA intends to optionally make use of the remote notification for revocation (see section 3.4), the RCA organization shall also provide the necessary information to identify the RCA RA through eIDAS (e.g., identifiers, eIDAS provider) to the CPA.
4. The CPA shall execute the following steps:

a. Collect the RCA Authorized Representative information that the CPOC ENTRY will use to authenticate when delivering the self-signed RCA certificate,
b. validate the RCA Authorized Representative identification and authentication data, as described in the Certificate Policy [2],
c. securely convey the application approval (including the approval identifier and the approval time) in digital form (i.e., PDF file) to the RCA (CP Flow 4 [2]). A paper copy can also be provided to the RCA Authorized Representative.
d. securely convey the pplication approval (including the approval identifier and the approval time) and/or its metadata to the TLM and CPOC ENTRY (CP [2] Flow 1). The eIDAS information shall also be provided to the CPOC ENTRY, if the RCA RA provided it in the previous step. The CPOC ENTRY will calculate the hash of the application approval in digital form for future use.

Note: the approval documents and the outcome of an approval request (either successful or unsuccessful) will be recorded in the DG JRC administration system as well.

3.3.3.2 Detailed description of the Manual Flow

The ASN.1 encoded data structures according to the ETSI standards [4] and [5] are transferred by manual delivery via temporary storage devices (e.g., external hard drive, USB flash drive, tokens) 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 root CA 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. The European Commission DG JRC acting as the CPOC only supports this protocol at this moment in time.

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 sending RCA link certificates remotely). However, this initial version of the CPOC protocol under the governance of the European Commission does not support any such possibility.

1. Following section 4.1.2.1. of the CP [2] the RCA's Authorized Representative (AR) shall:
    a. travel to the CPOC ENTRY, in possession of the following:
        - physical media containing
            1. the self-signed RCA Certificate formatted as a EtsiTs103097Certificate structure according to [4]
            2. in case of an re-keying of the RCA certificate, the new RCA self-signed certificate and the link certificate (certificate signed with the current valid private key) shall be formatted as an EtsiTs103097Certificate according to [4].
        - its Authorized Representative authenticators as defined in the CP [2] (in particular, sections 3.2.2.1 and 3.2.3.1)
        - the CPA-authenticated application approval (including the unique approval identifier and the approval time) received from the CPA.
        - Additional information and data required by the CP [2].
    b. Authenticate the CPOC's Authorized Representative (AR) using the CPA provisioned CPOC ENTRY authenticators (provided in CP Flow 1)
    c. Provide his/her own Authorized Representative identification/authentication materials to the CPOC ENTRY AR.
1. The CPOC ENTRY AR shall:
    a. Authenticate the RCA AR based on its presented credentials
    b. Verify the root's application approval received out-of-band from the CPA is the same as that presented by the RCA AR:

- Match the RCA application approval against the approval document hash information provided out-of-band from the CPA to the TLM/CPOC ENTRY (see step 4.d in paragraph 3.3.3.1). This is accomplished by generating a hash of the received digital document and comparing to the known hash.
- The RCA's Authorized representative identifiers match
- (*If there are any miss-matches, the operation is discontinued, logged and the mismatch is investigated)*

c. On a secure, isolated system:
   - Insert the RCA's physical token (e.g., USB drive) and extract the RCA add/remove message data for validation. This is the self-signed RCA certificate and optionally link certificate from the ECTL.
   - Generate a hash over any RCA certificates 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 (i.e. delta ECTL).

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 approval form). In addition all the parameters and signatures in the RCA certificate must also be verified. These parameters are also listed on the application form (see CP [2]).
   - 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).
     Note that the approval time are recorded by the DG JRC administration and the CPOC ENTRY repository.
   - In case of an update of a RCA certificate, where hence a link certificate is provided: validate the signature over the RCA link certificate (using the old RCA's public key. Verify the self-signed signature of the new certificate and validate all parameters.

- *(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 in case of an update of a RCA certificate,) to the TLM via interface over CP Flow 8 [2],
  - Log the successful procedure and transfer to the TLM
  - Provide an accounting receipt to the RCA AR, indicating:
    1. Identifiers of the CPOC ENTRY AR
    2. Identifiers of the RCA AR
    3. Receipt Date and Time
    4. Date and Time of the Root addition
    5. Planned Publication Date in the ECTL
    6. Hash of the new RCA
    7. Hash of the associated digital application approval

Note: the outcome and the digital artefacts collected and produced in the steps above will be recorded in the DG JRC administration system as well.

3.3.4 Errors and exceptions

This section provides the ASN.1 errors the CPOC ENTRY may return to the Root. The full list of errors is as follows, followed by a description of only those errors that pertain to Root certificate upload requests.

```
ErrorCode ::= CHOICE {
    representativeAuthorizationFailed          INTEGER(0),
    uploadPeriodNotStarted                     INTEGER(1),
    approvalNotFound                           INTEGER(2),
    rootCACertificateSignatureFailed           INTEGER(3),
    rootCACertificateFormatFailure             INTEGER(4),
    rootCACertificateValidityPeriodOutOfBounds INTEGER(5),
    linkageSignatureFailed                     INTEGER(6),
    linkageRootUnknown                         INTEGER(7),
    requestedRevocationDatetimeTooFarInFuture  INTEGER(8),
    rootCertificateNotFound                    INTEGER(9),
    hashCollision                              INTEGER(10),
    requestMessageNotAcknowledgedOrReceived    INTEGER(11),
    hashapplicationapprovalfailure             INTEGER(12),
    ...
}
```

representativeAuthorizationFailed

The CPOC ENTRY checks that the Root AR's credentials are applicable to the requested operation. If not, this error is returned to indicate that the requestor (Root AR) was not authorized to perform the requested operation.

uploadPeriodNotStarted

The CPOC ENTRY returns this error to the RCA representative if the requested operation was performed too early, per the time window provided by the CPA to the Root and CPOC ENTRY.

approvalNotFound

The CPOC ENTRY returns this error to the RCA representative if the hash of the RCA's indicated application approval was not found.

rootCACertificateSignatureFailed

The CPOC ENTRY returns this error to the RCA representative if signature verification of the new RCA cert failed (signature mismatch)

rootCACertificateFormatFailure

The CPOC ENTRY returns this error to the RCA representative if the CPOC ENTRY is unable to read the Root Certificate due to incorrect formatting or encoding.

rootCACertificateValidityPeriodOutOfBounds

The CPOC ENTRY returns this error to the RCA representative if the CPOC ENTRY receives the new Root Certificate and its validity period does not overlap the CPA-allowed certificate upload window.

linkageSignatureFailed

The CPOC ENTRY returns this error to the RCA representative if the uploaded linkCertificate fails to verify (the old root signature over the new root failed).

linkageRootUnknown

The CPOC ENTRY returns this error to the RCA representative if the old root used to sign the new root (as contained in the linkCertificate) is unknown to the TLM/CPOC ENTRY and/or is not contained in the ECTL.

hashCollision

The CPOC ENTRY returns this error to the RCA representative if the HashedId8 of the submitted root certificate is identical to the HashedId8 of a root certificate that is already on the ECTL. Since revocation on the CTL identifies a revoked root certificate by its HashedId8, it is a requirement that all root certificates have different HashedId8s to ensure that revocation statements are unambiguous.

requestMessageNotAcknowledgedOrReceived

The CPOC ENTRY returns this error to the RCA representative if the CPOC ENTRY receives a status request message for a request message it did not receive (i.e., the hash of the indicated, original request is unknown)

Hashapplicationapprovalfailure

The CPOC ENTRY returns this error to the RCA representative if the CPC ENTRY receives an application approval, whose hash does not match the recorded hash for the application approval of that RCA.

3.4 RCA-CPOC ENTRY: RCA Certificate Revocation

This section describes the RCA to CPOC ENTRY RCA revocation protocol, which implies the deletion of a RCA certificate.

3.4.1 Overview

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 Root provides the CPOC ENTRY with a hash of the to-be-revoked Root certificate, and the CPOC ENTRY acknowledges the removal request.

Building upon section 7.3.1 of the CP [2], for the purpose of this CPOC protocol the RCA certificate revocation are described in the following scenarios:

- ***Scenario 1:*** *The compromise or suspected compromise of a RCA system. If the compromise or suspected compromise is considered of critical importance by the RCA management entity and/or the CPA, the removal of the associated RCA certificate from the ECTL should be executed as soon as possible. See section 3.4.3.2 of this report for details.*
- ***Scenario 2:*** *The need to upgrade an entire certificate chain's cryptographic algorithm type/strength,*
- ***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.*
- ***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 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 2: 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.

Root 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.

3.4.2 Data Structures

RCA Revocation shall be performed using the following ASN.1 data structure:

```
RevokeRoot ::= SEQUENCE {
    rootCAHash              HashedId32,           -- the hash of the RootCA certificate to be revoked
    revocationNotBefore     Time32 OPTIONAL,      -- the earliest requested datetime the RootCA Cert
        may be removed from the ECTL (if requested)
    ...
}
```

3.4.3 Protocol Description

3.4.3.1 Prerequisites:

1. *Authorized Representative authenticators (C-ITS Certificate policy [2], sections 3.2.2.1 and 3.2.3.1) have been pre-shared*
2. *The CPA has a policy indicating how far in the future a revocation request can be made.*
3. *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.*

3.4.3.2 Detailed description of the flow

Note: the first two steps are different depending on the scenarios identified in section 3.4.1. If a RCA needs the urgent revocation of its RCA because the first case (compromise or suspected compromise of a RCA system) has been assessed as a critical compromise, the first two steps will be implemented in a different way:

Flow for Scenarios 2,3,4 (and 1 when it is not considered critical or urgent) according to chapter 3.4.1:

1. The RCA Authorized Representative shall travel to the CPOC ENTRY.

2. The RCA and CPOC ENTRY ARs shall mutually authenticate according to the CP [2]. If authentication fails, STOP and notify the CPA; otherwise PROCEED.

3. The RCA Authorized Representative shall populate, date and sign a Root Revocation form (i.e. revocation request in addition to the CRL from [2]) that indicates the following information:

- *RCA Authorized Representative identifying information*
- *RCA certificate identifying information:*
  - *HashedId32 of the RCA Certificate*
  - *Original expiration date of RCA Certificate*
  - *The requested revocation time, which is indicated either:*
    - *1. with an envisaged maximum time frame[8], OR*
    - *2. Next ECTL Publication time*

4. The RCA Authorized Representative shall:

- *present a storage device (e.g., thumb drive) containing a valid signed RevokeRoot message,*
- *present the application approval.*

Flow for Scenario 1 when it is considered critical or urgent according to chapter 3.4.1:

1. The RCA Authorized Representative can choose to not physically travel to the CPOC ENTRY.

2. Instead, The RCA Authorized Representative shall send an email to the CPOC ENTRY (MOVE-JRC-C-ITS-POLICY-AUTHORITY@ec.europa.eu) with a request for revocation with the following information:

- *A document containing the revocation information (i.e. according to [2] the CRL in digital form, which includes the hash of the root CA certificate to be revoked and the application approval) signed by the RCA AR requesting the revocation of its own RCA certificate.*
- *HashedId32 of the RCA Certificate*
- *Original expiration date of RCA Certificate*
- *The requested revocation time, which is either:*

  1. Within an envisaged maximum time frame[9], OR
  2. Next ECTL Publication time

The digital document in the e-mail request shall be signed using the eIDAS system. [6]

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.

From this point, the flow is common for all the cases identified in Scenarios 1,2,3,4:

[8] Which according to the CP [2] will trigger a revocation as soon as possible and without undue delay.
[9] Which according to the CP [2] will trigger a revocation as soon as possible and without undue delay.

4. The CPOC ENTRY shall validate the following:
   - *The RCA certificate exists (based on its HashedId32), is currently valid, and is published in the ECTL*
   - *The RCA Authorized Representative is entitled to represent the identified RCA certificate, and the representative's credentials can be verified by the CPOC ENTRY*
   - *The requested revocation time is within the policy-constrained maximum time in the future*
   - *The provided hash of the application approval matches the recorded hash.*

5. If any validation checks fail, STOP and notify the CPA. Otherwise, PROCEED.

6. The CPOC ENTRY shall provide the RCA Authorized Representative with the next ECTL publication date that will reflect the Root Certificate removal.

7. The CPOC ENTRY shall provide an acknowledgement receipt to the RCA Authorized Representative, indicating:

   - *Root revocation request is validated and approved*
   - *HashedId32 of the Root Certificate to be removed*
   - *Time of the approval Datetime*
   - *Planned ECTL publication date that will reflect the revocation CPOC ENTRY identifying information*

3.4.4 Errors and exceptions

This section provides the ASN.1 errors the CPOC ENTRY may return to the Root upon its requesting a Root certificate revocation. The full list of errors is as follows, followed by a description of those errors that only pertain to Root revocation requests.

```
ErrorCode ::= CHOICE {
    representativeAuthorizationFailed          INTEGER(0),
    uploadPeriodNotStarted                     INTEGER(1),
    approvalNotFound                           INTEGER(2),
    rootCACertificateSignatureFailed           INTEGER(3),
    rootCACertificateFormatFailure             INTEGER(4),
    rootCACertificateValidityPeriodOutOfBounds INTEGER(5),
    linkageSignatureFailed                     INTEGER(6),
    linkageRootUnknown                         INTEGER(7),
    requestedRevocationDatetimeTooFarInFuture  INTEGER(8),
    rootCertificateNotFound                    INTEGER(9),
    requestMessageNotAcknowledgedOrReceived    INTEGER(11),
    ...
}
```

Only the new fields in comparison to section 3.3.4 are described.

representativeAuthorizationFailed

The CPOC ENTRY checks that the Root AR's credentials are applicable to the requested operation. If not, this error is returned to indicate that the requestor (Root AR) was not authorized to perform the requested operation.

requestMessageNotAcknowledgedOrReceived

The CPOC ENTRY returns this error to the Root if the CPOC ENTRY receives a status request message for a request message it did not receive (i.e., the hash of the indicated, original request is unknown)

requestedRevocationDatetimeTooFarInFuture

The CPOC ENTRY returns this error to the Root if the CPOC ENTRY detects that the requested revocation is too far in the future, by policy.

rootCertificateNotFound

The CPOC ENTRY returns this error to the Root if the Root's requested revocation is for a Root Certificate (based on its hash) that the CPOC ENTRY/TLM is not aware of and is not in the ECTL.

4 Conclusions

This report provides a description of the protocol between the CPOC Entry and the RCAs in the EU CCMS. As described in the report, this is a manual protocol, where representatives from the RCAs will come to the CPOC facilities (at the European Commission premises of DG JRC in Ispra, Italy) to provide the RCA certificate and additional information when needed. The various root certificates are then given to the Trust List Manager, which are subsequently published via the ECTL on the CPOC web site. Further, the mechanisms for revocation and interaction with the CPOC is described.

References

[1]. ITU-T Recommendation X.696 (08/2014), Information Technology—Specification of Octet Encoding Rules (OER), 2014. Available from http://www.itu.int/rec/T-REC-X.696-201408-I

[2]. Certificate policy for deployment and operation of European cooperative intelligent transport systems (C-ITS)
Current published release 1.1:
https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf
Future regulation to be adopted by the Commission, fully replacing release 1.1 with the corresponding certificate policy Annex of the C-ITS delegated regulation under ITS Directive 2010/40/EU, once formally adopted by the Commission – Draft Annex already available at: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-2592333_en#isc-2018-08207

[3]. IEEE 1609.2-2016 ("IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages")

[4]. ETSI TS 103 097 V1.3.1 (2017-10). Intelligent Transport Systems (ITS); Security; Security header and certificate formats https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf.

[5]. ETSI TS 102 941 V1.2.1 (2018-05). Intelligent Transport Systems (ITS); Security; Trust and Privacy Management

https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

[6]. 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

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=IT

[7]. ETSI TS 102 965 V1.4.1 (2018-11) Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration

https://www.etsi.org/deliver/etsi_ts/102900_102999/102965/01.04.01_60/ts_102965v010401p.pdf

List of figures

List of tables

5 Annex: ASN.1 definitions for potential future use

This annex describes the ASN.1 definition for the data types, which are defined apart from the ones already defined in ETSI standards for potential future use within the CPOC protocol:

ETSI TS 103 097 V1.3.1 [4]

and

ETSI TS 102 941 V1.2.1 [5]

```
CpocProtocol
{iso(1) identified-organization(3) european-commission(130) information-systems(1) c-its-systems(3) cpocProtocol (1) version1(1)}

DEFINITIONS AUTOMATIC TAGS ::= BEGIN

IMPORTS

EtsiTs103097Certificate
FROM EtsiTs103097Module
{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103097) v1(0)}

Time32, Uint8
FROM Ieee1609dot2BaseTypes {iso(1) identified-organization(3) ieee(111)
   standards-association-numbered-series-standards(2) wave-stds(1609)
   dot2(2) base(1) base-types(2) major-version-2(2)}



;

-- ------------------------------------------------------------------
--
--          RCA / CPOC ENTRY interface

--
-- ------------------------------------------------------------------

-- SignedCpocRootCaPDU is the top-most message type
-- This structure is enclosed in an Ieee1609Dot2Data of content type SignedData per
-- ETSI 103097 Clause 5.2.
```

```
-- The ITS-AID for CTL service is allocated in the ISO AID registration table and the value
is specified in ETSI TS 102 965 V1.4.1 [10]

RootCaCpocPDU ::= SEQUENCE {
   version         Uint8,
   messageContent  CpocRootMessage,
   ...
}

CpocRootMessage ::= CHOICE {
   request         CpocRootRequestMessage,
   response        CpocRootResponseMessage,
   ...
}

CpocRootRequestMessage ::= SEQUENCE {
   requestTime     Time32,
   content         CpocRootRequest,
   ...
}
CpocRootRequest ::= CHOICE {
   addRootWithoutLinkage AddRootWithoutLinkage,
   addRootWithLinkage    AddRootWithLinkage,
   revokeRoot            RevokeRoot,
   statusRequest         CpocRootStatusRequest,
   ...
}
AddRootWithoutLinkage ::= AddRoot (WITH COMPONENTS {...,
   linkageInfo           ABSENT
  })

AddRootWithLinkage ::= AddRoot (WITH COMPONENTS {...,
   linkageInfo           PRESENT
  })

AddRoot ::= SEQUENCE {
   rootCert              EtsiTs103097Certificate,
   linkageInfo           EtsiTs103097Certificate OPTIONAL, -- Root certificate signed by old
root
```

```
    rootCertApprovalTime  Time32,     -- Approval time provided by the CPA
    rootCertApprovalId    IA5String,  -- Identifier for Root Certificate approval from CPA
    ...
}

RevokeRoot ::= SEQUENCE {
    rootCAHash              HashedId32,          -- the hash of the RootCA certificate being revoked
    revocationNotBefore     Time32 OPTIONAL,     -- the earliest requested datetime the RootCA Cert may be removed from the ECTL (if requested)
    ...
}

CpocRootStatusRequest ::= SEQUENCE {
     -- Hash of the encoded RequestMessage for which the Root is requesting status
     -- This is only for asynchronous use in an automated protocol
    requestHash          HashedId32,
    ...
}

-- CPOC-to-RootCA Response Message
CpocRootResponseMessage ::= SEQUENCE {
    responseTime    Time32,
    requestHash       HashedId32,  -- hash of request message to which this response message corresponds
    content         ResponseContent,
    ...
}

-- the request has been successfully processed. RCA will be added/removed in the next ECTL update
ResponseContent ::= CHOICE {
    success        INTEGER(0),
    errors         SEQUENCE OF ErrorCode,
    ...
}

ErrorCode ::= CHOICE {
    representativeAuthorizationFailed          INTEGER(0),
    uploadPeriodNotStarted                     INTEGER(1),
```

```
    uploadPeriodExpired                     INTEGER(2),
    approvalNotFound                        INTEGER(3),
    rootCACertificateSignatureFailed        INTEGER(4),
    rootCACertificateFormatFailure          INTEGER(5),
    rootCACertificateValidityPeriodOutOfBounds INTEGER(6),
    linkageSignatureFailed                  INTEGER(7),
    linkageRootUnknown                      INTEGER(8),
    requestedRevocationDatetimeTooFarInFuture  INTEGER(9),
    rootCertificateNotFound                 INTEGER(10),
    hashCollision                           INTEGER(11),
    requestMessageNotAcknowledgedOrReceived    INTEGER(12),
    ...
}


HashedId32::= OCTET STRING (SIZE (32))

END
```

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

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, or

- by electronic mail via: https://europa.eu/european-union/contact_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 at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-29634-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/77171
ISBN 978-92-79-99079-3