



C-ITS SECURITY REQUIREMENTS & SPECIFICATIONS

23.09.2025



Co-funded by
the European Union

Table of Contents

1.	Introduction.....	5
1.1	C-Roads platform for harmonisation of C-ITS deployment.....	5
1.2	C-ITS services	6
1.3	Purpose of a reading guide to the WG2 C-Roads documentation	7
1.4	Story board C-Roads C-ITS deployment documentation.....	8
1.5	C-ITS documentation release and version overview	12
2.	Security requirements from reference documents.....	14
2.1	ETSI standards	14
2.2	Certificate Policy.....	14
2.2.1	Stations enrolment	15
2.2.2	Authorization	16
2.3	Security Policy.....	17
2.4	CPOC & TLM.....	17
2.5	Specific security requirements	17
2.5.1	Certificate format and validity times.....	17
2.5.2	Cryptographic operations.....	18
2.5.3	Stations permissions.....	18
2.5.4	Certificate Authorities permissions	19
2.5.5	Security initialisation	23
2.5.6	Message signature.....	23
2.5.7	Verification of message signature	24
2.5.8	Permissions delegation.....	24
2.5.9	Cryptoagility	24
2.5.10	Logging.....	24
2.6	Hybrid related requirements	25
2.7	Other vehicle stations requirements.....	26
	Annex A - Security initialisation steps	28
	Annex B - Signature verification steps.....	31
	Annex C - Certificate examples.....	35
	Example of Root CA certificate.....	35
	Example of EA certificate.....	37
	Example of AA certificate	38
	Example of RCA-CTL.....	39
	Example of CRL	44

Table of figures

FIGURE 1: OVERVIEW OF C-ROADS COVERAGE	6
FIGURE 2: OVERVIEW OF C-ROADS WORKING GROUPS	9
FIGURE 3: STORY BOARD AND C-ROADS DOCUMENTATION	9
FIGURE 4: DEFINITION AND EXAMPLES OF C-ITS STATIONS PERMISSIONS	19
FIGURE 5: AA - AT APP PERMISSION CHECK.....	32
FIGURE 6: RCA - AA APP PERMISSION CHECK.....	32
FIGURE 7: CERT ISSUE PERMISSION CHECK.....	33

Document history

Version	Date	Description, updates and changes	Status
0.5	25.10.2019	First draft for WG2 review	Draft
0.6	07.05.2020	Update following 1 st review Integration of former report's annexes A & B	Draft
0.7	12.05.2020	Minor modifications before review	Draft
0.8	04.06.2020	Integration of comments from WG2 review	Draft
0.82	06.07.2020	Inclusion of agreed modifications after WG2 review, insertion of common C-Roads' introduction	Draft
0.91	29.09.2020	Feedback from all WG2 observation forms	Draft
1.8.0.SC	01.12.2020	Updated following discussion of pending issues and Change Requests within TF1. Versioning aligned with all task forces	Draft
1.8.2	22.10.2021	Update of RS_SEC_014 & RS_SEC_032 following March 2021 WG2 meeting. Correction of IVI bitmask values in CAs. Note regarding ATs validity period for testing purposes.	Draft
2.0.1	18.02.2022	Insertion of delegation mechanisms for IVI Service Provider ID SSPs. Minor updates.	Draft
2.0.4	03.06.2022	Internal TF1 review and WG2 meeting outputs (delegation in draft, update of 103 301 version, secure link update)	Draft
2.0.5	Aug./Sept. 2022	Transfer of the delegation concept to the governance document, alignment of the documents, comment resolution in TF1	Draft
2.2.0	May 2024	Update following the availability of the PP and the CP/SP update	Draft
3.0.0	August 2025 September 2025	Updated reference to the CPOC for the maximum permissions allowed in Root CA certificates. Update of introduction and references	Approved

List of used abbreviations

AA	Authorization Authority
AT	Authorization Ticket
API	Application Programming Interface
C2C-CC	Car 2 Car Communication Consortium
CA	Certificate Authority
C-ITS	Cooperative Intelligent Transport Systems
CCMS	C-ITS Security Credential Management System
CP	Certificate Policy
CPA	Certificate Policy Authority
CPS	Certificate Practice Statement
CPOC	C-ITS Point of Contact
CTL	Certificate Trust List
EA	Enrolment Authority
EC	Enrolment Certificate
ECTL	European Certificate Trust List
EE	End Entity
EU	European Union
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IP-based	The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking and essentially establishes the Internet.
ITS	Intelligent Transport System
ITS-G5	ITS-G5 is a European standard for ad-hoc short-range communication of vehicles among each other (V2V) and with Road ITS Stations (V2I). The ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band is given in ETSI EN 302 663. ITS-G5 is a profile of the amendment IEEE 802.11p, which has been incorporated into the main IEEE 802.11 standard, and an IEEE 802.2 LLC. It uses the 5.9 GHz frequency band to support safety- and non-safety ITS applications.
ITS-S	ITS Station
MS	Member State
OBU	On Board Unit
PKI	Public Key Infrastructure
SP	Security Policy
TBC	To Be Confirmed
TBD	To Be Defined
TF#	Task Forces (TF1 – Security Aspects)
TLM	Trust List Manager
TLS	Transport Layer Security - Internet Engineering Task Force (IETF) RFC 8446
V2I	Vehicle to Infrastructure communication; Information exchange between vehicles and infrastructure.
V2I2V	Vehicle to Infrastructure to Vehicle communication; Information exchange from vehicles to infrastructure to vehicles
V2V	Vehicle to Vehicle Communication; information exchange between vehicles.
WG#	Working Groups

References

All References (in square brackets) refer to the global reference document WG2 REFERENCES 3.1.0 (9/2025).

1. Introduction

1.1 C-Roads platform for harmonisation of C-ITS deployment

The C-Roads Platform is a joint initiative of European Member States and road operators for testing and implementing C-ITS services in light of cross-border harmonisation and interoperability. Through the C-Roads Platform, authorities and road operators join together to harmonise the deployment activities of cooperative intelligent transport systems (C-ITS) across Europe. The goal is to achieve the deployment of interoperable cross-border C-ITS services for road users.

C-ITS enables vehicles to interact directly with each other and the surrounding road infrastructure. In road transport, C-ITS typically involves vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. To enable an efficient and undisturbed exchange of information within these services as well as a cross-border implementation, harmonised C-ITS specifications are indispensable. The approach starts from a functional perspective, then requirements applicable to all implementations and then towards technology specifications of currently validated implementations (ITS-G5 for short range communication, IP based for long range cellular). To meet these challenges, there are four Working Groups in which technical and organisational topics are addressed as the working level of C-Roads. The first Working Group is concerned with organisational tasks, the second with Technical Aspects and the third with Evaluation and Assessment. The fourth Working Group is about Digital Transport Infrastructure (DTI). Next to these working groups there are 3 collaboration groups (Blue-light, Urban and Rail) which interact on specific thematic topics with the working groups. The Working Group “Operations and C-ITS Deployment Strategy” (WG-OS) focuses on the setup of a structure for permanent operation of the infrastructure-based European C-ITS system and networks in a multi-stakeholder environment. Here, not only C-Roads implementations are considered, but also the foundations for a general European C-ITS framework are created.

The C-Roads Platform is steered by the C-Roads Steering Committee which is composed by Member State representatives. With the support of the Supporting Secretariat, decisions for achieving the goal of the implementation of interoperable end-user services are taken. In this respect specifications, plans and reports, which are proposed and recommended by specific Working Groups, are approved. Within WG2 these specifications are harmonized in 5 Task Forces and derived from pilot and implementation activities and the basis for further pilot and implementation activities. This especially goes with technical decisions, which influence deployment and procurement decisions at pilot sites.

The Working Groups are installed as decision support for the Steering Committee to ensure proper decisions towards interoperable deployments. Individual experts participating in the single pilots work together in these Working Groups to prepare proposals and recommendations.



Figure 1: Overview of C-Roads coverage

1.2 C-ITS services

Cooperative ITS (C-ITS or cooperative systems) encompass a group of ITS technologies and applications that allow data exchange through wireless communication technologies between components and actors of the transport system either between vehicles (vehicle-to-vehicle or V2V) or between vehicle and infrastructure (vehicle-to-infrastructure or V2I).

The deployment of C-ITS is an evolutionary process that will start with less complex ITS applications. These are referred to as “Day-1-services”, encompassing messages about for example traffic jams, hazardous locations, roadworks, signalised intersections, as well as weather information and speed advice to harmonise traffic.

The intend of these services is to preserve traffic safety, traffic flow efficiency and minimum externalities. In addition, the tasks and responsibilities of road authorities also include operation of the traffic network and safeguarding collective interest. In light of the 1968 Vienna Convention, the C-ITS services are much related to operational tasks:

- Provide **informative** information to road users intended to guide road-users while they are travelling or to provide them with other information which may be useful (e.g. facility, direction, position, road/place identification or confirmation signs).
- Set **regulatory** boundaries through signs intended to inform road-users of special obligations, restrictions or prohibitions with which they must comply e.g. priority, prohibitions, restrictions, obligations and special regulations. .
- Provide danger (safety) **warnings** to road users through signs intended to warn road-users of a danger on the road and to inform them of its nature.

All three tasks are significantly different, with varying levels of importance and performance requirements. C-ITS services are gradually becoming an integrated part of the complete set of instruments, measures and tools that support road authorities and road operators to execute their operational tasks. Moreover, there is a parallel between aforementioned operational tasks and the C-ITS messages used by Day-1-services. For example, there are messages that provide informative and advisory information on road signage, driving context, road works and road topology. In addition, there are messages that provide regulatory information on road signage, speed limits and traffic lights, while the last category of messages contains information on road hazards and abnormal traffic conditions.

1.3 Purpose of a reading guide to the WG2 C-Roads documentation

The purpose of this reading guide is to support the following objectives:

- Stakeholders must be able to find their way through the C-Roads documentation based on their (policy) objectives, interests and needs.
- Stakeholders must be able to recognize their tasks and responsibilities in the service definitions and specifications.
- The C-Roads library must have a clear single entrance and should naturally and logically unfold from the functional definitions.
- The scope of C-Roads in the broader context of traffic management and tasks and responsibility of road authorities must be explained.

The primary target audience of the C-Roads specifications are road authorities (e.g. policy makers, road operators, traffic managers, traffic engineers) who are in charge of maintaining and operating roads in order to preserve traffic safety, traffic flow efficiency and minimize externalities, and industry and service providers who deliver the capabilities for the required functionality.

Working Group 2 is the key working group to fulfil the harmonised functional, technical and process specifications for the C-ROADS platform and is itself divided into five task forces, which cover different subjects according to the subdivision below.

1. Task Force Security Aspects (TF1)
2. Task Force Service Harmonisation (TF2)
3. Task Force Infrastructure Communication (TF3)
4. Task Force Hybrid Communication (TF4)
5. Task Force Cross-Testing and Validation (TF5)

The C-Roads documentation and requirements focusses on the harmonised communication profile for C-ITS services and comprises the results of several test cycles of the C-Roads partners across Europe and is already fine-tuned with the automotive industry (C2C Communication Consortium). Initially the new services and Use Cases were specified, regarding the European, multi-operator and multi-vendor environment. This was done through structured definitions of each individual service and use case. Traffic management issues, such as usage and processing of data for traffic management, were identified and integrated into the overall picture of influencing factors, which will also contain the link to urban environments. Moreover, in order to ensure C-ITS service consistency for users, recommendations from the road operator's point of view on the visualisation or presentation of messages on HMIs are discussed. On this basis, further requirements were defined which form the common basis for the functional and technical specifications. These specifications target the communication between road operators and vehicles and form the basis for the roll-out of infrastructure driven C-ITS services all across Europe and will be extended with each new release. Working Group 2 established a process to ensure the delivery of a new release every 6 months. The release documents contain specific requirements, standards or use case descriptions. This document provides an overview of all the deliverables and the specifications which are part of the latest release.

1.4 Story board C-Roads C-ITS deployment documentation

The C-Roads C-ITS Deployment Documentation and Requirements is much related to a common project life cycle of a system implementation. As a guide to the C-Roads Documentation, a story board based on such a project life cycle is provided in this section. The story board should be read from left to right and shows the different stages of the project life cycle and how the C-Roads Documentation is related to it, thereby can be supportive to road authorities and other stakeholders.

Figure 2 provides a high-level overview of the C-Roads Working Groups. The story board starts with the assumption that a road authority has a basic understanding of C-ITS and decided to implement a C-ITS service. Roughly, the implementing authority will face three phases as depicted. The scope of this general introductory document is limited to phase 2, the technical aspects, which are addressed by working group 2. Further details are shown in Figure 3.

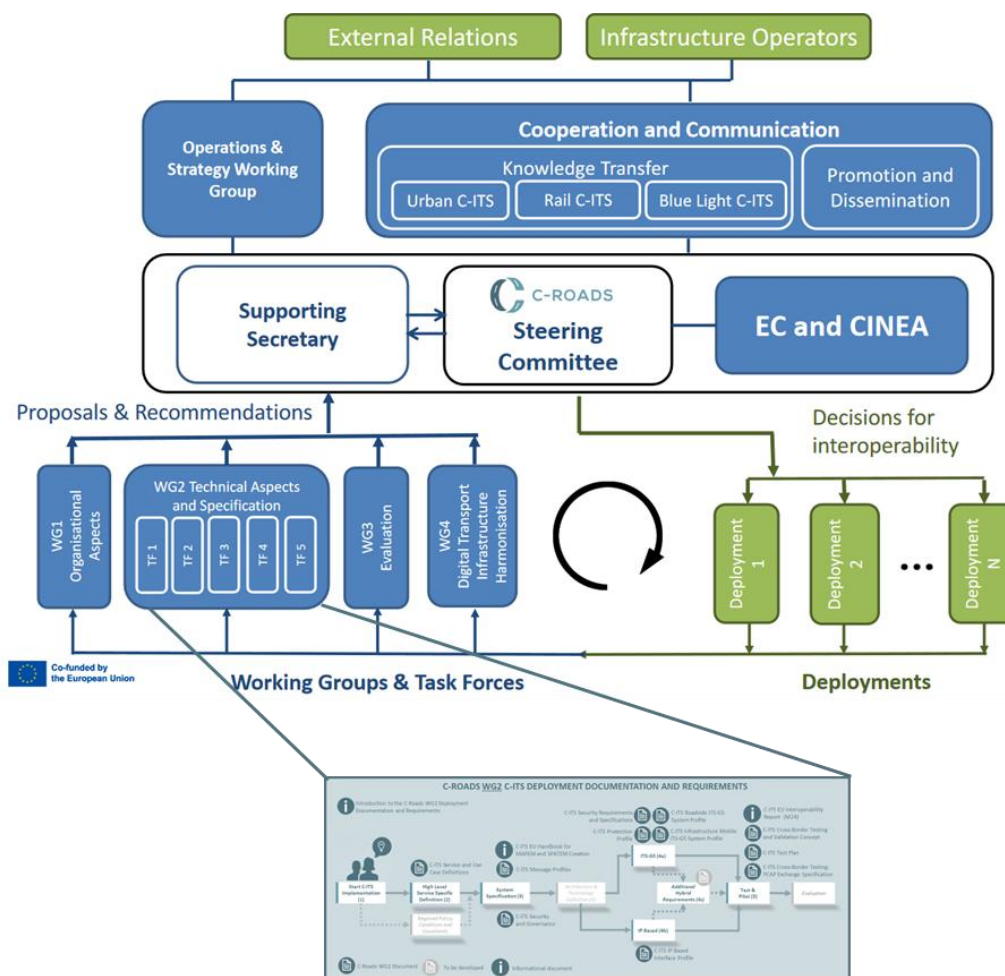


Figure 2: Overview of C-Roads Working Groups

Figure 3 shows on a more detailed level the storyboard of a C-ITS implementation project and which C-Roads WG2 documents are related to each of the stages. The stages are briefly described below, and a brief description of the documents is provided in Section 1.5. The grey marked parts of the charts indicate that there is no WG2 documentation available (yet) for that part. The document icons mark the specific WG2 documentation. The orange indicated document is the present document.

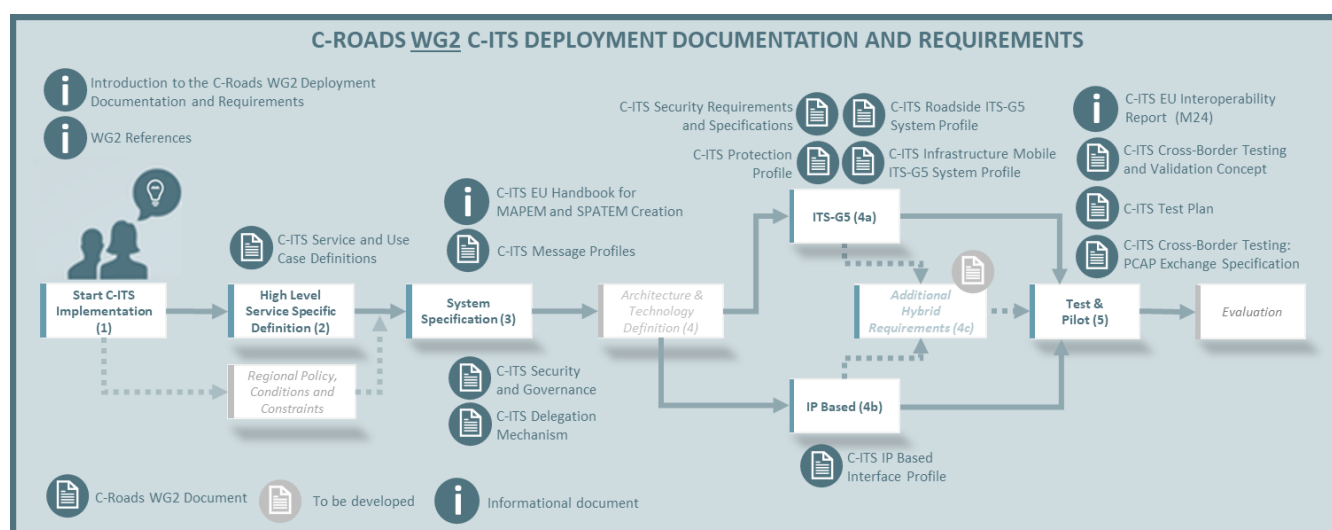


Figure 3: Story board and C-Roads documentation

Stage 1: Start C-ITS Implementation

This stage is the project initiation. It is assumed that the road authority has a basic understanding of C-ITS and decided to implement a C-ITS service. This general introductory document is the main entry point for the road authority and other involved stakeholders to the C-Roads Deployment Documentation and Requirements. The reference document gives an overview of all references used in all C-Roads WG2 documentation.

Associated C-Roads document(s):

- **WG2: Introduction to the C-Roads WG2 Deployment Documentation and Requirements**
- **WG2: Reference document**

Stage 2: High Level Service Specific Definitions

In this stage the road authority and other involved stakeholders further define the intended C-ITS service and for what use cases it should be implemented. Objectives, expectations of the system, the involvement, and responsibilities of actors, etc. all need to be declared.

Associated C-Roads document(s):

- **TF2: C-ITS Service and Use Case Definitions**

Note: an important aspect, but not in scope of the C-Roads Documentation, are regional policy, conditions and constraints. These are likely to be a decisive factor when implementation choices have to be made, therefore are recommended to be clearly reported as a supportive documentation but not provided by C-Roads.

Stage 3: System Specification

Once the service(s) and use cases are defined, the common system specifications for C-ITS Messages and C-ITS Security follow naturally. These common specifications apply to all C-ITS implementations and are a prerequisite to be part of the C-ITS trust domain, irrespective of the architecture and technology choice.

Associated C-Roads documents:

- **TF1: C-ITS Security & Governance**
- **TF2/TF3: European Handbook for MAPEM/SPATEM creation**
- **TF3: C-ITS Message Profiles**

Stage 4: Architecture & Technology Definition

This stage is not supported by C-Roads Documentation and can be very dependent on regional conditions and constraints, e.g. geography, financial resources, organisational processes, previous technology choices, legacy systems, etc. Once architecture and technology choices are made, the C-Roads Documentation covers requirements for either ITS-G5 implementation and/or Cellular IP-based implementation.

Stage 4a: ITS-G5

ITS-G5 is a communication for ad-hoc, short-range, direct communication of vehicles among each other (V2V) and with Roadside ITS Stations (V2I and I2V). It utilizes an option (dot11OCBAActivated) of the IEEE 802.11 WLAN standard in order to do so.

This technology (and possibly others) uses the 5.9 GHz frequency band to support safety- and non-safety ITS applications.

For implementation of the C-ITS service based on ITS-G5, the road authority and involved stakeholders shall rely on the C-ITS Protection and System Profiles that specify the minimum set of standards and fill the missing gaps necessary for the realisation of an interoperable roadside implementation.

Associated C-Roads document(s):

- **TF1: C-ITS Protection Profile for a Roadside ITS Station Gateway**
- **TF3: C-ITS Roadside ITS G5 System Profile**
- **TF3: C-ITS Infrastructure Mobile ITS G5 System Profile**

Stage 4b: IP-Based

For implementation of the C-ITS service based through IP based long range communication networks/backend networks, the road authority and involved stakeholders need to decide in this stage how to establish the information-sharing network, i.e. a deployment model, to interconnect multiple C-ITS actors. Data communication for exchange of C-ITS messages between backend of C-ITS services is an important prerequisite for interoperability.

Associated C-Roads document(s):

- **TF4: C-ITS IP Based Interface Profile**

Stage 4a and 4b:

- **TF1: C-ITS Security Requirements & Specifications**
- **TF1: C-ITS Delegation mechanism**

Stage 4c: Hybrid

Hybrid communication means that C-ITS messages are transmitted to end-user devices using multiple communication channels, for example both ITS-G5 and cellular. It is probable that additional functional and technical requirements apply for such implementations, but at present this is not yet defined in the C-Roads Documentation.

Stage 5: Test & Pilot

To ensure that the implementation of C-ITS service works properly in a European, multi-operator and multi-vendor environment, it is important to test and validate system interoperability. To prove that the implemented system meets the requirements and specifications, the road authority and involved stakeholders have to perform compliance assessment, following a predefined procedure.

Associated C-Roads document(s):

- **TF5: C-ITS Cross-Border Testing and Validation Concept**
- **TF5: C-ITS Test Plan**
- **TF5: C-ITS Cross-Border Testing: PCAP Exchange Specification**
- **TF5: C-ITS EU Interoperability Report (M24)**

Note: the implementing road authority most probably will also be interested in the impact of the C-ITS service on indicators like traffic safety, traffic flow efficiency and externalities. An evaluation and assessment framework are not in scope of working group 2, but provided by working group 3.

1.5 C-ITS documentation release and version overview

The table below provides an up-to-date list of the latest applicable and agreed upon C-Road documents.

Task Force	Document	Current version	Date	Previous version
WG2	Introduction to the C-Roads WG2 Deployment Documentation and Requirements This document gives an introduction to, and an overview of the documentation developed in C-Roads WG2 and the structure of and the relation between these requirement documents.	3.0.0	30/06/2025	2.3.0
WG2	Reference Document This document gives an overview of all references used in all C-Roads WG2 documentation.	3.0.0	30/06/2025	N/A
TF1	C-ITS Security Requirements and Specifications This document provides the detailed specifications for the certificates that are required to sign C-ITS messages.	3.0.0	30/06/2025	2.3.0
TF1	C-ITS Security and Governance This document provides an overall introduction to the common European trust model and builds on the European Certificate Policy for C-ITS, which is referring to the relevant ETSI standards for certificates and PKI management as the underlying technical basis	3.0.0	30/06/2025	2.3.0
TF1	C-ITS Delegation mechanism This document describes a proposition to manage the delegation of IVIM's ServiceProviderID.	3.0.0	30/06/2025	2.3.0
TF1	C-ITS Protection Profile for a Roadside ITS Station Gateway This Protection Profile defines the Security Functional Requirements (SFRs) and the Security Assurance 136 Requirements (SARs) for a Roadside ITS Station Gateway. <i>*This document has a different status as it is published by the BSI, see https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_012_2.html</i>	1.0*	22/03/2024	N/A
TF2	C-ITS Service and Use Case Definitions In this document the services and use cases are described in a functional way. Next to these functional descriptions it contains per use cases the generic reference to needed specific other C-Roads WG2 documentation, and it contains the harmonized use case specific settings.	3.0.0	30/06/2025	2.3.0
TF2/TF3	European Handbook for SPATEM and MAPEM creation This <u>informational</u> document builds upon the other C-Roads documentation to provide recommended practices for the use and application of the data structures of MAPEM and SPATEM to convey intersection topology and signalling information. It offers examples of	3.0.0	30/06/2025	2.3.0

	intersection configurations and how to describe them using the data elements available.			
TF3	C-ITS Message Profiles This document specifies the Facility Layer Service profiles used in C-Roads to implement the different Application Layer Services and Use Cases	3.0.0	30/06/2025	2.3.0
TF3	C-ITS Infrastructure Mobile ITS G5 System Profile This document specifies the requirements necessary for the realization of an interoperable, mobile roadside ITS-Station	3.0.0	30/06/2025	2.3.0
TF3	C-ITS Roadside ITS G5 System Profile This document specifies the requirements necessary for the realisation of an interoperable roadside ITS-Station, except for mobile roadside ITS-Stations	3.0.0	30/06/2025	2.3.0
TF4	C-ITS IP Based Interface Profile This document specifies the requirements and interface profiles necessary for the realisation of backend communication for service interoperability.	3.0.0	30/06/2025	2.3.0
TF5	C-ITS Cross-Border Testing and Validation Concept This document describes the overall Cross-Border Testing and Validation concept. It provides a clear scope and necessary distinctions for the interoperability testing of C-Roads. It elaborates on the framework of interoperability testing. Finally, it documents the processes how the testing requirements were derived and provides recommendations for the tests.	3.0.0	30/06/2025	2.3.0
TF5	C-ITS Test Plan This deliverable contains detailed test cases to validate the interoperability of C-ITS implementations.	3.0.0	30/06/2025	2.3.0
TF5	C-ITS Cross-Border Testing: PCAP Exchange Specification This document contains a common procedure to execute one step of the methodology for validating the cross-border interoperability of C-ITS services.	3.0.0	30/06/2025	2.3.0
TF5	C-ITS EU Interoperability Report (M24) This informational document summarizes the results of the interoperability tests that were held during the 2021's spring organized by different MS.	3.0.0	30/06/2025	2.3.0

2. Security requirements from reference documents

The requirements defined in this section apply to any C-Roads station regardless its trust level (L0, L1 or above). See section 2.4 of [C-ITS Security and Governance] for a summarized description of these levels that are defined in [CPOC protocol].

As defined in the C-Roads TF1 Security and Governance document, full compliance to the Certificate Policy [EU C-ITS CP], the Security Policy [EU C-ITS SP] and standards [ETSI TS 103 097][ETSI TS 102 941] is not required for L0 stations. However, the following requirements apply.

2.1 ETSI standards

Requirement

RS_SEC_001

C-ITS stations (including central C-ITS stations) shall comply to at least **ETSI TS 103 097** [ETSI TS 103 097] and **ETSI TS 102 941** [ETSI TS 102 941] standards.

Please note: A CA is used to issue certificates to backend C-ITS entities (i.e. central C-ITS stations) for message signing according to [ETSI TS 103 097]. Initially the specification only allowed signing on Geonetworking layer (according to [ETSI EN 302 636-4-1]). ETSI TS 103 630 also allows signing on facilities layer. However, at the time of publication C-ROADS only supports geonetworking layer signature, in order to support hybrid use cases. Signing at facility layer is studied by TF1/TF4 subgroup.

Requirement

RS_SEC_002

PKI shall comply to at least **ETSI TS 103 097** [ETSI TS 103 097] and **ETSI TS 102 941** [ETSI TS 102 941] standards.

Please note: The compliance to these standards is a prerequisite to any security test conducted in C-Roads. C-ITS station and PKI should have passed basic interoperability tests described in ETSI TS 103 600 [ETSI TS 103 600]. These tests can be done during the test phases specific to each Member State.

2.2 Certificate Policy

A full compliance to the Certificate Policy is not required in C-Roads L0 pilots. However, the following CP requirements (for stations enrolment and authorization) shall be covered to ensure the proper level of security in nominal scenarios.

2.2.1 Stations enrolment

Compliance to ETSI Security standards requires C-ITS stations to be enrolled in a PKI. This procedure may be different from a PKI provider to another.

Stations operators should check with PKI providers the prerequisites to stations enrolment. At least, a canonical name (under a format to be defined) and a technical key under RFC 5480 SubjectPublicKeyInfo format are required.

Requirement

RS_SEC_003

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

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

Requirement

RS_SEC_004

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

Requirement

RS_SEC_005

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

Requirement

RS_SEC_006

The C-ITS station shall update its Enrolment Credential (EC) in advance before the expiration of its current valid EC, when the remaining validity duration of its Enrolment Credential is less than or equal to 3 Months.

2.2.2 Authorization

Requirement

RS_SEC_007

AT key pair must be generated inside the HSM of the station. Stations shall request ATs according to the process described in TS 102 941 [ETSI TS 102 941].

Requirement

RS_SEC_008

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

Requirement

RS_SEC_009

EE subjects of ATs shall authenticate themselves when requesting ATs by using their unique enrolment private key. The AA shall forward the signature to the EA for validation; the EA shall validate it and confirm the result to the AA. Request protocol described in TS 102 941 [ETSI TS 102 941] shall be used by the EE and PKI.

Requirement

RS_SEC_010

The AA shall submit an authorisation validation request for each authorisation request it receives from an EE certificate subject according to TS 102 941 [ETSI TS 102 941]. The EA shall validate this request with respect to:

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

Requirement

RS_SEC_011

AT preloaded in the C-ITS station shall be compliant to [EU C-ITS CP].

Please note: For testing purposes (L0), AT's validity and preloading periods may be set to higher values to ease the management of stations during operations.

2.3 Security Policy

A full compliance to the Security Policy [EU C-ITS SP] is not required in C-Roads projects (L0). While the technical implementation according to the Certificate policy needs to be in line, the information security management system and related audit procedures are not required for testing purposes.

2.4 CPOC & TLM

In C-Roads projects (L0), implementation of the complete CPOC protocol [CPOC protocol] is not required. However, in order to be compatible with common European trust model entities (i.e. TLM and CPOC), any Root CA used in the context of C-Roads should at least comply to the fundamental CPOC protocol aspects specified in Annex I "Requirements & best practices of TLM certificates, RCA certificates and the ECTL" to the CPOC Protocol.

2.5 Specific security requirements

2.5.1 Certificate format and validity times

Requirement

RS_SEC_012

The certificates formats for CAs, ATs and ECs used for the C-Roads project are defined in ETSI TS 103 097 [ETSI TS 103 097]. Each C-ITS certificate is composed of several main fields:

- Version = 3,
- Issuer = sha256AndDigest, sha384AndDigest or certificate,
- CRA CA Id = 0x000000,
- CRL Series = 0,
- Validity start with duration,
- App Permissions,
- Cert Issue Permissions only for CAs, and
- Signature (NIST or Brainpool with 256 Bit or Brainpool with 384 Bit).

Each certificate shall contain the complete list of explicit permissions.

Requirement

RS_SEC_014

Validity times of CA's certificates shall be compliant with the CP [EU C-ITS CP] (section 7.2) amended by the CPOC protocol [CPOC protocol] (section I.6.3).

2.5.2 Cryptographic operations

Requirement

RS_SEC_015

Cryptographic operations defined in the CP [EU C-ITS CP] shall be supported.

2.5.3 Stations permissions

Permissions are provided to C-ITS stations through SSPs contained in AT certificates, used to sign messages.

As described on Figure 4:

- **Top down:** permissions of AT certificates are inherited from Certificate Authorities. AT certificates are submitted to restrictions and cannot contain permissions that AA and RCA do not have. Permissions of Certificate Authorities are described in section 2.5.4.
- **Bottom-up:** permissions of AT certificates must match use cases requirements. Use cases and related permissions are defined in the TF2 document "Service and Use Case Definitions" [C-Roads SUD].

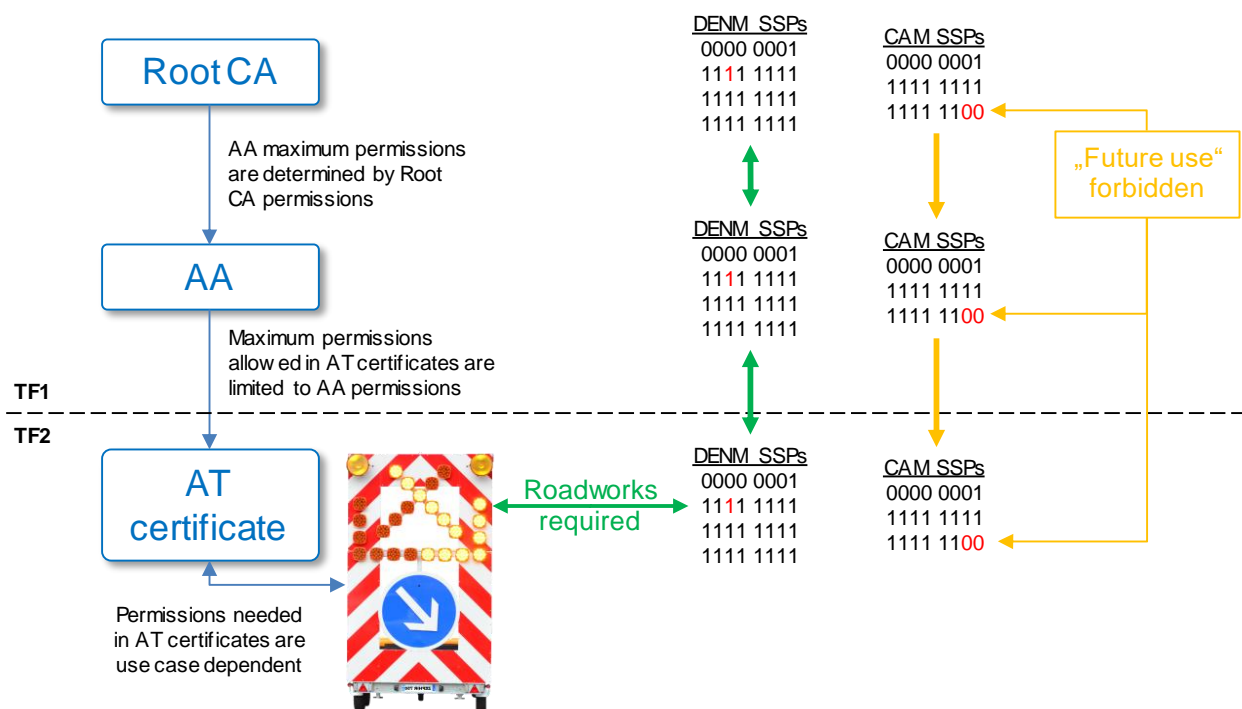


Figure 4: Definition and examples of C-ITS stations permissions

Requirement

RS_SEC_016

C-ITS stations shall use ATs with permissions (SSPs) in accordance with the use case / scenario as specified within TF2 document "Service and Use Case Definitions" [C-Roads SUD].

2.5.4 Certificate Authorities permissions

The field App Permissions contain the permission value in form of ITS-AID/PSID with SSP as long as specified for the respective ITS-AID. It needs to be considered that with ETSI TS 103 097 [ETSI TS 103 097] there is no certificate type explicitly given in the certificates. The App Permissions field defines for which operations the key related to the certificate is allowed to be used. In addition, a root CA certificate is distinguished from an EA and AA certificate based on the signer info set to self.

Requirement

RS_SEC_013a

The CA certificates shall contain Cert Issue Permissions which can be directly used by the CA to give them to the issued certificate into the App Permission field (EE Type set to app) or can be used in the enrolment process by an ITS station (EE Type set to enrol).

It needs to be considered that with ETSI TS 103 097 [ETSI TS 103 097] the end entity related to the EE Type is not necessarily the ITS station but can also be a CA if a specific permission end in the App Permission field of a CA certificate. Multiple elements of type Cert Issue Permission are used to distinguish between permissions that end in the directly issued certificates (permission with Minimum Chain Length = 1 and Chain Length Range = 0) or in certificates that are not directly issued by the certificate holder (permission with Minimum Chain Length > 1 and Chain Length Range = 0).

Requirement

RS_SEC_013b

The Chain Length Range shall be set in all CA certificates to 0.

Requirement

RS_SEC_013c

The Root CA shall ensure that no CA certificate has a Cert Issue Permission with SSP bit set to 0 and the related Bitmask bit set to 0 for all SSP values defined as bit list.

The Service Specific Permission (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the PSID. For example, there may be an SSP value associated with the PSID for CAM that indicates that the sender is entitled to send CAMs for a specific vehicle role. SSPs are used in certificate requests (get EC and get AT) and during initialization phase.

The first byte is the version number, indicating the list of supported SSPs. Details are given in each PSID standard.

Requirement

RS_SEC_013d

The maximum permissions of the Root CA are described in the annex I.4 of the CPOC Protocol [CPOC protocol]. For levels above level 0, the RCA certificate shall not have permissions that are not listed in [CPOC protocol].

The EA contains one cert issue permission element with EE Type = app that is given to the EC certificate into the app permission field. An EA with the permissions listed in the following Table 1 is permitted to issue EC certificates with all possible permissions.

Table 1 - Example of permissions contained in an EA certificate

App Permissions		sspValue (hex)	sspValue (binary)		
623	SCR	010E		0000 0001 0000 1110	
Explicit cert issue permissions with minimum chain length = 1 (default), chain length range = 0 (default) and end entity type = app (default)					
ITS-AID		sspValue (hex)	Bitmask (hex)	sspValue (binary)	Bitmask (binary)
623	SCR	01C0	FF3F	0000 0001 1100 0000	1111 1111 0011 1111

In addition, the EA and the Root CA certificates may contain in another cert issue permission element with EE Type = enrol all permissions that can be assigned to an ITS station registration. If the EA certificate would not contain the enrol permissions, the root CA could not limit the permissions of an EA, e.g. one EA is allowed to register stations with extended permissions and another EA is allowed to handle only normal private stations.

Table 2 - Example of permissions contained in an AA certificate

App Permissions		sspValue (hex)	sspValue (binary)		
623	SCR	0132		0000 0001 0011 0010	
Explicit cert issue permissions with minimum chain length = 1 (default), chain length range = 0 (default) and end entity type = app (default)					
Issue Permissions		sspValue (hex)	Bitmask (hex)	sspValue (binary)	Bitmask (binary)
36	CAM	01FFFC	FF0003	0000 0001 1111 1111 1111 1111 1100	1111 1111 0000 0000 0011
37	DENM	01FFFFFF	FF000000	0000 0001 1111 1111 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000
37	DENM	02FFFFFFF	FF00000000	0000 0010 1111 1111 1111 1111	1111 1111 0000 0000 0000

				1111 1111 1111 1111	0000 0000 0000 0000
137	TLM	01E0	FF1F	0000 0001 1110 0000	1111 1111 0001 1111
138	RLT	01C0	FF3F	0000 0001 1100 0000	1111 1111 0011 1111
139	IVI	01xxxxyyFFFF	FFwwwzzz0000	0000 0001 xxxx xxxx xxyy yyyy yyyy yyyy 1111 1111 1111 1111	1111 1111 wwww wwww wwzz zzzz zzzz zzzz 0000 0000 0000 0000
140	TLC Request Service	02FFFFFF8	FF000007	0000 0001 1111 1111 1111 1111 1111 1000	1111 1111 0000 0000 0000 0000 0000 0111
141	GN_MGM T				
637	TLC Status Service	01	FF	0000 0001	1111 1111

For IVI, the values 'x' and 'y' shall contain the serviceProviderID according to ETSI TS 103 301 V2.1. (i.e. three bytes, composed of a 10-bit country code according to ISO 3166-1 and a 14-bit provider ID according to ISO 14816). All 'x' and 'y' values may be set to 'F' to allow supporting all possible country codes and provider IDs. For these three specific SSP bytes the related bitmask value ('w' and 'z') might be set to 0.

Please note: The table above is an example of SSP values contained in AA certificate. It is up to the implementations to select the appropriate values, e.g. based on the services to be provided, their strategy of SSP assignment and potential organisational constraints.

Table 3 - Example of permissions contained in an EC certificate

App Permissions		sspValue (hex)	sspValue (binary)
623	SCR	01C0	0000 0001 1100 0000

2.5.5 Security initialisation

Requirement

RS_SEC_018

Receiving C-ITS stations shall operate the initial verifications as described in Annex A - Security initialisation steps.

2.5.6 Message signature

This section also applies to hybrid Basic Interface.

Requirement

RS_SEC_019

The C-ITS station shall use one end-to-end security header per message in accordance with [ETSI TS 103 097]

Requirement

RS_SEC_020

The signature shall be generated using a private key corresponding to a valid AT in accordance with clause 7.2.1 in [ETSI TS 103 097].

Please note: C2C-CC (*RS_BSP_170*) recommends using digital signatures and certificates based on ECDSA-256 using the elliptic curve NIST P-256, [EU C-ITS CP] also provides the option to use brainpoolP256r1 – a verification of both types is mandatory for the receiving station.

Requirement

RS_SEC_021

All addresses and identifiers of mobile stations transmitted shall be changed when the AT is changed according to section 6.5 of [ETSI TS 102 940].

To meet privacy requirements, a regular change of pseudonym certificates is required. Since there is no interoperability issue each member state should define its own pseudonym change strategy. Cf. [C-Roads_G Comm Pattern] for C-Roads presentation on the topic.

2.5.7 Verification of message signature

In section 2.2 (30), the Certificate Policy [EU C-ITS CP] requires the update of C-ITS stations with the ECTL and CRLs within a week of their publication.

C-ITS stations should check the availability of updated ECTL and CRLs in a higher frequency. Especially, it is recommended for RSUs to be closer to a daily frequency.

Requirement

RS_SEC_022

At each reception of message, C-ITS stations shall operate the signature verifications as described in Annex B - Signature verification steps. It is based on the section 5.2.3.2.1a *Signature verification of IEEE 1609-2*.

Requirement

RS_SEC_023

The C-ITS station shall forward only verified messages.

2.5.8 Permissions delegation

Requirement

RS_SEC_033

If a Service Provider (delegator) needs to authorize an ITS station of another Service Provider (delegate) to use certificates suitable to sign IVI messages with the content of the delegator, both the delegator and the delegate shall comply with C-ITS Delegation mechanism [C-ITS Security Requirements].

2.5.9 Cryptoagility

NIST and Brainpool curves may be used in signature and encryption algorithms as defined in [EU C-ITS CP] and [ETSI TS 103 097]. Different key sizes may also be used. This information can be explicitly derived during decoding of each received C-ITS message. During signature verification, the received packet can be decoded, and the signature is extracted, which is a CHOICE structure composed of `ecdsaNistP256Signature`, `ecdsaBrainpoolP256rlSignature` or `ecdsaBrainpoolP384rlSignature`.

2.5.10 Logging

Disclaimer: security logging requirements have to be discussed with TF5 on a broader level.

In case of failure during initialisation or signature verification, the C-ITS station should log the reason of the verification error.

Logs should at least include the type of error (e.g. invalid certificate, permissions mismatch) and the targeted element (e.g. TLM, ECTL, RCA, AA, AT).

Non exhaustive list of errors examples:

- Invalid TLM certificate
- Non trusted RCA
- Revoked AA
- RCA-AA permission mismatch
- Invalid message signature

2.6 Hybrid related requirements

The following requirements apply to C-ITS message exchanged on the Basic Interface as defined by TF4 [C-ITS IP Based Interface Profile].

Requirement

RS_SEC_024

C-ITS actors shall ensure the integrity of the information they exchange.

Requirement

RS_SEC_025

According to the European C-ITS Certificate Policy [EU C-ITS CP], individual messages transmitted on the Basic Interface shall be signed according to ETSI TS 103 097 [ETSI TS 103 097].

Please note: Since standards on the subject are evolving, please refer also to section 2.3 of the TF1 Security Governance document.

Requirement

RS_SEC_026

The originating ITS station shall sign and timestamp each message.

*Requirement**RS_SEC_027*

No signature change during message transport from the original sender to the final receiver shall be allowed.

*Requirement**RS_SEC_028*

When transmitting C-ITS messages via different channels (technologies/ networks) all specific ETSI certificates and IDs created with them shall be preserved to guarantee message authenticity.

2.7 Other vehicle stations requirements

A vehicle C-ITS station from series production should be securely linked to one specific vehicle. When the vehicle C-ITS station is powered, it should verify that it is operating in the vehicle with which it has been securely linked. If such correct functioning condition cannot be verified, the C-ITS station should be deactivated, preventing it from sending messages (i.e. deactivate at least the radio transmission level of the C-ITS station).

Please note: Securely linked means paired in the factory or in an authorized repair shop, which does not apply to retrofitted vehicles.

*Requirement**RS_SEC_029*

Requirement definition in progress

*Requirement**RS_SEC_030*

If the C-ITS station detects a collision of the least significant 32 bit of the "Certificate digest" / "hashedId8" with the "Certificate digest" / "hashedId8" of another ITS station (or C2CCC Basic System [C2C CC Vehicle C-ITS station]), it shall initiate a change of its authorization ticket if the certificate corresponding to the other "Certificate digest" / "hashedId8" is valid, if no such collision has triggered the current authorization ticket is used.

*Requirement**RS_SEC_031*

Facilities layer shall clear the own station's path history cache (used to fill into new messages) when the security entity changes its authorization ticket identity.

*Requirement**RS_SEC_032*

Applications shall be able to block the authorization ticket change as long as the vehicle does not move, i.e. PathPoint position information does not change. In other cases, applications shall only be able to block it for at most 5 minutes.

Exception:

- validity of the authorization ticket expired.
 - collision of "Certificate digest" / "hashedId8".
-

Annex A - Security initialisation steps

The TLM certificate is provided to the ITS-S during the initialization phase which is assumed to be valid and trustworthy.

- The ITS-S verifies that the issuer of the TLM certificate is set to self.
- The ITS-S verifies that the signature in the TLM certificate can be successfully verified with the public verification key provided in the TLM certificate.
- The ITS-S verifies that no Cert Issue Permissions are present in the TLM certificate.
- The ITS-S verifies that the start time of the TLM certificate is before the end time of the TLM certificate.
- The ITS-S verifies that the current time is equal to or after the start time of the TLM certificate.
- The ITS-S verifies that the current time is equal to or before the end time of the TLM certificate.

The ECTL is provided to the ITS-S during the initialization phase and is updated periodically according to the European C-ITS Certificate Policy release 1.1.

The home RCA certificate ID is provided to the ITS-S during the initialization phase. The ITS-S extracts the RCA certificate from the ECTL by using the ID. Alternatively, if the RCA certificate itself is provided to the ITS-S then the ITS-S must ensure that an exact copy of the RCA certificate is listed on the ECTL.

- The ITS-S verifies that the issuer of the RCA certificate is set to self.
- The ITS-S verifies that the signature in the RCA certificate can be successfully verified with the public verification key provided in the RCA certificate.
- The ITS-S verifies that the start time of the RCA certificate is before the end time of the RCA certificate.
- The ITS-S verifies that the current time is equal to or after the start time of the RCA certificate.
- The ITS-S verifies that the current time is equal to or before the end time of the RCA certificate.

The RCA-CTL is available in an RCA repository of each PKI operator.

The CRL is available in the RCA repository of each PKI operator and the ITS-S is equipped with a valid CRL of each RCA listed on the ECTL.

- For each Root CA Entry on the ECTL a DC Entry should be available on the ECTL, i.e. each RCA HashedId8 should be listed in at least one DC Entry Cert element.
- The operator of the ITS-S or the ITS-S itself connects periodically (i.e. every 48h) to all required DC URLs to download the CRL of each Root CA listed on the ECTL.
- The ITS-S verifies that the signer of the CRL is listed on the ECTL as RCA.
- The ITS-S verifies that the CRL signature can be successfully verified with the public verification key provided in the RCA certificate.

The ITS-S verifies that the PSID 622 with SSP value 0x01 is listed in the App Permission element of the RCA certificate.

- The ITS-S verifies that the start time of the RCA certificate is equal to or before the time given in the CRL for this update.
- The ITS-S verifies that the end time of the RCA certificate is equal to or after the time given in the CRL for next update.
- The ITS-S verifies that the start time of the RCA certificate is before the end time of the RCA certificate.
- The ITS-S verifies that the time given in the CRL for this update is before the time given in the CRL for next update.
- The ITS-S verifies that the current time is equal to or after the time given in the CRL for this update.
- The ITS-S verifies that the current time is equal to or before the time given in the CRL for next update.

The ITS-S shall verify that the ECTL is signed by the TLM.

- The ITS-S shall check the CTL format and the CTL sequence. If the format is set to FullCtl the ITS-S shall ensure that the latest ECTL (highest sequence number) is present. If the format is set to DeltaCtl the ITS-S shall ensure that all delta ECTLs with lower sequence numbers down to the last full ECTL (or sequence number = 0 if no full ECTL was processed previously) are present and will be checked with the following steps.
- The ITS-S verifies that the signer of the ECTL is the trusted and verified TLM certificate.
- The ITS-S verifies that the ECTL signature can be successfully verified with the public verification key provided in the TLM certificate.
- The ITS-S verifies that the PSID 624 is set in the ECTL header information.
- The ITS-S verifies that the PSID 624 with SSP value 0x01C8 is listed in the App Permission element of the TLM certificate.
- The ITS-S verifies that the start time of the TLM certificate is equal to or before the generation time given in the ECTL header information.
- The ITS-S verifies that the end time of the TLM certificate is equal to or after the time given in the ECTL for next update.
- The ITS-S verifies that the start time of the TLM certificate is before the end time of the TLM certificate.
- The ITS-S verifies that the generation time given in the ECTL header is before the time given in the ECTL for next update.
- The ITS-S verifies that the current time is equal to or after the generation time in the ECTL header information. The ITS-S verifies that the current time is equal to or before the time given in the ECTL for next update.

The ITS-S shall verify that the TLM link certificate is valid if present on the ECTL.

Please note: This section has been modified following the update of the CPOC protocol by the European Commission. Implementation of these updates is left optional in this version of security requirements.

- The ITS-S ensures that the old TLM certificate is present, as well as the new TLM certificate and the TLM link certificate. According to CPOC Protocol Release 1.1 the EU CCMS will provide different options to PKI participants to facilitate the update of their TLM Trust Anchors, i.e. the TLM Certificate.
- The ITS-S verifies the validity of the old and the new self-signed TLM certificates based on the steps above.
- The ITS-S verifies that the signer of the TLM link certificate message is set to the old TLM certificate.

- The ITS-S verifies that the certificate hash in the TLM link certificate is set to the new TLM certificate.
- The ITS-S verifies that the expiry time in the TLM link certificate is equal to the end of the validity period of the old TLM certificate that signs the TLM link certificate message.
- The ITS-S verifies that the signature in the TLM link certificate message can be successfully verified with the public verification key provided in the old TLM certificate.

The ITS-S shall verify that the RCA-CTL is signed by the home RCA.

- The ITS-S shall check the CTL format and the CTL sequence number. If the format is set to FullCtl the ITS-S shall ensure that the latest RCA-CTL (highest sequence number) is present. If the format is set to DeltaCtl the ITS-S shall ensure that all delta RCA-CTLs with lower sequence numbers down to the last full RCA-CTL (or sequence number = 0 if no full RCA-CTL was processed previously) are present and will be checked with the following steps.
- The ITS-S verifies that the signer of the RCA-CTL is the home RCA, which is listed on the ECTL.
- The ITS-S verifies that the RCA-CTL signature can be successfully verified with the public verification key provided in the RCA certificate.
- The ITS-S verifies that the PSID 624 is set in the RCA-CTL header information.
- The ITS-S verifies that the PSID 624 with SSP value 0x0138 is listed in the App Permission element of the RCA certificate.
- The ITS-S verifies that the start time of the RCA certificate is equal to or before the generation time given in the RCA-CTL header information.
- The ITS-S verifies that the end time of the RCA certificate is equal to or after the time given in the RCA-CTL for next update.
- The ITS-S verifies that the start time of the RCA certificate is before the end time of the RCA certificate.
- The ITS-S verifies that the generation time given in the RCA-CTL header is before the time given in the RCA-CTL for next update.
- The ITS-S verifies that the current time is equal to or after the generation time in the RCA-CTL header information.
- The ITS-S verifies that the current time is equal to or before the time given in the RCA-CTL for next update.

Annex B - Signature verification steps

All RCA certificates contained on the ECTL are stored as trust anchor in a secure way in order to prevent unauthorized modification or exchange, e.g. inside the HSM.

Step (1): The ITS-S receives a secured message and verifies the message signature with the associated AT certificate.

- The ITS-S verifies that the signer in the security header info matches with the AT certificate.
- The ITS-S verifies that the signature can be successfully verified with the public verification key provided in the AT certificate.
- The ITS-S verifies that the PSID in the security header info is listed in the App Permission element of the AT certificate.
- The ITS-S verifies that required SSP bits are set to 1 in the signer AT certificate if the received message contains the respective container or element. The content of the message payload (e.g. existence of an emergencyContainer) need to be compared with the SSP bits in the signer AT certificate.
- The ITS-S verifies that the start time of the AT certificate is equal to or before the generation time in the security header info.
- The ITS-S checks the existence of expiration time in the security header info. If it exists, then the ITS-S verifies that the end time of the AT certificate is equal to or after the optionally contained expiration time in the security header info.
- The ITS-S verifies that the start time of the AT certificate is before the end time of the AT certificate.
- The ITS-S checks the existence of expiration time in the security header info. If it exists, then the ITS-S verifies that the generation time in the security header info is before the optionally contained expiration time in the security header info.
- The ITS-S verifies that the transmission location is within the optionally contained region restriction of the AT certificate.

Step (2): The ITS-S verifies that the AT certificate is issued by an AA with a valid certificate (e.g.: presence of the right PSID list, time start and duration...). The AA certificate may be retrieved either from a V2X secured exchange (requestedCertificate) or from an RCA-CTL.

- The ITS-S verifies that the issuer in the AT certificate matches with the AA certificate.
- The ITS-S verifies that the issuer signature in the AT certificate can be successfully verified with the public verification key provided in the AA certificate.
- The ITS-S verifies that PSID 623 with SSP bit 2 and 3 (2nd byte, the 1st one being the version) are set in the App Permission element of the AA certificate.
- The ITS-S verifies that all PSID with related SSP values in the App Permission element of the AT certificate are listed in one of the Cert Issue Permission elements of the AA with appropriate chain length (e.g. Min Chain Length set to 1 and Chain Length Range set to 0) and EE Type set to App.
 - Check 1: For each SSP Bitmask bit set to 1 in the AA Cert Issue Permission the related SSP bit value in the AA certificate needs to be set in the AT certificate App Permission.

Issuer SSP bit:	0*	0*	0	0	1	1	1	1
Issuer bitmask bit:	0*	0*	1	1	0	0	1	1
Certificate App SSP bit:	0	1	0	1	0	1	0	1
Result of check at ITS-S	Not allowed		OK	NO	OK	OK	NO	OK

Check algorithm that is used to get the result			1	1			1	1
--	--	--	---	---	--	--	---	---

Figure 5: AA - AT app permission check

**Please note: The configuration SSP = 0 and Bitmask = 0 should not appear in CA certificates which should be enforced by the TLM, Root CA and AA. This does not apply to IVI ServiceProviderId SSPs, as noted in section 0,*

- The ITS-S verifies that the start time of the AA certificate is equal to or before the start time of the AT certificate.
- The ITS-S verifies that the end time of the AA certificate is equal to or after the end time of the AT certificate.
- The ITS-S verifies that the start time of the AA certificate is before the end time of the AA certificate.
- The ITS-S verifies that the start time of the AT certificate is before the end time of the AT certificate.
- If the AT certificate contains a region restriction the ITS-S verifies that this is within the region restriction of the AA certificate.
- If the AT certificate contains an assurance level the ITS-S verifies that this is equal to or smaller the assurance level contained in the AA certificate.
- The ITS-S verifies that a valid CRL is available and that the HashedID8 of the AA is not listed on this CRL.

Step (3): The ITS-S verifies that the AA certificate is issued by RCA.

- The ITS-S verifies that the issuer in the AA certificate matches with an RCA certificate listed in the ECTL.
- The ITS-S verifies that the issuer signature in the AA certificate can be successfully verified with the public verification key provided in the RCA certificate.
- The ITS-S verifies that all PSID with related SSP values in the App Permission element of the AA certificate are listed in one of the Cert Issue Permission elements of the RCA with appropriate chain length (e.g. Min Chain Length set to 1 and Chain Length Range set to 0 in RCA certificate) and EE Type set to App.
 - Check 1: For each SSP Bitmask bit set to 1 in the RCA Cert Issue Permission the related SSP bit value in the RCA certificate needs to be set in the AA certificate App Permission.

Issuer SSP bit:	0*	0*	0	0	1	1	1	1
Issuer bitmask bit:	0*	0*	1	1	0	0	1	1
Certificate App SSP bit:	0	1	0	1	0	1	0	1
Result of check at ITS-S	Not allowed		OK	NO K	OK	OK	NO K	OK
Check algorithm that is used to get the result			1	1			1	1

Figure 6: RCA - AA app permission check

**Please note: The configuration SSP = 0 and Bitmask = 0 should not appear in CA certificates which should be enforced by the TLM, Root CA and AA. This does not apply to IVI ServiceProviderId SSPs, as noted in section 0,*

- The ITS-S verifies that all PSID with related SSP values in the Cert Issue Permission element of the AA certificate are listed in one of the Cert Issue Permission elements of the RCA with appropriate chain

length where the chain length is decreased by one (e.g. Min Chain Length set to 2 and Chain Length Range set to 0 in RCA certificate) and EE Type set to App.

- Check 1: For each SSP Bitmask bit set to 1 in the RCA Cert Issue Permission the related SSP bit value in the RCA certificate needs to be set in the AA certificate Cert Issue SSP.
- Check 2: For each SSP Bitmask bit set to 1 in the RCA Cert Issue Permission this Bitmask value in the RCA certificate need to be set in the related AA certificate Cert Issue SSP Bitmask value.

Root SSP bit:	0*	0*	0*	0*	0	0	0	0	1	1	1	1	1	1	1	1
Root bitmask bit:	0*	0*	0*	0*	1	1	1	1	0	0	0	0	1	1	1	1
AA SSP bit:	0	0	1	1	0*	0	1	1	0*	0	1	1	0*	0	1	1
AA bitmask bit:	0	1	0	1	0*	1	0	1	0*	1	0	1	0*	1	0	1
Result of check at ITS-S	Not Allowed		NOK	NOK	NOK	OK	NOK	NOK	NOK	OK	OK	OK	NOK	NOK	NOK	OK
Check algorithm that is used to get the result					2	1, 2	1, 2	1					1, 2	1	2	1, 2

Figure 7: Cert issue permission Check

**Please note: The configuration SSP = 0 and Bitmask = 0 should not appear in CA certificates which should be enforced by the TLM, Root CA and AA. This does not apply to IVI ServiceProviderId SSPs, as noted in section 0,*

- The ITS-S verifies that the start time of the RCA certificate is equal to or before the start time of the AA certificate.
- The ITS-S verifies that the end time of the RCA certificate is equal to or after the end time of the AA certificate.
- The ITS-S verifies that the start time of the RCA certificate is before the end time of the RCA certificate.
- The ITS-S verifies that the start time of the AA certificate is before the end time of the AA certificate.
- If the AA certificate contains a region restriction the ITS-S verifies that this is within the region restriction of the RCA certificate.
- If the AA certificate contains an assurance level the ITS-S verifies that this is equal to or smaller the assurance level contained in the RCA certificate.
- The ITS-S verifies that a valid CRL is available and that the HashedID8 of the RCA is not listed on this CRL.

Step (4): The ITS-S verifies the RCA certificate

- The ITS-S verifies that the issuer of the RCA certificate is set to self.
- The ITS-S verifies that the signature in the RCA certificate can be successfully verified with the public verification key provided in the RCA certificate.
- The ITS-S verifies that the start time of the RCA certificate is before the end time of the RCA certificate.
- The ITS-S verifies that the current time is equal to or after the start time of the RCA certificate.
- The ITS-S verifies that the current time is equal to or before the end time of the RCA certificate.

At every step of this procedure, if one verification fails, then the signed message must be considered as invalid and must be rejected by the ITS-S.

Post-conditions

The ITS-S has verified the integrity of the received message by validating the signature of the secured message as well as its authenticity by validating the certificate trust chain. The authorization of the message sender needs to be checked by the application which verifies that the required ITS-AID and SSP values are set in the sender's AT certificate.

Annex C - Certificate examples

The following decoded example certificates illustrate the contents of CA certificates used in C-Roads.

Example of Root CA certificate

```
EtsiTs103097Certificate ::= {
  version 3,
  type explicit,
  issuer self : sha256,
  toBeSigned {
    id name : "BSI V2X Pilot PKI Root",
    cracaId '000000'H,
    crlSeries 0,
    validityPeriod {
      start 477215871,
      duration hours : 17544
    },
    appPermissions {
      {
        psid 624,
        ssp bitmapSsp : '0138'H
      },
      {
        psid 622,
        ssp bitmapSsp : '01'H
      }
    },
    certIssuePermissions {
      {
        subjectPermissions explicit : {
          {
            psid 36,
            sspRange bitmapSspRange : {
              sspValue '01FFFC'H,
              sspBitmask 'FF0003'H
            }
          },
          {
            psid 37,
            sspRange bitmapSspRange : {
              sspValue '01FFFFFF'H,
              sspBitmask 'FF000000'H
            }
          },
          {
            psid 137,
            sspRange bitmapSspRange : {
              sspValue '01E0'H,
              sspBitmask 'FF1F'H
            }
          }
        }
      }
    }
  }
}
```

```

{
  psid 138,
  sspRange bitmapSspRange : {
    sspValue '01C0'H,
    sspBitmask 'FF3F'H
  }
},
{
  psid 139,
  sspRange bitmapSspRange : {
    sspValue '01940000FFF8'H,
    sspBitmask 'FF0000000007'H
  }
},
{
  psid 140,
  sspRange bitmapSspRange : {
    sspValue '01FFFFE0'H,
    sspBitmask 'FF00001F'H
  }
},
{
  psid 141
},
{
  psid 623,
  sspRange bitmapSspRange : {
    sspValue '01C0'H,
    sspBitmask 'FF3F'H
  }
}
},
minChainLength 2,
eeType {app}
},
{
  subjectPermissions explicit : {
    {
      psid 623,
      sspRange bitmapSspRange : {
        sspValue '013E'H,
        sspBitmask 'FFC1'H
      }
    }
  }
}
},
verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'9ACFAF8ADEA9C44C205A09BB7C62C694DE3E4B97AEBF48B9A4D3A3A422BAECA0'H
},
signature ecdsaBrainpoolP256r1Signature : {
  rSig x-only :
'72FCEE7A523D048A9126103D36679B823F8277439BDA9A797DA673E0988244E'H,
  sSig
'4A9E4F88DD1AA1B90B6416736D097C71BC0BEB08A39A6C23C470E0E4AD9D48D5'H

```

```
}
}
```

Example of EA certificate

```
EtsiTsl03097Certificate ::= {
  version 3,
  type explicit,
  issuer sha256AndDigest : '35F33313404A473C'H,
  toBeSigned {
    id name : "BSI V2X Pilot PKI EA",
    cracaId '000000'H,
    crlSeries 0,
    validityPeriod {
      start 477243000,
      duration hours : 13128
    },
    appPermissions {
      {
        psid 623,
        ssp bitmapSsp : '010E'H
      }
    },
    certIssuePermissions {
      {
        subjectPermissions explicit : {
          {
            psid 623,
            sspRange bitmapSspRange : {
              sspValue '01C0'H,
              sspBitmask 'FF3F'H
            }
          }
        }
      }
    },
    encryptionKey {
      supportedSymmAlg aes128Ccm,
      publicKey eciesBrainpoolP256r1 : compressed-y-1 :
'A6EAC551C411D02C43B97B8F25F8B64155449D9F11E4E4855F5193FA9B12D910'H
    },
    verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'93B2A4C9E1D1F434C3DDA1DF03D413A2040F110291C057F10849AAA1D5EA12ED'H
    },
    signature ecdsaBrainpoolP256r1Signature : {
      rSig x-only :
'29602DE33CF5E0B5222EB6ED9166692ECF493872C8AB7804119E054CBACA73C6'H,
      sSig
'784FEC48A1E43E4C4071AF620DBBC34A7FB73480BE1835724BDB0CFBDCEA4B7A'H
    }
  }
}
```

Example of AA certificate

```
EtsiTs103097Certificate ::= {
  version 3,
  type explicit,
  issuer sha256AndDigest : '35F33313404A473C'H,
  toBeSigned {
    id name : "BSI V2X Pilot PKI AA",
    cracaId '000000'H,
    crlSeries 0,
    validityPeriod {
      start 477243242,
      duration hours : 8760
    },
    appPermissions {
      {
        psid 623,
        ssp bitmapSsp : '0132'H
      }
    },
    certIssuePermissions {
      {
        subjectPermissions explicit : {
          {
            psid 36,
            sspRange bitmapSspRange : {
              sspValue '01FFFC'H,
              sspBitmask 'FF0003'H
            }
          },
          {
            psid 37,
            sspRange bitmapSspRange : {
              sspValue '01FFFFFF'H,
              sspBitmask 'FF000000'H
            }
          },
          {
            psid 137,
            sspRange bitmapSspRange : {
              sspValue '01E0'H,
              sspBitmask 'FF1F'H
            }
          },
          {
            psid 138,
            sspRange bitmapSspRange : {
              sspValue '01C0'H,
              sspBitmask 'FF3F'H
            }
          },
          {
            psid 139,
            sspRange bitmapSspRange : {
```

```

        sspValue '01940000FFF8'H,
        sspBitmask 'FF0000000007'H
    }
},
{
    psid 140,
    sspRange bitmapSspRange : {
        sspValue '01FFFFE0'H,
        sspBitmask 'FF00001F'H
    }
},
{
    psid 141
}
}
},
encryptionKey {
    supportedSymmAlg aes128Ccm,
    publicKey eciesNistP256 : compressed-y-1 :
'7C6A29E10B28C6B5EDE509879096862BACA2B017CBAB304C16F12D173C81151D'H
},
verifyKeyIndicator verificationKey : ecdsaNistP256 : compressed-y-
1 :
'D3432034D3D5C80F660076BEF8BC06306EA5D2E3A611B21B269B443918EFA29B'H
},
signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'6D4425E909516CDF1CCD204BCD865FA7807CD76A6DAD8FF670392918C8ECC29B'H,
    sSig
'60A2701A5EBC9CD37BA3ED18C9B2BDF44F92D9EB22DAE58239AD52E1B7FA9042'H
}
}

```

Example of RCA-CTL

```

RcaCertificateTrustListMessage ::= {
    protocolVersion 3,
    content signedData : {
        hashId sha256,
        tbsData {
            payload {
                data {
                    protocolVersion 3,
                    content unsecuredData : CONTAINING {
                        version v1,
                        content certificateTrustListRca : {
                            version v1,
                            nextUpdate 485016345,
                            isFullCtl TRUE,
                            ctlSequence 0,
                            ctlCommands {
                                add : ea : {
                                    eaCertificate {

```

```

version 3,
type explicit,
issuer sha256AndDigest : '35F33313404A473C'H,
toBeSigned {
  id name : "Test BSI V2X Pilot PKI EA",
  cracaId '000000'H,
  crlSeries 0,
  validityPeriod {
    start 477243000,
    duration hours : 13128
  },
  appPermissions {
    {
      psid 623,
      ssp bitmapSsp : '010E'H
    }
  },
  certIssuePermissions {
    {
      subjectPermissions explicit : {
        {
          psid 623,
          sspRange bitmapSspRange : {
            sspValue '01C0'H,
            sspBitmask 'FF3F'H
          }
        }
      }
    }
  },
  encryptionKey {
    supportedSymmAlg aes128Ccm,
    publicKey eciesBrainpoolP256r1 : compressed-y-
1 :
'A6EAC551C411D02C43B97B8F25F8B64155449D9F11E4E4855F5193FA9B12D910'H
  },
  verifyKeyIndicator verificationKey :
ecdsaBrainpoolP256r1 : compressed-y-1 :
'93B2A4C9E1D1F434C3DDA1DF03D413A2040F110291C057F10849AAA1D5EA12ED'H
  },
  signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'29602DE33CF5E0B5222EB6ED9166692ECF493872C8AB7804119E054CBACA73C6'H,
    sSig
'784FEC48A1E43E4C4071AF620DBBC34A7FB73480BE1835724BDB0CFBDCEA4B7A'H
  }
  },
  aaAccessPoint "http://test.bsi.v2x-pilot.escript.c"
-- truncated --,
  itsAccessPoint "http://test.bsi.v2x-pilot.escript.c"
-- truncated --
  },
  add : aa : {
    aaCertificate {
      version 3,

```



```

type explicit,
issuer sha256AndDigest : '35F33313404A473C'H,
toBeSigned {
  id name : "Test BSI V2X Pilot PKI AA",
  cracaId '000000'H,
  crlSeries 0,
  validityPeriod {
    start 477243242,
    duration hours : 8760
  },
  appPermissions {
    {
      psid 623,
      ssp bitmapSsp : '0132'H
    }
  },
  certIssuePermissions {
    {
      subjectPermissions explicit : {
        {
          psid 36,
          sspRange bitmapSspRange : {
            sspValue '01FFFC'H,
            sspBitmask 'FF0003'H
          }
        },
        {
          psid 37,
          sspRange bitmapSspRange : {
            sspValue '01FFFFFF'H,
            sspBitmask 'FF000000'H
          }
        },
        {
          psid 137,
          sspRange bitmapSspRange : {
            sspValue '01E0'H,
            sspBitmask 'FF1F'H
          }
        },
        {
          psid 138,
          sspRange bitmapSspRange : {
            sspValue '01C0'H,
            sspBitmask 'FF3F'H
          }
        },
        {
          psid 139,
          sspRange bitmapSspRange : {
            sspValue '01940000FFF8'H,
            sspBitmask 'FF0000000007'H
          }
        },
        {
          psid 140,

```

```

        sspRange bitmapSspRange : {
            sspValue '01FFFFE0'H,
            sspBitmask 'FF00001F'H
        }
    },
    {
        psid 141
    }
}
},
encryptionKey {
    supportedSymmAlg aes128Ccm,
    publicKey eciesNistP256 : compressed-y-1 :
'7C6A29E10B28C6B5EDE509879096862BACA2B017CBAB304C16F12D173C81151D'H
    },
    verifyKeyIndicator verificationKey :
ecdsaNistP256 : compressed-y-1 :
'D3432034D3D5C80F660076BEF8BC06306EA5D2E3A611B21B269B443918EFA29B'H
    },
    signature ecdsaBrainpoolP256r1Signature : {
        rSig x-only :
'6D4425E909516CDF1CCD204BCD865FA7807CD76A6DAD8FF670392918C8ECC29B'H,
        sSig
'60A2701A5EBC9CD37BA3ED18C9B2BDF44F92D9EB22DAE58239AD52E1B7FA9042'H
    }
},
accessPoint "http://test.bsi.v2x-pilot.escript.c" --
truncated --
    },
    add : dc : {
        url "http://test.bsi.v2x-pilot.escript.c" --
truncated --,
        cert {
            '35F33313404A473C'H
        }
    }
}
}
},
headerInfo {
    psid 624,
    generationTime 477240345929000
}
},
signer certificate : {
    {
        version 3,
        type explicit,
        issuer self : sha256,
        toBeSigned {
            id name : "Test BSI V2X Pilot PKI Root",
            cracaId '000000'H,
            crlSeries 0,

```

```

validityPeriod {
    start 477215871,
    duration hours : 17544
},
appPermissions {
    {
        psid 624,
        ssp bitmapSsp : '0138'H
    },
    {
        psid 622,
        ssp bitmapSsp : '01'H
    }
},
certIssuePermissions {
    {
        subjectPermissions explicit : {
            {
                psid 36,
                sspRange bitmapSspRange : {
                    sspValue '01FFFC'H,
                    sspBitmask 'FF0003'H
                }
            },
            {
                psid 37,
                sspRange bitmapSspRange : {
                    sspValue '01FFFFFF'H,
                    sspBitmask 'FF000000'H
                }
            },
            {
                psid 137,
                sspRange bitmapSspRange : {
                    sspValue '01E0'H,
                    sspBitmask 'FF1F'H
                }
            },
            {
                psid 138,
                sspRange bitmapSspRange : {
                    sspValue '01C0'H,
                    sspBitmask 'FF3F'H
                }
            },
            {
                psid 139,
                sspRange bitmapSspRange : {
                    sspValue '01940000FFF8'H,
                    sspBitmask 'FF0000000007'H
                }
            },
            {
                psid 140,
                sspRange bitmapSspRange : {
                    sspValue '01FFFFE0'H,

```

```

        sspBitmask 'FF00001F'H
    },
    {
        psid 141
    },
    {
        psid 623,
        sspRange bitmapSspRange : {
            sspValue '01C0'H,
            sspBitmask 'FF3F'H
        }
    },
    minChainLength 2,
    eeType {app}
},
{
    subjectPermissions explicit : {
        {
            psid 623,
            sspRange bitmapSspRange : {
                sspValue '013E'H,
                sspBitmask 'FFC1'H
            }
        }
    }
},
verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'9ACFAF8ADEA9C44C205A09BB7C62C694DE3E4B97AEBF48B9A4D3A3A422BAECA0'H
},
signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'72FCEE7A523D048A9126103D36679B823F8277439BDA9A797DA673E0988244E'H,
    sSig
'4A9E4F88DD1AA1B90B6416736D097C71BC0BEB08A39A6C23C470E0E4AD9D48D5'H
}
},
signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'1D537B5E5A2FEFAF2FC12CF7E2AAAD98A3B699E7C2707719C4F27BFEB785A8BE'H,
    sSig
'9EAFE59AD1F51FF122F16E988D70B6286987EBE93F57F3B0BF1F1072B2543544'H
}
}
}

```

Example of CRL

```
CertificateRevocationListMessage ::= {
```

```

protocolVersion 3,
content signedData : {
  hashId sha256,
  tbsData {
    payload {
      data {
        protocolVersion 3,
        content unsecuredData : CONTAINING {
          version v1,
          content certificateRevocationList : {
            version v1,
            thisUpdate 477843763,
            nextUpdate 485619763,
            entries {
              '7044E6B91D9E3DC6'H
            }
          }
        }
      }
    },
    headerInfo {
      psid 622,
      generationTime 477843763856000
    }
  },
  signer certificate : {
    {
      version 3,
      type explicit,
      issuer self : sha256,
      toBeSigned {
        id name : "Test BSI V2X Pilot PKI Root",
        cracaId '000000'H,
        crlSeries 0,
        validityPeriod {
          start 477215871,
          duration hours : 17544
        },
      },
      appPermissions {
        {
          psid 624,
          ssp bitmapSsp : '0138'H
        },
        {
          psid 622,
          ssp bitmapSsp : '01'H
        }
      },
      certIssuePermissions {
        {
          subjectPermissions explicit : {
            {
              psid 36,
              sspRange bitmapSspRange : {
                sspValue '01FFFC'H,
                sspBitmask 'FF0003'H
              }
            }
          }
        }
      }
    }
  }
}

```

```

    }
  },
  {
    psid 37,
    sspRange bitmapSspRange : {
      sspValue '01FFFFFF'H,
      sspBitmask 'FF000000'H
    }
  },
  {
    psid 137,
    sspRange bitmapSspRange : {
      sspValue '01E0'H,
      sspBitmask 'FF1F'H
    }
  },
  {
    psid 138,
    sspRange bitmapSspRange : {
      sspValue '01C0'H,
      sspBitmask 'FF3F'H
    }
  },
  {
    psid 139,
    sspRange bitmapSspRange : {
      sspValue '01940000FFF8'H,
      sspBitmask 'FF0000000007'H
    }
  },
  {
    psid 140,
    sspRange bitmapSspRange : {
      sspValue '01FFFFE0'H,
      sspBitmask 'FF00001F'H
    }
  },
  {
    psid 141
  },
  {
    psid 623,
    sspRange bitmapSspRange : {
      sspValue '01C0'H,
      sspBitmask 'FF3F'H
    }
  }
},
minChainLength 2,
eeType {app}
},
{
  subjectPermissions explicit : {
    {
      psid 623,
      sspRange bitmapSspRange : {

```

```

        sspValue '013E'H,
        sspBitmask 'FFC1'H
    }
}
}
},
    verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'9ACFAF8ADEA9C44C205A09BB7C62C694DE3E4B97AEBF48B9A4D3A3A422BAECA0'H
    },
    signature ecdsaBrainpoolP256r1Signature : {
        rSig x-only :
'72FCEEA7A523D048A9126103D36679B823F8277439BDA9A797DA673E0988244E'H,
        sSig
'4A9E4F88DD1AA1B90B6416736D097C71BC0BEB08A39A6C23C470E0E4AD9D48D5'H
    }
}
},
    signature ecdsaBrainpoolP256r1Signature : {
        rSig x-only :
'A54E0C59CE3AD8C5D9660112C8546F6EF853FE837D2901F64ABB7FA4A23DD0DD'H,
        sSig
'14EF3E9BA921537CAFDDA39FFEA81E4A1A2F979FFAD7C69E194AF2F9D4B0E543'H
    }
}
}

```