Draft Report on European Security Mechanism

Version 1.3

Working Group 2, Task Force 1 Report

4th December 2018

Co-financed by the European Union
Connecting Europe Facility

Table of Content

Disclaimer

The Annexes A and B represent the current status and might be subject to changes in later releases.

The security aspects described in the Annexes must match the functional (TF2) and technical (TF3) specifications for all services and use cases covered by C-Roads. Since not all C-Roads services have been detailed in the current release of documents, some services are neither implemented in a harmonized way nor tested yet, Nevertheless, all the detailed security specifications need to be validated in actual tests. The number and depth of test cases for the different services and use cases will increase (TF5). Therefore the Annexes will have to evolve based on experience and best practises derived from actual tests.

Document history

Version	Date	Description, updates and changes	Status
0.3	28.08.2017	First draft for telco	Draft
0.4	07.09.2017	New structure according to discussions at Paris meeting, Atech Scope section completed, four chapters with lead editors	Draft
0.41	15.10.2017	Chapter 4 input by M. Medina, comments M. Helene Badiali, IDNomic	Draft
0.5	17.10.2017	Chapter 3 input by A. Froetscher, Atech	Draft
0.6	Oct./Nov. 2017	Chapter 5 outlined by N. Bissmeyer, Comments received from G. Ampt, M.H. Badiali	Draft
0.7	20.11.2017	Consolidated version after TF1 conference call , input received from X	Draft
0.8	20.12.2017	Update chapter 2, and comments Atech	Draft
0.83	15.02.2018	Update chapter 3, including statements from C-Roads members	Draft
0.85		Updated content in various chapters	Draft
0.90	March/April 2018	TF3 Eindhoven Meeting, changes discussed and accepted	Draft
0.95		TF1 Telco and accepted changes and comments	Draft
0.99b		TF1 and aspects of X-Test Reims inn chapter 2.6 included	Draft
1.0	Sep. 2018	UK comments and native speaker review	Draft
1.1	Sep. 2018	Annex B included, document upated according to French comments and feedback from Nordic countries	Draft
1.2	Nov. 2018	Resolving remaining French comments, structural alignment of annexes, document clean-up	Draft
1.3	Dec. 2018	Following the WG2 agreement, a disclaimer has been added explaining the current status of the Annexes and the vehicle station type has been removed from the SSP specifications	For approval

Scope of this TF1 security document

This document describes security aspects that are specific to the domain of cooperative intelligent transport systems (C-ITS), especially addressing the needs of the European C-Roads pilots, whether they are based on short-range communication (ETSI ITS G5) or existing cellular networks (3G/4G). The main focus of this document is to identify the requirements for the interoperability of different C-Roads pilotsand the technical specification needed to implement the harmonized solution in all C-Roads pilots.

This report mainly covers the security of ETSI ITS G5 communication. Within this it references the common EU Trust Model, the related requirements for Public Key Infrastructure (PKI) and the technical and organisational elements linked to it. The next version of this report will also consider cellular network technologies in more detail, so that the general provisions for a future "hybrid" communication approach between road infrastructures and vehicles in C-ITS are included.

Introduction

The security task force of work group 2 of C-Roads was tasked with describing the overall security solution for secure and trustful communication between C-ITS stations in a pilot phase.

The C-ITS security aspects described within this document are based on two documents from the EU C-ITS platform phase two the CP – its Certificate Policy (CP) and its Security Policy (SP). Further reference documents are ETSI and CEN/ISO standards that provide security requirements for the use of a PKI to secure V2X communications.

This report concentrates on the implementation of the European C-ITS CP and SP in the C-Roads pilots, including full lifecycle security, e.g. the process steps to register, start-up, operate (including updates) and decommission C-ITS stations and the respective secure certificate materials at the end of their lifetime.

The next version of this report will give advice regarding the "hardening" (logical and physical) of C-ITS stations against misuse of the C-ITS station by external parties under any circumstances. Future versions of this report will also need to look at how trust in the wider ecosystem can be established.

This report does not provide a comprehensive list containing all overall "cybersecurity aspects" of C-ITS stations and technical elements and the necessary provisions for preventing general IT security attacks. Out of scope of this report are topics which are not (yet) included in the EU CP. This includes: misbehaviour detection of single ITS stations; misuse of certificates; intrusion detection; security for the integration of C-ITS stations into other systems; misuse of the entities within the EU Trust Model.

List of used abbreviations

AA	Authorization Authority
API	Application Programming Interface
CA	Certificate Authority
C-ITS	Cooperative ITS
CP	Certificate Policy
CPA	Certificate Policy Authority
CPS	Certificate Practice Statement
CPOC	C-ITS Point Of Contact
CTL	Certificate Trust List
EA	Enrolment Authority
ECTL	European Certificate Trust List
GDPR	General Data Protection Regulation
ITS	Intelligent Transport System
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
TF1	Task Force 1
TLM	Trust List Manager
WG2	Working Group 2

1 Gap analysis for interoperable security within the EU-C-ITS system

The purpose of this chapter is to compare the security specifications of C-ITS defined by C-ITS platform with all available implementations from C-Roads partners. Existing PKI solutions with their status and the planned efforts for piloting for C-Roads members are provided in more detail in [1] and in Section 2 of the current document.

The main interoperability aspects considered within this analysis are:

- Architecture and Technical specifications
- Governance

More details about the Gap analysis operation are provided in deliverable [1].

1.1 Gap analysis for hybrid communications

Currently the term “C-ITS” is defined in the common European policy documents by referencing ETSI EN 302 665 with the phrase “functional entity specified by the ITS station (ITS-S) reference architecture” [2, 3]. Currently this is applicable for ETSI ITS G5 communication based on IEEE 802.11p in the 5.9 GHz band, whereas security mechanisms covering a hybrid communication system still need to be defined.

For hybrid communication systems, a distinction may need to be made between backend/cloud-based solutions relying on existing 3G/4G (UMTS/LTE) networks and and those that will use developing telecommunication technologies, i.e. LTE-V2X/C-V2X or 5G “new radio” technologies. Security approaches relevant for LTE-V2X/C-V2X and 5G technologies still need to be determined.

For communication to and between backend systems, potentially using cloud services and neutral servers, message content and quality need to correspond to agreed guidelines. Appropriate security mechanisms are required to assure that only thrustworthy parties interact with such “interchange nodes”, and that confidentiality, integrity and authenticity of content is maintained.

Since the architecture of a future hybrid communication system is still open, also the security aspects have not yet been figured out. This needs to be done in close collaboration with Task Force 4 of C-Roads Working Group 2.

1.2 Existing standards

Within the context of TF1, a deep analysis of the existing security standards is required. A careful definition of any additional elements is needed for the implementation of security in the C-Roads pilots.

The main interoperability requirements detailed in existing standards are summarized in the following Table 1. A full list of TF1 standards is provided in [4].

Specifications	Details
Governance	Security Policy & Governance Framework Release 1
Trust Model	Certificate Policy Release 1.1

Certificate Data Structure	ETSI TS 103 097 v.1.2.1 ETSI TS 103 097 v.1.3.1
Cryptographic Algorithms	ETSI TS 103 097 v.1.2.1 (NIST only) ETSI TS 103 097 v.1.3.1 (NIST / Brainpool) Certificate Policy v1.1
Download C-Roads CTL	ETSI TS 102 941 (1.2.1)
Download C-Roads CRL	ETSI TS 102 941 (1.2.1)
C-Roads CTL data structure	ETSI TS 102 941 (1.2.1)
C-Roads CRL data structure	ETSI TS 102 941 (1.2.1)

Table 1: Main Interoperability Requirements

1.2.1 The impact of ETSI TS 103 097 1.3.1 implementation

One specific gap concerns the choice of ETSI TS 103 097 version. In order to decide the C-Roads certificate data structure version, the impact of the migration of ETSI TS 103 097 from version 1.2.1 to version 1.3.1 has been studied.

The following consequences can directly be derived from the choice to implement the ETSI TS 103 097 version 1.3.1:

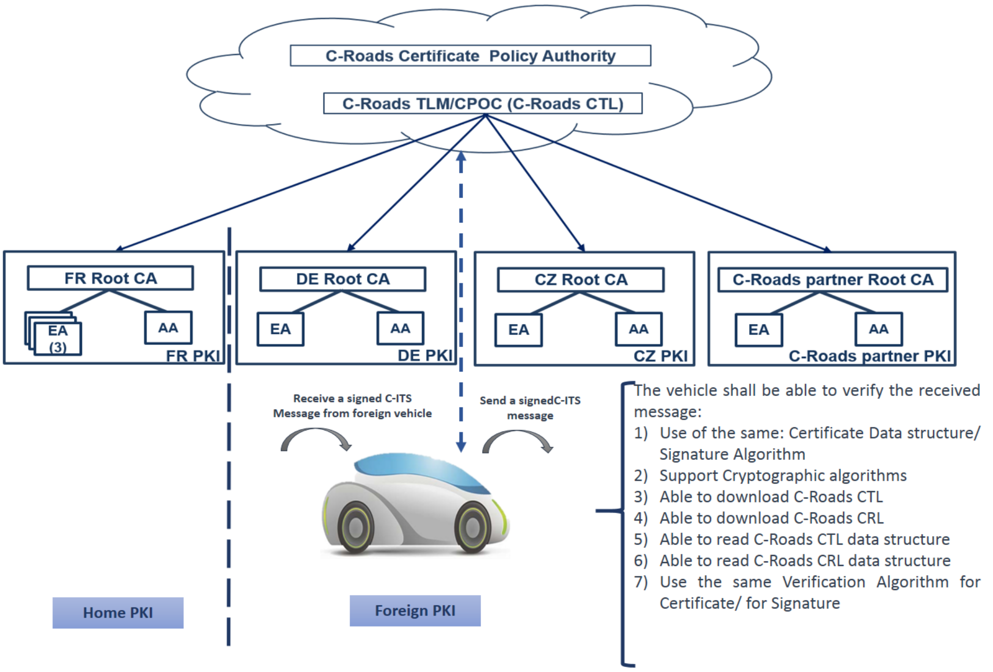
- If ETSI TS 103 097 v 1.3.1 is selected then the new version of ETSI TS102 941 v1.2.1 shall be implemented.
- In order to match ETSI TS 103 097 v1.3.1, the certificate verification has been updated in ETSI TS 102 941 v1.2.1. Also other PKI management protocols are not backward compatible with ETSI TS 102 941 v1.1.1.
- Updating from the previous versions of those two standards to the newly released versions causes a significant impact on pilots sites, since new implementations (PKI side and ITS-S side) are required and all home PKI requests and responses (AT request, EC request, etc.…) will change. Relevant differences are covered in the detailed specifications in Annex A and Annex B.

Due to the significant impact on existing implementations, a migration plan shall be defined, in the context of C-Roads TF1, enabling all C-Roads partners to switch to ETSI TS 103 097 v1.3.1 before the end of the project.

This is of particular importance as all EU common elements provided by the European Commission in its pilot setup of CPOC, TLM (i.e. access to ECTL) and EU Root-CA will exclusively support ETSI TS 103 097 v1.3.1 and the corresponding version of ETSI TS 102 941 (v1.2.1).

1.3 Other areas identified in the gap analysis

As indicated in figure below, there are several security interoperability aspects that need to be further considered.


C-Roads Certificate Policy Authority
C-Roads TLM/CPOC (C-Roads CTL)
FR Root CA
EA (3)
AA
FR PKI
DE Root CA
EA
AA
DE PKI
CZ Root CA
EA
AA
CZ PKI
C-Roads partner Root CA
EA
AA
C-Roads partner PKI
Receive a signed C-ITS Message from foreign vehicle
Send a signedC-ITS message
Home PKI
Foreign PKI

The vehicle shall be able to verify the received message:

1) Use of the same: Certificate Data structure/ Signature Algorithm
2) Support Cryptographic algorithms
3) Able to download C-Roads CTL
4) Able to download C-Roads CRL
5) Able to read C-Roads CTL data structure
6) Able to read C-Roads CRL data structure
7) Use the same Verification Algorithm for Certificate/ for Signature

Figure 1: C-Roads Interoperability Process

1.4 Governance

In C-Roads TF1, the classification and the definition of roles indicated in [3] has been adopted (see chapter 3), some more details about the essential roles are provided in [1].

There are central entities foreseen in CP and SP which are missing, in particular the following:

- TLM – Trust List Manager
- CPOC – C-ITS Point of Contact

These will need tobe developed commonly with the European Commission based on ETSI TS 103 097 1.3.1 and ETSI TS 102 941 1.2.1

Co-financed by the European Union
Connecting Europe Facility

2 C-ITS security aspects for the piloting phase

This chapter contains the main elements for guaranteeing basic security for the communication in a C-ITS network during the piloting phase of C-Roads.It will try to identify those aspects of the EU CP document which need to be further developed for the piloting of C-ITS. It will also identify elements which need to be validated during this phase in order to prepare for the full operative roll out of C-ITS on roads in Europe.

2.1 Functional security requirements for C-ITS

As a starting point it needs to be stated that the functional security requirements for I2V and V2V communication are similar, in most of the aspects even the same for all ITS stations involved. Since there are several ITS station types forming a communication network, e.g. C-ITS-S, R-ITS-S and V-ITS-S, there is also a number of “network operators” which collectively are performing the required tasks, including the security related duties of a network operator of a communication network. One major difference regarding the various station types is concerning potential privacy issues, i.e. the risk of tracking C-ITS stations. Therefore “normal” vehicle C-ITS stations, which are operated for the provision of C-ITS services to (private) end users, need to change their (pseudonymous) identities in C-ITS messages according to requirements given in the CP and/or the Basic System Profile of C2C-CC. This privacy requirement is not necessarily applicable for road side stations or road operator vehicles.

The “Day One C-ITS services” as basically defined in the C-ITS Strategy [5] COM (2016) 766 and more detailed in the Infrastructure based communication profile, elaborated in TF3 of C-Roads, are very similar warnings and dynamic traffic notifications for different transport environments, vehicle categories etc., which all share the same security requirements. Therefore the basic technical elements needed for guaranteeing secure communications in a C-ITS network will be independent from the single application or message format transmitted between the stations involved.

To ensure EU-wide interoperability of C-ITS services it is widely accepted that C-ITS in Europe is working within one trust model, and this trust model is based on a PKI-Infrastructure comprising all C-ITS stations, vehicle based ones and road infrastructure based ones within the same CP. This CP describes the details of the security provisions from the single C-ITS station operator with the complete link of the chain of trust via the EA – Enrolment Authority, AA –Authorisation Authority and sub-CA´s to the central EU elements, CPOC – C-ITS Point of Contact and TLM-Trust List Manager as well as a European Root CA.

In the CP, also the process and communication steps between these entities are defined for the connection to other basic elements of the PKI infrastructure. These special provisions have to be taken into account by the single organisation participating to the PKI system. In order to ensure the same level of security as applied within the PKI structure, also the communication links with external entities need to be properly defined, e.g. when transmitting authorisation tickets or enrolment certificates to a single C-ITS station.

The functional security requirements are defined for the whole group of “Day One C-ITS Services “ as one common group with the following details:

a. Authorization level (including the verification of the validity of certificates, verification of revocation status of the certificate, verification of trust chain as a whole): The verification of the validity of a certificate is performed by using the message signature and the public key contained in a certificate. The respective CA, which issued the certificate and its key pair, is also included, so that the corresponding CA can also be validated. Following this socalled chain of trust up to the issuing Root CA and checking the currently valid ECTL", the trustworthiness of received messages can be checked.

The verification of the trust chain as a whole works according to the principle that all elements in the trust chain need to be covered by a trust relation and the overall chain is only as trustful as the "weakest link" in this chain. This means that a consistently high level of trust needs to be applied to all elements involved in the trust chain. This is defined in the CP, including processes for all elements involved.

b. Data retention (affecting privacy and data protection regulation): Data retention should be performed in accordance with the guidance provided in the SP (see below). Data retention periods might also be subject to local legislation (according to GDPR Art.5), and inconsistencies and repercussions should be investigated.
   - For communications from road side units and infrastructure ITS stations, data privacy is not considered a major issue since the requirements have already been defined in the SP. The applied general concept in the SP for all these Infrastructure based C-ITS stations is that personally identifiable information (e.g. certificates and identifiers that are attached to C-ITS messages) should not be retained for more than a maximum of 5 minutes in order to achieve widest data anonymity.
   - This concept implies that only anonymized data and/or average values will be used, e.g. for traffic management purposes. This may have consequences for the output of road side related traffic monitoring e.g. for vehicle speed calculations in traffic flow models, or for vehicle trajectories at intersections.
   - Additionally, road operator's and road authority's vehicles might be subject to specific regulation, particularly regarding the supervision of workers and the right to privacy of the people using these vehicles containing C-ITS stations.
   - The most critical factor is the vehicle ITS-S and the risk of being tracked as a user. This aspect is out of scope for C-Roads TF1

c. Data privacy: Data privacy is provide through the structure of the PKI as defined in the CP. Organisational separation of roles is a general design principle of the European Trust Model. The,roles of EA and AA are completely separate, with separation of processes relating to long term keys (for signing certificate requests) and the short term keys (used for authentication of the single messages). Additionally the short term certificates, used for the signature of the message, are regularly changed in the C-ITS station during operations and repetition of the use of the same certificate is restricted. This is to reduce the possibility to track or follow a specific user over an extended period of time. The CP defines the maximum number of certificates that may be active at one time as 100 certificates for a validity period of 1 week.

d. Permissions: The permission levels and attributes for different kinds of vehicles (private, public e.g. police, or service vehicles) are currently not widely implemented, but at least the right of CAs to issue certain SSP (Service Specific Permissions) within the certificates should be addressed in the piloting phase of C-Roads. The detailed SSP specifications can be found in the Annexes.

e. Common central elements of the European Trust Model: Central entities like TLM and CPOC need to come to common specifications within C-Roads. Some of the related definitions (e.g. ECTL format) have just recently been completed in the update of standard TS 102 941, version 1.2.1 in May 2018. Preparations for first implementations are currently in progress and expected to be available soon. In order to make first steps for implementations for the piloting phase possible, these central elements will be set up according to the decisions taken by all C-Roads members together with the European Commission.

f. Revocation: Revocation of single C-ITS stations is not foreseen in the current CP. Instead a "revocation by expiry" is specified, which means that short term certificates for communication have a rather short validity time, e.g. one week, and after that defined period they are not trusted anymore. In this mechanism it is important to limit the maximum preloading time to a reasonable time span. Preloading defines how long in advance short term certificates, which are valid for a specified period and are intended for later use, can be loaded onto the vehicle. A too long preloading period, e.g. of several years, would pose a risk to the C-ITS trust system, since these certificates cannot be individually revoked later on.

Revocation of CA's is foreseen. This requires a reliable, frequent distribution of the ECTL to all system operators using online access where appropriate. If a single CA from one operator is revoked, e.g. in case of a severe security breach, all certificates of the respective CA are revoked at the same time because they are not trusted members of the C-ITS network any more.

2.2 Compliance assessment for security

This subsection deals with security requirements on C-ITS system level as defined by the common European policy documents, focusing mainly on ITS stations operated in the name of road authorities. There are similar requirements for all other ITS stations, which are not explicitly addressed in this report.

There is currently no common protection profile for road side stations defined in C-Roads.

According to the security requirements from the European CP and SP, Common Criteria (ISO 15408) and the international SOG-IS agreement provides a part of the security framework to be used for the assessment/certification of C-ITS stations. Self-assessments of operators of C-ITS stations are acceptable only during the initial setup phase.

This point of view is shared and takes into account the existing provisions in terms of security of the road operators and public authorities responsible for large IT and sensor networks and their regular and reliable operation. For the fully operational phase beyond 2020, one necessary step will be to define a common protection profile for roadside C-ITS stations and perform a certification scheme according to an agreed Common Criteria catalogue. The discussion of this process has only recently been kicked off in TF1.

Full detailed definition of the certification scheme and auditing requirements foreseen in the CP and SP is needed. This will be required for the operational phase of C-ITS at large scale.

2.3 Agreed security elements

For the piloting phase of C-Roads, with limited numbers of C-ITS stations deployed on public roads, the following elements are agreed between the C-Roads members in order to harmonize the first elements put into operation on public roads:

- ECTL format and the use of this ECTL in C-Roads pilots using the specifications provided by the new version 1.2.1 of ETSI TS 102 941 released in May 2018.
- agreement on a provisional CTL/CRL format and the use of this provisional CTL/CRL format in pilots which have not yet updated from TS 103 097 v1.2.1 and TS 102 941 v1.1.1,see also Annex A and [1].
- an interoperable C-ITS station implementation including the security layer in the basic ETSI standards, including the secure key storage, for details please see the full list of standards.
- a common TLM with responsibilities and tasks defined for the piloting phase of C-Roads and the future extension to full operational capability, preferably operated by the EC asap.

2.4 Security provisions of C-Roads pilots

The following subsections/tables provide an overview for the provision of central elements in the C-ITS piloting phase in different C-Roads member states for the setup/piloting phase of C-Roads (until 2020), and for a fully operational phase of C-ITS in Europe (beyond 2020).In order to take full advantage of the piloting phase for the later operations many C-Roads members have planned to take their decisions regarding the operational phase in 2019/2020.

2.4.1 Pilot Phase (until 2020)

The security activities of the C-Roads pilots and their contributions to the Pilot phase of C-ITS.

C-Roads Member State	TLM	CPOC	RootCA	EA	AA	ITS station types	Included in C-Roads Pilot	Pilot Operation ongoing?
Austria	No	No	Contract	Contract	Contract	R-ITS-S	Yes/contractor	Yes
Belgium (Flanders and Wallonia)	No	No	TBD	TBD	TBD	C-ITS-S	Yes (see below)	By Q4/2018 - Q1/2019
Czech Republic	No	No	National	National	National	All	Yes	Yes, operated by O2
Denmark	No	No	TBD	TBD	TBD	C-ITS-S	NordicWay2	Starting Q2/2019
Finland	No	No	TBD	TBD	TBD	C-ITS-S	NordicWay2	Starting Q2/2019
France	Yes, PMA at national level	Yes, on national level	National	National	National	ALL	Yes	Yes
Germany	No	No	National	National	National	R-ITS-S	Yes	Yes
Hungary								TBD
Italy	No	No	Contract	Contract	Contract	R-ITS-S	Yes	TBD
Netherlands	No	No	National CA Provider	RWS / RDW-V-ITS	RWS / RDW-V-ITS	R-ITS-S	Yes	TBD

Co-financed by the European Union
Connecting Europe Facility

C-Roads Member State	TLM	CPOC	RootCA	EA	AA	ITS station types	Included in C-Roads Pilot	Pilot Operation ongoing?
Norway	No	No	TBD	TBD	TBD	C-ITS-S	NordicWay2	Starting Q2/2019
Portugal	No	No	National	National	National	All	Yes	TBD
Slovenia								TBD
Spain	No	No	National	National	National	All	yes	TBC
Sweden	No	No	TBD	TBD	TBD	C-ITS-S	NordicWay2	Starting Q2/2019
UK								TBD
EC DG JRC	Q1/2019 TBC	Q1/2019 TBC	2019 TBC	2019 / 2020	2019 / 2020	All	Yes	by 2018 or 2019

For this table of the security provisions the C-ITS stations are divided into Roadside ITS Stations – R-ITS-S and Vehicle ITS-Stations – V-ITS-S, and Central ITS Stations – C-ITS-S. In some C-Roads pilots the security preparations are executed for all C-ITS Stations.

A conclusion of this overview table for the piloting phase of C-Roads is that the provisional central elements are needed for the interoperability of the security solution provided. An interim solution will be made available from the EC by Q1/2019 (Tbconf.). This may comprise the TLM and a simple web site to provide the ECTL. Piloting and setup of this function needs to coordinated with the C-Roads Member States. The detailed setup conditions and the partners who can/will use these elements in the piloting phase of C-ITS need to be agreed between the parties involved. At the same time all pilots need to make sure that they are future proof for, or prepare a migration path to, the future common solution which will be provided by the future EU wide network layouts of C-ITS.

Co-financed by the European Union
Connecting Europe Facility

2.4.2 Operational Phase (beyond 2020)

The initial setup described in section 2.4.1 will have to migrate to the targeted European Trust Model in the future. Therefore the table will look different for the operational phase of the European C-ITS system, once the central European entities, e.g. Trust List Manager, CPOC, European RootCA and sub-CAs, are fully operational and available to all stakeholders, which will be the case from 2020 on.

C-Roads Member State	TLM	CPOC	RootCA	EA	AA	ITS station types	Pilot elements	operational
Austria	EU	EU	Contract	Contract	Contract	ALL	SSP´s	Open, decision by 2019
Belgium (Flanders and Wallonia)	EU	EU	tdb	tdb	Tdb	Tdbef.		TBD
Czech Republic	EU	EU						TBD
Denmark	EU	EU	TBD	TBD	TBD	TBD		TBD
Finland	EU	EU	TBD	TBD	TBD	TBD		TBD
France	EU	EU	National	National	National	ALL		TBD
Germany	EU	EU	National	National	National	R-ITS-S		TBD
Hungary	EU	EU						TBD
Italy	EU	EU	Contract	Contract	Contract	ALL		TBD
Netherlands	EU	EU						TBD
Norway	EU	EU	TBD	TBD	TBD	TBD		TBD
Portugal	EU	EU	TBD	TBD	TBD	TBD	TBD	TBD
Slovenia	EU	EU						TBD

Co-financed by the European Union
Connecting Europe Facility

C-Roads Member State	TLM	CPOC	RootCA	EA	AA	ITS station types	Pilot elements	operational
Spain	EU	EU	National	National	National	All		TBD
Sweden	EU	EU	TBD	TBD	TBD	TBD		TBD
UK	EU	EU						TBD
EC DG JRC	EU	EU	EU	EU	EU	All	TBD	2020 TBC

For this table of the security provisions the C-ITS stations are divided into Roadside ITS Stations – R-ITS-S and Vehicle ITS-Stations – V-ITS-S, and Central ITS Stations – C-ITS-S. In some C-Roads pilots the security preparations are executed for all C-ITS Stations.

Pilot elements in the table above are intended to be included in the C-ITS piloting phase in C-Roads in order to be discussed afterwards, based on the pilot results, when these elements can be introduced. E.g. SSP´s for public service vehicles

A conclusion of the overview table for the operational phase is that currently Germany and France have planned to setup Root CA , EA, and AA at national level and these are defined to be responsible for R-ITS-S in Germany and for all ITS-S in France. Most of the other C.Roads members still need to decide how to proceed after the piloting phase. It can be concluded that currently all members support the foreseen EU central elements. In addition to public authorithies setting up CA's it is probable that also vehicle manufacturers may do so and form part of the secure and trusted C-ITS network in Europe. The time frame for setting up all the necessary elements for operating this future trusted network is from 2020 onwards. The technical aspects are only one part to be solved. The governance elements, which are defined in the following chapter of the report, also need to be elaborated and agreed during the piloting phase of C-ITS.

The explanation of the single elements in the table above will be added in more details; currently the situation is as follows:

1. Austria: Motorway Operator ASFINAG has decided in the cooperative corridor project to use the central elements of the PKI system from the German partners and have contracted the provision of the security certificates for the road side ITS Stations involved directly from project partners. These partners have also taken over the role of the EA and AA for the duration of the corridor project and for the testing and validation sessions involved. For the later operational phase of C-ITS introduction on Austrian motorways this position needs to be evaluated once again and therefore the position for the operational C-ITS roll-out is currently open, the decision will be taken in till 2019.
2. Belgium/Flanders: The questions around the PKI are under investigation and need to be agreed. Details about Setup Phase:

   The Belgium Flanders Pilot currently being built for C-Roads is using cellular communication to personal devices. The cloud Central-ITS-Station will be in the EU Trust domain, the personal devices may be outside the EU Trust domain. The PKI specifications for the cellular implementation still are to be decided in TF4. In the scope of the pilot for InterCor a combination of ITS-G5 and cellular is being deployed in Belgium Flanders, with operations from Q3-Q4 2018 until Aug 2019. For ITS-G5, the communication is using the Intercor PKI specifications for R-ITS-S and V-ITS-S (outside EU Trust domain, since the previous versions of the relevant security standards are still in use). PKI specifications for cellular are also still under investigation within Intercor.
3. Czech Republic: For the piloting phase of C-Roads the PKI elements have been contracted from a telecom provider for all types of C-ITS stations, the decision for the future operational phase still has to be taken.
4. Denmark: The NordicWay2 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trst domain. The details of the security are to be discussed in collaboration with TF4. For the operational stage, the decision will depend on the national policy covering future deployments.
5. Finland: The NordicWay2 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trst domain. The details of the security are to be discussed in collaboration with TF4. For the operational stage, the decision will depend on the national policy covering future deployments.
6. France: Has decided to setup also central elements of the PKI infrastructure, like the CPOC because they were necessary to support the piloting phase of the SCOOP@F project and the mobile and fixed C-ITS stations. For the national pilot also the data privacy authority was formally involved and agreed to the proposed end user involvement and data procedures. For the C-ITS deployment phase no final decision in relation to Central PKI elements has been taken yet, so the information provided in the table above should be seen as preliminary.
7. Germany: A pilot version of the required PKI has been set up as part of the German C-ITS Corridor activities. The German PKI provides Root CA as well as EA and AA. Serving as a basis for tests of first C-ITS implementations and the required trust relations, the PKI is fully operational and already used by different stakeholders. The policy of this PKI has been created in close collaboration with the German Federal Office for Information Security (BSI), and it can also be updated, e.g. switching to certificate and protocol formats/versions, in order to be in line with common C-Roads specifications. In a later stage, where fully operational entities are also provided on a European level, the system will have to be adopted in terms of

protocols used for requesting certificates, and the format of the ECTL agreed with the implementers of the central elements.

8. Hungary: No decision taken yet.
9. Italy: No decision taken yet.
10. Netherlands : Rijkswaterstaat will start piloting with certificates according to the EU CP for InterCor and the cooperative corridor in 2018. Initially the certificates will be provided by the national CA provider. No decision has been made yet for C-ITS deployment.
11. Norway: The NordicWay2 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trst domain. The details of the security are to be discussed in collaboration with TF4. For the operational stage, the decision will depend on the national policy covering future deployments.
12. Portugal: For the piloting phase, CTAG will setup national authorities (Root CA, EAs and AAs) for the Portuguese pilot sites. A decision regarding the operational phase is not taken yet.
13. Slovenia: No decision taken yet.
14. Spain: For the piloting phase, CTAG will setup all authorities (Root CA, EAs and AAs) for the Spanish pilot sites. It is planned to keep this configuration also for the operational phase, but final decision is bind to the piloting phase results.
15. Sweden: The NordicWay2 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trst domain. The details of the security are to be discussed in collaboration with TF4. For the operational stage, the decision will depend on the national policy covering future deployments.
16. United Kingdom is not yet in a position to complete this until the A2M2 design has been approved. This will be the first deployment of a C-ROADS pilot and UK will take a decision on the C-ITS security implementation for the piloting in Q2/2018. The UK have yet to make a decision on the structure for the operational phase.

C-Roads partners who did not provide detailed feedback still have to make the decision how to proceed with the necessary security elements for C-ITS introduction. Most of them will use the experiences and lessons learned during the piloting phase in 2018/2019 and then decide for the next steps, especially for the R-ITS-S and the central elements of the PKI.

2.5 Certificate Policy and proposals for piloting

The EU Security Policy version 1.0 for C-ITS has been published and the Certificate Policy has been released as version 1.1. These documents define several aspects, also for the piloting phase, e.g. the concrete number of concurrently valid certificates, their validity duration, and the exchange mechanism for them.

However, as stated previously, there will still be elements that need to be further defined for the piloting stage for example the following elements need to be taken into account:

- The exact data format of the (E)CTL, which will be used for the operation of the C-Roads pilots. The ECTL format is specified in ETSI TS 102 941 v1.2.1, which requires the use of certificates according to ETSI 103 097 v1.3.1. For certificates according to ETSI TS 103 097 v1.2.1, there is no standardised CTL format available. Therefore close collaboration with EC is required in order to allow for a smooth introduction and transition, especially in case of potential (decentralised) preliminary solutions that had already been set up wihin C-Roads projects and that need to the migrate to the use of central trust entities (TLM/CPOC).

- As an interim solution, proposals for the ECTL can be considered within TF1 and may be officially approved by the C-Roads SCOM. This path is suggested as the certificate policy authority foreseen in the CP has not yet been established in time for the start of the piloting phase.
- As piloting progresses, further elements of the security policy may also need to be defined ahead of the formation of the EU C-ITS governance structure. It is proposed that a similar approach is adopted for these. Where technical elements are implemented in the piloting phase it is further proposed that there should be a feedback mechanism for technical validation.

There will be other elements like these, where a provisional definition of policy elements is needed in C-Roads in order to start the piloting and demonstration phase with security mechanisms in place.

These elements will need to be set up and established for the operational phase of C-ITS fully in line with the EU Security policy document, and the time frame of the C-ITS piloting should also be used to define and agree on these entities.

3 Governance structure for security

The document Security Policy & Governance Framework for Deployment and Operation of C-ITS (Release 1. Dec. 2017) (hereafter SP) defines the Governance Framework and roles in its section A, and the Security Policy in section B. The aim of this chapter 3 of this document is to highlight the points that require clarification for the implementation of the C-ITS pilots in C-Roads project.

In section 3.1 a brief description of the required entities is given, followed by separate sections describing the interactions between those entities in a stepwise aproach.

The aim of those latter sections is to summarise the main governing functions and responsibilities associated to those interactions, providing a basis for the definition of the communication processes that need to be defined as part of the sub-roles activity. SP describes those activities, but in many cases, it is centered in the governing body, mentioning only one of the sides of the communication, and making difficult to understand the shared responsibilities associated to the interaction between the counterparts. This could make difficult to understand what is needed to make the exchange of information. For this reason, the following sections complement the descriptions made in SP and aim at summarising the descriptions given there from a communications interface perspective.

3.1 Governance Framework requirements

Based on SP, the bodies acting as stakeholders in the governance of the C-ITS framework are:

1. European Commission (EC)
2. Member States
3. Vehicle Manufacturers
4. Road Infrastructure Managers / Operators
5. Users and Transport Associations
6. Equipment Suppliers: Manufacturers / Operators
7. Accredited security auditors
8. Article 29 GDPR / Data Protection Authorities

For most of the governing bodies, as indicated in Table 2, the SP foreses a public private partnership (PPP) as the type of legal entity, but this is not applicable for all roles.

Roles	Sub-Roles	Legal Entity	Coordinating Stakeholders	Participating Stakeholders
Policy Framework	C-ITS Governing body	C-ITS PPP #1	SE 1 or 2	1,2,3,4,5,6
	C-ITS Supervision Body	C-ITS PPP #2	SE 1 and/or 2	1,2,3,4,5,6,
	C-ITS Certificate Policy Authority	C-ITS PPP #3	SE composed by 2	1,2,3,4,5,6
	Privacy Policy Authority	C-ITS PPP #3	SE 2	1, 2, 3, 4, 5, 6, 8
	Security Policy Authority	C-ITS PPP #3	SE composed by 2	1,2,3,4,5,6
	Compliance Assessment Body	C-ITS PPP #4	SE 2 and/or 3 and/or 4	1,2,3,4,5,6,7,
C-ITS System Management	Operations Governing Body	C-ITS PPP #5	SE 2 and/or 3 and/or 4	1,2,3,4,5,6,

Roles	Sub-Roles	Legal Entity	Coordinating Stakeholders	Participating Stakeholders
C-ITS System operation	Operations Manager	-	MI	2,3,4
	Trust List Manager	EC	1	
	C-ITS Point of Contact (CPOC)	EC	1	
	Accredited PKI Auditor	See existing List of Member States	2	7

Table 2: Stakeholder categories involved in governing bodies (SE=Single Entity on EU level, MI=Multiple Instances on EU level)

The detailed structure of the C-ITS PPP legal entities is still to be defined in the SP. This section considers requirements for the governing boards that are needed for the piloting phase of the C-Roads project. For this state the key entities needed are the Certificate Policy Authority, the Trust List Manager and C-ITS Point of Contact:.

- For the C-ITS Certificate Policy Authority (CPA) during the pilot phase, Member States representatives in C-Roads, SCOM and EC could provisionally lead such a PPP for C-ITS. OEMs representative organisations like C2C-CC and ACEA could also participate. This interim CPA would only be expected to perform tasks needed for the pilot phase. The main task would the approval process for Certificate Authorities to be listed in the provisional ECTL.
- Trust List Manager and C-ITS Point of Contact (CPOC) are assigned and assumed directly by the EC, even in the early stages of C-Roads pilots, so no interim approach definition is needed.

In later stages of the project, if resources are available, other interim entities required for the correct functioning of the C-ITS could be considered, including:

- Privacy Policy Authority: Its role could be observation of Data Privacy regulations in the Member States, and liaising with the Art 29 Committee, and the Member States Data Protection Authorities. Its main responsibility would be advising Compliance, Operations and CP bodies about relevant legislative changes that could require updates in the C-ITS units and interactions.
- C-ITS Governing Body and C-ITS Supervision Body: EC may lead this PPP in the future, in the short term C-Roads steering committee could be asked to assume this role, if it is agreed that this is required for the piloting phase.
- Compliance Assessment Body:An interim body could be established to coordinate compliance activities in the piloting phase (in relation to interoperatibility and liaise with standardisation bodies, such as ETSI and CEN/CENELEC. If resources permit , WG2 or its TF1 could assume this role. The desired outcome would be identification of standards and profiles that are needed to guarantee the desired interoperability.
- Operations Manager and Accredited PKI Auditor roles will be played by individual organisations actors under the supervision of Member States, e.g. operator of the infrastructure of every pilot, or PKI Auditor appointed by the PKI of one Member State or Manufacturer.

In the mid-term, it could be interesting to start creating the referenced PPP's as ad-hoc groups within C-Roads, composed by the members of the consortium in the different member states, that belong to the categories of stakeholders that should participate in every C-ITS PPP, as defined in the SP. This would allow testing the interactions between the governing bodies of the framework and clarifying their responsibilities and functions associated to every sub-role.

The following sections describe the interactions between the governing bodies in three steps, starting with the interactions between the certificates management governing entities (C-ITS Certificate Policy Authority, CPOC and TLM), adding interactions of these with other entities in a second step, and ending with the final operational scenario defined in SP.

3.2 Interactions between certificate management governing entities

Figure 2 shows the overall C-ITS governance structure as outlined in the SP, including the interactions between the governing bodies. As defined in the governance framework, this includes the roles that are involved in the management of the PKI, which are most relevant for TF1.

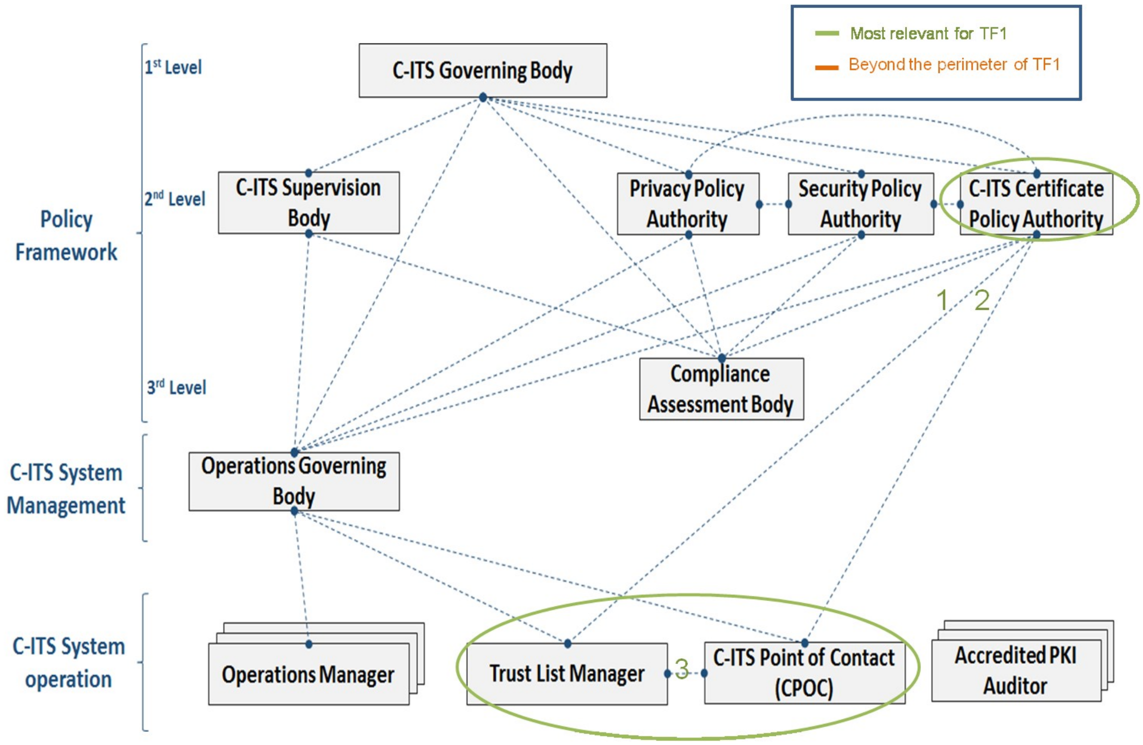


Figure 2: Governance structure including security aspects, e.g. PKI and certificate management entities

The main focus of the interactions in this section are those required in the early pilot implementations, between the three bodies managing the PKI certificates required by the pilots to guarantee integrity and authenticity of the exchanged messages (The complete description of the roles of the C-ITS Certificate Policy Authority, TLM and CPOC can be found in the CP and fully apply to all C-Roads pilot deployments):

1. Certificate Policy Authority (CPA) vs Trust List Manager (TLM) interactions:
    - CPA is responsible of authorising the TLM to operate and report regularly,
    - CPA should inform the Trust List Manager about updates in the CP and PKI authorisation management.
    - TLM reports to the policy authority for the overall secure operation of C-ITS trust model, including generation and update of the ECTL and compliance with valid CP.
    - CPA is responsible of notifying the TLM about trustable/non-trustable root CAs and their certificates on the basis of the received approval reports of the root CAs and the regular operations reports

- TLM is responsible of inclusion/exclusion of root CA certificates in ECTL upon notification by the Policy Authority,
- TLM is responsible of operation of the ECTL according to the common valid CP and regular activity reporting to the CPA for the overall secure operation of C-ITS trust model,

2. CPA vs C-ITS Point of Contact (CPOC) interactions:
   - CPA is responsible of authorising the CPOC to operate and report regularly,
   - CPA should inform the CPOC about updates in the CP and PKI authorisation management.
   - CPA is responsible of the approval of the root CA's CPS if in line with the common and valid CP,
   - CPA is responsible of decision if root CAs are trustable,
3. CPOC vs TLM interactions:
   - CPOC reports individual root CA updates to TLM for publication and update of the ECTL,
   - TLM is responsible of reception of root CA certificates from the CPOC,
   - TLM is responsible of regular and requested transmission of ECTL to the CPOC.

In general, all exchange requirements with CPOC have to be established bearing in mind that it is a unique entity, appointed by the CPA. The CPOC is responsible for:

- Establishing and contributing to secure communication exchange between all entities of the C-ITS trust model in an efficient and fast way, (internal exchange)
- Reviewing of procedural change requests and recommendations submitted by other trust model participants (i.e., root CAs), (internal exchange)

SP annex A.3 sections A.3.1 and A.3.3 contains descriptions of their detailed roles. Figure 3 shows the trust model from a different perspective and in more detail, indicating the required interoperability requirements between different kinds of CA, CPOC and TLM.

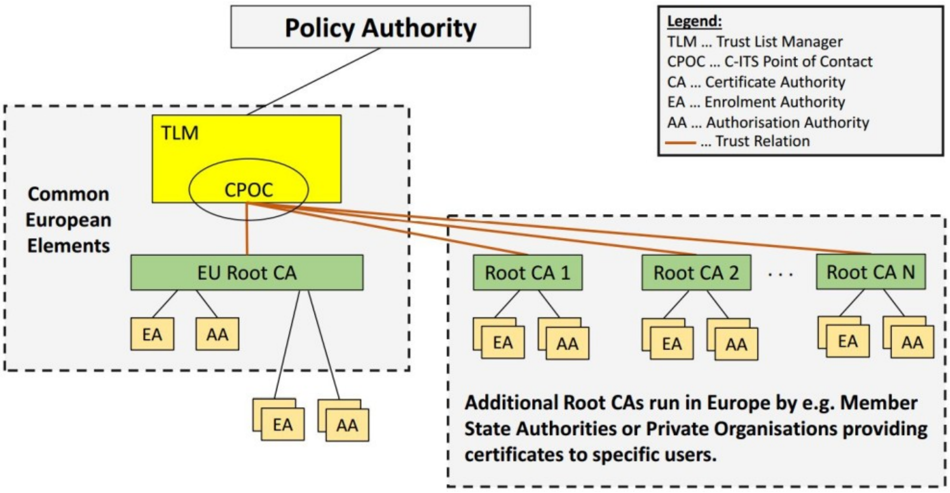

Policy Authority
Legend:
TLM ... Trust List Manager
CPOC ... C-ITS Point of Contact
CA ... Certificate Authority
EA ... Enrolment Authority
AA ... Authorisation Authority
... Trust Relation
TLM
CPOC
Common European Elements
EU Root CA
EA
AA
EA
AA
Root CA 1
Root CA 2
Root CA N
EA
AA
EA
AA
EA
AA
Additional Root CAs run in Europe by e.g. Member State Authorities or Private Organisations providing certificates to specific users.

Figure 3: Interoperability Requirements: European Trust Model

Moreover Figure 3 is showing that CPOC is acting as coordination point between individual root CAs, these exchanges are not visible as CPOC responsibilities in the general C-ITS Governance Framework as depicted in Figure 2.

3.3 Interactions between certificate management entities and other governing entities

This section describes the interactions between the three most important bodies and the other bodies of the Governance Framework. In the first stages of the project pilots these will be considered interactions with the “external world”, since the other bodies will not have been implemented yet.

This section describes potential interim solutions for the functioning of the governance structure of the PKI foreseen in the CP/SP during the piloting phase, until those entities are established. Figure 4 provides an overview of the interactions of the various entities and those entities that are potentially needed for the piloting phase.

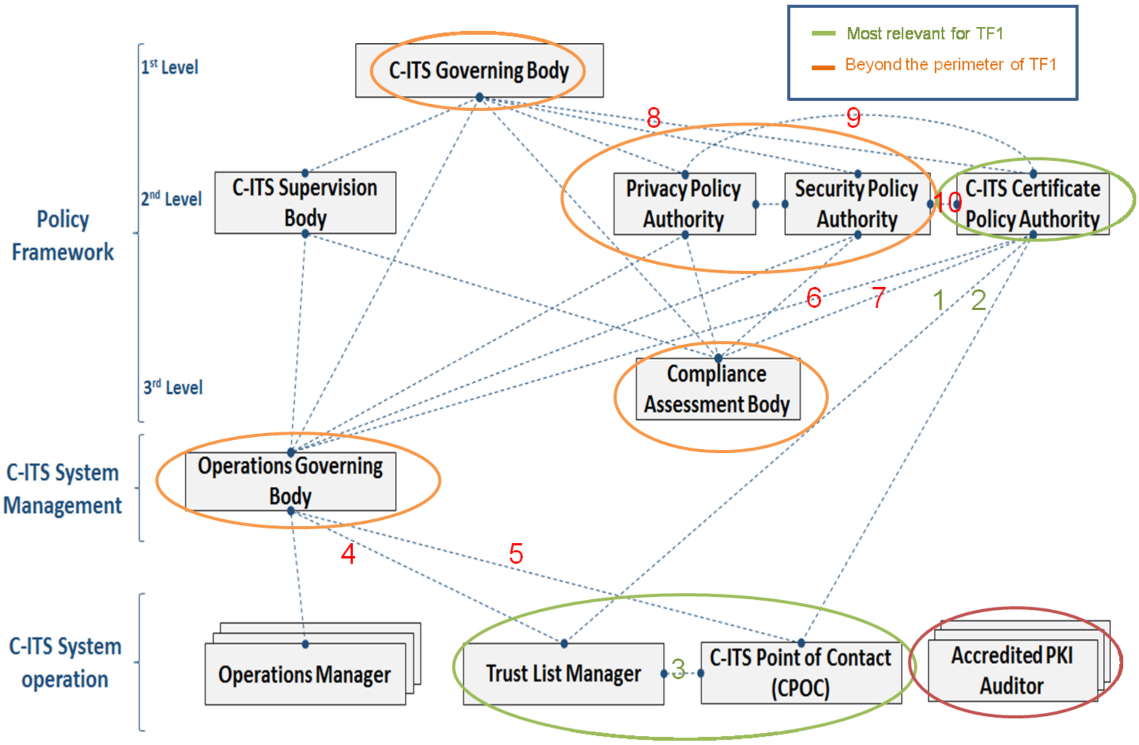


Figure 4: Interactions between PKI certificate management entities and other governing bodies (red numbers)

Those interactions are shown in Figure 4 and are listed below:

4. TLM vs Operations Governing Body interactions:
   - TLM is responsible of reporting Operations Governing Body about any updates in the ECTL and root CA. Whilst the Operations Governing body will not be implemented, those notifications should be made directly to Pilot Operators
   - TLM is responsible of Signing of the ECTL,
5. CPOC vs Operations Governing Body interactions:
   - CPOC is responsible of reporting Operations Governing body about any updates in the public key of the tlm and individual root CA managers. Whilst the Operations Governing body will not be implemented, those notifications should be made directly to Pilot Operators.

- CPOC is responsible of publication of the common trust anchor (public key certificate of the TLM),
- CPOC is responsible of publication of the ECTL.

6. CPA vs Operations Governing body interactions:
    - CPA should inform the Operations Governing body about updates in the CP (incl. PKI authorisation management). Whilst this body will not be implemented, those notifications should be made directly to Pilot Operators.
    - CPA will receive and take decision on the change requests and recommendations to review of CP, submitted by other PKI participants or entities, through the Operations Governing body.
    - CPA is responsible of the approval of the root CA’s Certificate Practice Statement (CPS) of the operational entities, if in line with the common and valid CP.
7. CPA vs compliance assessment body interactions:
    - CPA should agree with the Compliance Assessment body about CP compliance assessment criteria, and inform C-Roads partners responsible of the implementation of PKI agents and other software components aimed to interact with them, about those compliance assessment criteria. In the mid/long-term, the Compliance Assessment body will intermediate in those notifications.
    - CPA is responsible of the approval of the common CP, and the approval of future CP Change Requests, and notify them to Operations Governing and Compliance Assessment bodies.
    - Compliance Assessment body is responsible of defining, deciding and publishing the CPS approval and CA audit procedures (collectively referred to as CA approval procedures),
    - Compliance Assessment body is responsible of scrutiny of the audit reports for all root CAs by the Accredited Auditor.
    - CPA is responsible of decision if root CAs are trustable, based on Compliance Assessment audit reports.
8. The C-ITS CPA should be the body to gather and consolidate input from bodies that are responsible for the definition of security requirements in individual member states or private organisations. This interaction will be aimed at the definition of common baseline Certificate Practise Statements and PKI Trust List management. In the long term this will be in the responsibility of C-ITS Governing Body.
9. The data protection rules for C-ITS defined in the CP, drafted and maintained by the C-ITS CPA, have to be aligned with requirements from Data Protection Authorities. Currently the privacy requirements are well reflected, potentially receiving an update during the C-Roads project lifetime. In the mid/long term, this communication will be done in collaboration with Privacy Policy Authority (which is currently, as of June 2018, not yet established in accordance to SP definition).
10. CPA needs to monitor and contribute to the definition of new releases of the SP, in order to guarantee that CP and PKI authorisation management can adequately address the SP requirements (and vice versa). Short-term solution will require that C-Roads actively supports this interaction by providing feedback from the initial operating phase. In the mid/long-term, this coordination will be established with the Security Policy Authority (which is currently, as of June 2018, not yet established in accordance to SP definition).

3.4 Additional interactions in the final governance operational scenario

Additionally there are recommendations made for the remaining interactions between the governing bodies not considered a priority in the pilots, which are shown in Figure 5

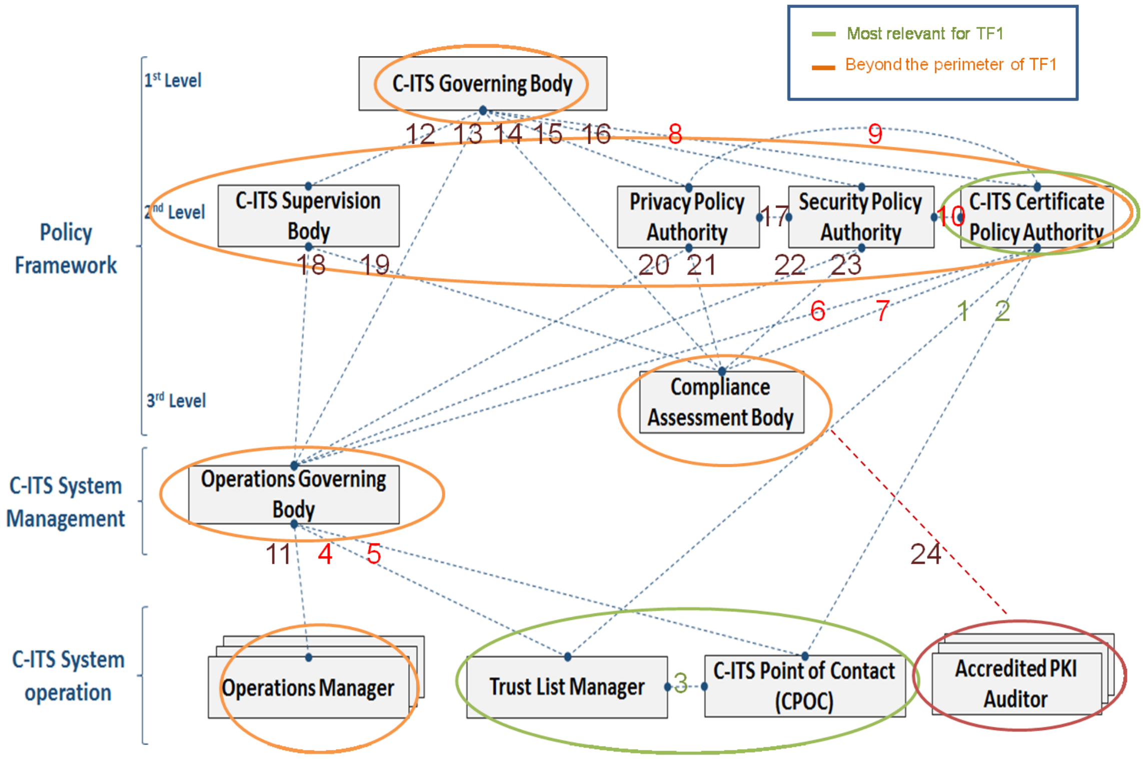


Figure 5: Interoperability Requirements: Final operational Governance interactions (purple numbers)

They are provided here just for completeness, but those interactions will only be applied in case of availability of resources to implement all the governing bodies as described in the SP for the complete framework:

11. Operations Governing Body issues to Operations Managers, operational requirements derived from the high-level requirements, coordinates and manages incidents reported by them, and checks and ensures compliance of operation management requirements. Operations Governing Body acts as a central coordination point between Operation Managers, sharing operational relevant information between them, mainly those activities and issues, which go beyond the jurisdiction of a specific Operation Manager.
12. The C-ITS Governing Body will act as main contact point to the general European policy makers. Defines rules (including conflict resolution process) for the resolution of issues detected by the C-ITS Supervision body. It is the main contact to policy makers.
13. The C-ITS Governing Body will act as main contact to C-ITS Operators and manufacturers. Defines C-ITS strategy is the high-level plan to enable C-ITS services to be deployed and operated. On operational level other types of strategy may exists such as a short or mid-term strategy to improve or change the service due to changes in requirements. Operations Governing body will receive instructions from Governing body about implementation strategy of the ITS-S operational requirements.

14. This interaction is aimed to reach agreement on the Definition of Compliance Assessment Reference Framework, including: Assessment criteria by testing laboratories, Reference Specifications and standards for assessment, system Profiles.
15. Definition of Data Privacy strategy and policy, including conflict resolution.
16. Defines the C-ITS strategy including the security strategy and derives rough guidelines from the strategy based on the input from the stakeholder groups.
17. Coordination between Privacy and Security Policy authorities, in order to guarantee that Security Policy statements address adequately the citizen‘s data privacy requirements, stated in the Privacy Policy.
18. Operations Governing Body should report to Supervision Body incidents of large scale and high severity, which affect the entire C-ITS trust system (e.g., disaster recovery situation where the cryptographic algorithm is compromised) and which cannot be resolved by the Operation manager and the Operations governing body. Supervision Body will supervise and manage those large-scale incidents through a dedicated CERT. This includes providing directives, guidelines and recommendations to the Operations Governing Body. Supervision Body will also issue directives, guidelines and recommendations, and update the requirements to Operations Governing body accordingly.
19. Compliance Assessment Body reports its activity to C-ITS supervision body, agreeing on the governing rules and procedures for the compliance assessment tests and procedures and compliance testing involving external existing compliance schemes.
20. Privacy Policy Authority should inform the Operations Governing body about updates of data protection rules for C-ITS Operations, including the ones defined in the CP.
21. Privacy Policy Authority should inform the Compliance Assessment body about Privacy Policy compliance assessment criteria.
22. Security Policy Authority should inform the Operations Governing body about updates of security policy strategy and regulations for C-ITS Operations.
23. Security Policy Authority should inform the Compliance Assessment body about Security Policy compliance assessment criteria.
24. Accredited PKI Auditors should report the Compliance Assessment Body about their activities and lists of accredited devices and PKI.

4 Recommendations for a C-Roads security mechanism for C-ITS

4.1 Proposal of an organisational structure for C-ITS security

For C-Roads the organisational structure is based on the setup described in chapter 0. Depending on the migration time from certificates based on ETSI TS 103 097 v1.2.1 to ETSI TS 103 097 v1.3.1 there might be an intermediate security solution required considering interoperability aspects.

4.2 Cooperation models for implementation

As indicated in section 3.1 several interoperability aspects have to be considered for C-Roads. In addition to fulfil these requirements the following aspects could be considered within C-Roads in order to cooperate with respect to security.

It seems reasonable and recommendable to define a common set of processes and forms to perform common steps in a harmonized way for the C-Roads pilot deployments. However, this might not be possible or efficient in all cases if components and processes have already been deployed by different C-Roads PKI operators in different ways – in that case the required harmonisation effort might outweigh the potential benefits. A list of the processes and specifications which should be considered for potential harmonisation contains the following aspects:

- Processes under control of the Root CA according to the CP [2].
    - EA and AA registration at the Root CA in order to request a Sub-CA certificate.
    - Termination and transfer of EA and AA certificate at a specific Root CA.
    - Revocation of EA or AA certificate at a specific Root CA.
    - Registration including authentication of end-entity subscriber organizations (manufacturer / operator) according to the CP [2] section 3.2.2.4.
        - Initial registration, re-keying and re-registration of ITS stations at the EA.
        - API specification to register a new ITS station at the EA.
        - API specification to update a registration with respect to change the permissions, the validity, and the region restriction.
        - API specification for temporary deactivation / revocation of a ITS station at the EA.
        - API specification to deregister a ITS station at the EA.

    NOTE: Since the registration process has already been deployed at different C-Roads PKI operators harmonization might create high effort and incompatibilities.
- Processes under control of the Policy Authority (PA) according to the CP [2].
    - Root CA registration at the PA in order to be accepted and trusted to be added to the ECTL by the TLM. Definition of a technical process to transfer the ECTL to the CPOC to make it available.
    - Termination of Root CA registration at the PA in order to let the existing RCA certificate expire without an update of the ECTL.
    - Revocation of Root CA certificate in order to update the ECTL by removing the affected RCA certificate as soon as possible and renew the ECTL at the CPOC.
    - Request for re-keying or key changeover of the Root CA certificate at the PA in order to update the ECTL by the TLM and renew the ECTL at the CPOC.

4.3 Recommendations for C-ITS start – up phase (until 2020)

In the setup phase of the various C-Roads pilots (2018-2019), some limitations and restricted requirements need to be considered, as described in the previous chapters. These are relevant for the governance level and (future) decisions, since they have impact on root CA operators and the involved stakeholders of the C-ITS network. Therefore the recommendations in this section are made with respect to how the pilots may be assessed against the SP and CP in the initial phase.

- A temporary PA, TLM and CPOC may be operated within C-Roads if no EU instance is available in the first time. This temporary C-Roads instance may also be used by selected external partners, e.g. C2C-CC or private station operators.

It is recommended that each Root CA operator should create a CPS for the RCA, EA and AA according to the CP. The Root CA operator should ensure correctness and completeness of the CPS and the compliance to it. This may be subject to internal or an external audit, even if it might not necessarily be verified by a accredited PKI auditor during the pilot phase, cf. section 3.3. A full audit is not recommended as, until all entities of the CP are in place, it will be impossible to comply with it.

It is recommended that Root CA operator should create a compliance audit report which notes all aspects where the Root CA and its EA/AA does and does not fulfil the requirements of the CP [2]. Ideally such a report contains an indication how the missing elements can be set up and put into operation for the fully operational phase from 2020 on.

Within such an approach the following limitations for the pilot phase are noted:

- Physical security controls and other mandatory requirements, e.g. compliance with ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27005, may not be certified in the pilot phase.
- Backup installations might not be fully available and automated for all PKI components in the pilot phase. Some components of the PKI might need manual recovery and manual switch from primary to backup installation.
- Full off-site back-ups of root CA components might not be realized in the pilot phase.
- Segregation of duties may not be enforced in the PKI operator companies in the pilot phase according to CP [2] section 5.2.4.
- Personnel controls according to CP [2] section 5.3 may not be implemented completely.
- Audit logging procedures according to CP [2] section 5.4 may not be implemented completely.
- Records archival according to CP [2] section 5.5 may not be implemented completely.
- EA / AA might operate without HSM in the pilot phase.
- The compliance audit and the creation of an audit report from an Accredited Auditor for the root CA is optional. The PKI operator might not be able to fulfil all requirements of section 1.7.5, section 4.1.2.1 and chapter 8 of the CP [2] in the pilot phase.
- The creation of a compliance assessment certificate regarding conformity of the EA/AA by a national body or a private entity is optional, cf. section 1.7.5 and 4.1.2.3 of the CP [2].
- Since no common protection profile for ITS stations is available for the pilot phase the operators can request a self-assessment of the ITS station manufacturer and the EA can request a self-assessment of the operator that registers the station.

In order to consider the possibly higher risk due to missing certification from an accredited auditor, the PA could request modified certificate validity times from the Root operator as listed in Table 3. If the Root CA, EA and AA are not certified, the root CA certificate might have a limited lifetime that does not exceed a validity of two years (1y private key usage). Accordingly, the related EA, AA and EC have a maximum validity of one year. This measure should ensure that a PA and TLM can accept a root CA in the pilot phase without fulfilling all requirements of the CP [2].

Entity	Max. Private Key Usage period	Maximum Validity time
Root-CA	1y	2y
EA	6m	1y
AA	6m	1y
EC	1y	1y
TLM	1y	2y

Table 3: Reduced validity periods of the certificates inside the C-ITS trust model

The necessary future evolution of the trust network, e.g. delisting of old/expired entities, registration of new members and new entities, will require processes also at policy level, which need to be brought to life. The temporary PA shall organize all necessary steps for their stakeholders to migrate to a fully operational C-ITS network including the necessary governance elements mentioned in [2] by 2021 latest.

4.4 Recommendations for the C-ITS operational phase (beyond 2020)

The operational phase is currently assumed to start 01.01.2021. This is right after the end of the C-Roads project. The following highlights what will be additionally required for the operational phase.

- The PA, TLM and CPOC shall be managed and operated by a single central European operator. These entities shall fulfil the CP [2] completely.
- There shall be at least one PKI that consists of RCA, EA and AA that is operated by a European operator. This PKI can be used by C-Roads members and other road operators in the operational phase. The PKI shall fulfil the CP [2] and security policy [3] completely and the root certificate of the PKI shall be listed on the ECTL.
- There might be several PKIs of different countries that consist of RCA, EA and AA. Each PKI shall fulfil the CP [2] and security policy [3] completely and the root certificate of the PKI shall be listed on the ECTL.
- Each ITS station (C-ITS-S, R-ITS-S and V-ITS-S, etc.) shall fulfil the CP [2] and security policy [3] completely.
- Each ITS station (C-ITS-S, R-ITS-S and V-ITS-S, etc.) shall be certified to ensure trust in the station (hardware and software). For the certification the requirements of the CP [2] and the protection profile shall fully apply.
- The operator of the ITS station shall assign the minimum set of permissions to the registered station and shall reduce the permissions as soon as they are not required anymore.
- Road operators shall monitor their ITS stations and shall deactivate broken, stolen or manipulated stations as soon as possible.
- The operator of ITS stations shall deregister all stations that reached their end of life.
- PKI operators shall ensure that secure software updates are possible for the central components like TLM and CPOC as well as for the PKI components like RCA, EA, and AA. PKI components with known vulnerabilities shall be fixed immediately or shall be revoked.
- Road operators and the ITS station supplier shall ensure that secure software updates are possible for the ITS stations. Stations with known vulnerabilities shall be fixed immediately or deactivated at the EA

Stakeholders of the PA shall setup a governace structure were all C-ITS station operators can participate in the strategic decisions to develop C-ITS security according to new risks and future options of development in policy, changing cooperation partners and upcoming technology developments.

References

[1]: C_Roads_WG2_TF1_Security_Gap_Analysis_v1.0_01042018

[2]: C-ITS Platform: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) v1.1 June 2018

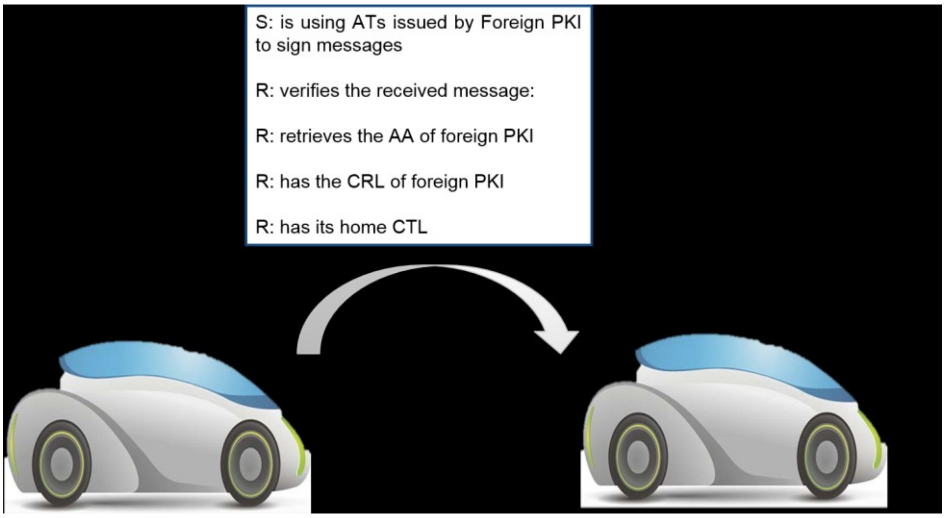
[3]: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1 (Release 1.1 currently under preparation, expected to be released in Q1/Q2 2018)

[4]: C_Roads_WG2_TForce1_Reference_Documentation_List_v1.0_01042018

[5]: European Commission, COM (2016) 766 "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", 30th of November 2016

[6]: The ITS-AID information is contained in ETSI TS 102 965 v.1.4.1 (November 2018) and could previously be found at the following URL https://standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers

ANNEX A – Cross-test requirements based on ETSI TS 103097 1.2.1 / TS 102 941 1.1.1



S: is using ATs issued by Foreign PKI to sign messages

R: verifies the received message:

R: retrieves the AA of foreign PKI

R: has the CRL of foreign PKI

R: has its home CTL

Figure 6: ETSI TS 103097 1.2.1 Security Cross-Tests process

In this section, we treat all security cross-test requirements. These specifications concern the interactions in different trust domains as given in Figure 6 They detail the secure exchange between ITSSs retrieving their ATs from different PKIs. The main objective of the tests is to verify messages authentication and validate the trust chain as illustrated in Figure 7.

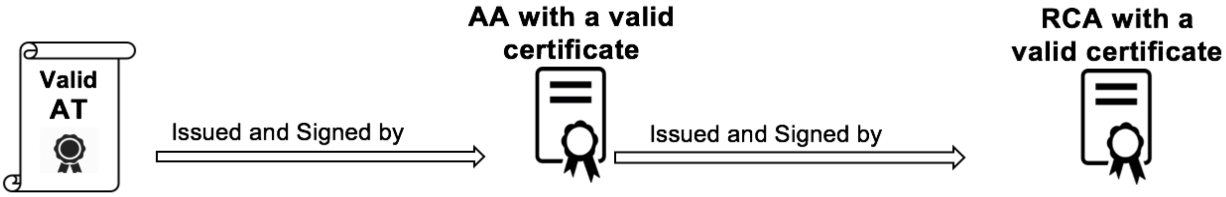


Figure 7: Trust chain validation

A1.1. Certificates formats

The certificates formats for CAs, ATs and ECs used for the C-Roads project are defined in ETSI TS 103 097 v1.2.1. Each ITS-S certificate is composed of several main fields: Version, Signer_Info, Subject_attributes, Validity_restrictions and Signature (64 bytes). The assurance level field shall contain the assurance level of the sender or certificate authority. A certificate shall contain an assurance level that is equal to or lower than the assurance level of the certificate referenced by the signer_info. If the assurance level is unknown for the certificate, then the default assurance level 0 shall be used. (cf 103 097 v1.2.1). In C-Roads Project, we set the values of both assurance level and confidence level in ITSS-certificates to 0.

A1.2. Certificate Validity

The CAs certificates duration is set to 5 years for the different EAs and the AAs and to 8 years for the RCA. The EC duration is set to 3 years for all partners.

A1.3. Cryptographic operations

There are different types of algorithms defined in ETSI Standard TS 103 097 v1.2.1, some used for signing, others for encryption.
Here are the algorithms defined:

- ECDSA_nistP256_with_SHA256
- ECIES_nistP256_with_AES128_CCM

A1.4. C-Roads ITS Application ID (ITS-AID)

The ITS-AID format used in C-Roads project is of type IntX (as described in ETSI TS 103 097 v1.2.1). Follwing [6], the ITS-AIDs chosen for the C-Roads project are listed in Table 4.

ITS-AID	Values
CAM	36
DENM	37
SPAT	137
MAP	138
IVI	139

Table 4: ITS-AID values based on ETSI/ISO

A1.5. Specific Service Permissions (SSPs)

The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. For example, there may be an SSP value associated with the ITS-AID 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.

SSPs for CAM message are defined using 3 bytes (as presented in ETSI EN 302 637-2 v1.3.2 section 6.2.2.2). SSPs for DENM message are defined using 4 bytes (as presented in ETSI EN 302 637-3 v1.2.2, section 6.2.2.2).

The SSP format used in C-Roads project is of type opaque (as described in ETSI TS 103 097 v1.2.1).

The following sections provide the SSPs adopted in C-Roads project (DENM, IVI, MAP, SPAT, CAM).

A1.5.1. DENM SSPs

ITS-AID value : 37 (ref. TS 102 965)

SSP (ref. ETSI EN 302 637-3)

Octet Position	Bit Position	CauseCodeType / Container	R-ITS-S (RSU)
1	0	trafficCondition(1)	1
1	1	accident(2)	1
1	2	roadworks(3)	1
1	3	adverseWeatherCondition-Adhesion(6)	1
1	4	hazardousLocation-SurfaceCondition(9)	1
1	5	hazardousLocation-ObstacleOnTheRoad(10)	1
1	6	hazardousLocation-AnimalOnTheRoad(11)	1
1	7	humanPresenceOnTheRoad(12)	1
2	0	wrongWayDriving(14)	1
2	1	rescueAndRecoveryWorkInProgress(15)	0
2	2	adverseWeatherCondition-ExtremeWeatherCondition(17)	1
2	3	adverseWeatherCondition-Visibility(18)	1
2	4	adverseWeatherCondition-Precipitation(19)	0
2	5	slowVehicle(26)	0
2	6	dangerousEndOfQueue(27)	1
2	7	vehicleBreakdown(91)	0
3	0	postCrash(92)	0
3	1	humanProblem(93)	0
3	2	stationaryVehicle(94)	1
3	3	emergencyVehicleApproaching(95)	0
3	4	hazardousLocation-DangerousCurve(96)	0
3	5	collisionRisk(97)	0
3	6	signalViolation(98)	0
3	7	dangerousSituation(99)	0

Table 5 : DENM SSPs.

A1.5.2. IVI SSPs

ITS-AID value : 139 (ref. TS 102 965)

SSP (ref. ETSI TS 103 301 V 1.2.1)

Octet Position	Bit Position	IVI data Item	R-ITS-S (RSU)
4	0	Vienna Convention Code for road sign	0
4	1	ISO/TS14823 traffic sign pictogram (danger warning)	1
4	2	ISO/TS14823 traffic sign pictogram (regulatory)	1
4	3	ISO/TS14823 traffic sign pictogram (informative)	1
4	4	ISO/TS14823 traffic sign pictogram (public facilities)	1
4	5	ISO/TS14823 traffic sign pictogram (ambient condition)	1
4	6	ISO/TS14823 traffic sign pictogram (road condition)	1
4	7	ITIS codes	0
5	0	Lane status	1
5	1	Road configuration container	1
5	2	Text container	1
5	3	Layout container	0
5	4	IVI status negation	0

Table 6: IVI SSPs.

A1.5.3. MAP (RLT) SSPs

ITS-AID value : 138 (ref. TS 102 965)

SSP (ref. ETSI TS 103 301 V 1.2.1*)

Octet Position	Bit Position	RLT service SSP data Item	R-ITS-S (RSU)
1	0	Intersection geometry list allowed to transmit	1
1	1	Road geometry list allowed to transmit	1

Table 7: MAP (RLT) SSPs.

** V 1.2.1 is preferred for SSP of RLT, because data item of V 1.1.1 seems inappropriate to specify properly the permissions in regard of the use cases.*

A1.5.4. SPAT (TLM) SSPs

ITS-AID value : 137 (ref. TS 102 965)

SSP (ref. ETSI TS 103 301 V 1.2.1*)

Octet Position	Bit Position	SPATEM data Item	R-ITS-S (RSU)
1	0	Signal Phase and Timing	1
1	1	Public transport prioritization status response	1
1	2	Maneuver assisting information	0

Table 8: SPAT (TLM) SSPs.

** V 1.2.1 is preferred for SSP of TLM, because data item of V 1.1.1 seems inappropriate to specify properly the permissions in regard of the use cases.*

A1.5.5. CAM SSPs

ITS-AID value : 36 (ref. TS 102 965)

SSP (ref. ETSI EN 302 637-2)

Octet Position	Bit Position	Permission Items	R-ITS-S (RSU)
1	0	CenDsrcTollingZone/ ProtectedCommunicationZonesRSU	1
1	1	publicTransport / publicTransportContainer	0
1	2	specialTransport / specialTransportContainer	0
1	3	dangerousGoods / dangerousGoodsContainer	0
1	4	roadwork / roadWorksContainerBasic	0
1	5	rescue / rescueContainer	0
1	6	emergency / emergencyContainer	0
1	7	safetyCar / safetyCarContainer	0
2	0	closedLanes /	0

		RoadworksContainerBasic	
2	1	requestForRightOfWay / EmergencyContainer: EmergencyPriority	0
2	2	requestForFreeCrossingAtATrafficLight / EmergencyContainer: EmergencyPriority	0
2	3	noPassing / SafetyCarContainer: TrafficRule	0
2	4	noPassingForTrucks / SafetyCarContainer: TrafficRule	0
2	5	speedLimit / SafetyCarContainer	0
2	6	reserved for future usage	0
2	7	reserved for future usage	0

Table 9: CAM SSPs.

** only for specific test-vehicles dedicated to test the emergency vehicle approaching use-case.*

A1.6. Secured Messages

Data Messages (DENM, IVI, MAP, SPAT, CAM) are signed following the guidelines of the standard ETSI 103 097 v1.2.1. Secured messages are built in Geonet layer and transmitted to the Security layer.

A1.7. Verification of message signature

The present section describes the general process of the message's signature verification by using CTL and CRL.

A1.7.1. Pre-conditions

For each native PKI system,

- The RCA certificate is provided to the ITS-S during the initialization phase.
- The RCA certificate, CTL and CRL are assumed to be valid.
- The CTL is available in an online repository.
- The CRL is available in the RCA repository of each country.
- The ITS-S shall verify that the CTL and the CRL are signed by home RCA

A1.7.2. Verification steps

The actual verification consists of the following four steps:

- **Step (1):** The ITS-S receives a secured message and verifies the message signature with the associated 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 AIDs list, time start and end…). The AA certificate may be retrieved either from a V2X secured exchange.
- **Step (3):** The ITS-S verifies that the AA certificate is issued by RCA.
- **Step (4):** The ITS-S checks that the HashedID8 of AA certificate is not present in CRL.

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.

A1.7.3. 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.

A1.8. CA certificates details

The following tables illustrate the details of the certificates used in test and issued by the different certificates authorities (CAs).

Co-financed by the European Union
Connecting Europe Facility

A1.8.1. Root CA certificate

Certificate data	Value
VERSION	2
SIGNER INFO	SELF
SUBJECT INFO	RCA
SUBJECT ATTRIBUTES	
Verification Key (0) **Algorithm:**	Ecdsa_nistp256_with_sha256
Encryption Key (1)	N/A
Assurance Level (2) **Assurance:** **Confidence:**	0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	N/A
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End **Start:** **End:**	Certificate issuance date 8 years after certificate issuance date
Geographic Region	NONE
SIGNATURE **Algorithm:**	Ecdsa_nistp256_with_sha256

Table 10: RCA certificate

A1.8.2. EA Certificate

Certificate data	Value
VERSION	2
SIGNER INFO	HashedId8 of RCA certificate
SUBJECT INFO	EA
SUBJECT ATTRIBUTES	
Verification Key (0) **Algorithm:**	ecdsa_nistp256_with_sha256
Encryption Key (1) **Algorithm:**	ecies_nistp56
Assurance Level (2) **Assurance:** **Confidence:**	0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	CA Basic Service (36) DEN Basic Service (37) SPAT (137) MAP (138) IVI (139)
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End **Start:** **End:**	Certificate issuance date 5 years after certificate issuance date
Geographic Region	NONE
SIGNATURE **Algorithm:**	Ecdsa_nistp256_with_sha256

Table 11: EA certificate

A1.8.3. AA Certificate

Certificate data	Value
VERSION	2
SIGNER INFO	HashedId8 of RCA certificate
SUBJECT INFO	AA
SUBJECT ATTRIBUTES	
Verification Key (0) **Algorithm:**	 ecdsa_nistp256_with_sha256
Encryption Key (1) **Algorithm:**	 ecies_nistp56
Assurance Level (2) **Assurance:** **Confidence:**	 0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	CA Basic Service (36) DEN Basic Service (37) SPAT (137) MAP (138) IVI (139)
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End **Start:** **End:**	 Certificate issuance date 5 years after certificate issuance date
Geographic Region	NONE

Table 12: AA Certificate

A1.9. C-Roads Cross Tests CTL and CRL formats

a. Certificate Revocation List

The Certificate Revocation List (CRL) is generated and signed by the RCA component.

ASN.1 notation definition

```
Crl ::= SEQUENCE {
    unsigned_crl ToBeSignedCrl,
    signature_algorithm SignatureAlgorithmIdentifier,
    signature Signature } -- signature is applied on unsigned_crl
```

```
ToBeSignedCrl ::= SEQUENCE {
    version Version,
    signer SignerIdentifier,
    -- ca_id HashedId8, -- redondant si le modèle crl_signer n'est pas supporté)
    thisUpdate Time32,
    nextUpdate Time32,
    entries SEQUENCE OF HashedId8 }
```

b. Trust-service Status List

ASN.1 notation definition

```
Tsl ::= SEQUENCE {
    unsigned_tsl ToBeSignedTsl,
    signature_algorithm SignatureAlgorithmIdentifier,
    signature SignatureValue }
-- signature is applied on unsigned_tsl
```

```
ToBeSignedTsl ::= SEQUENCE {
    version Version,
    signer_info SignerIdentifier,
    notBefore Time32,
    notAfter Time32,
    trust_services SEQUENCE OF TrustService }
```

```
TrustService ::= SEQUENCE {
    serviceId TRUSTSERVICE.&id ({TrustServiceSet}),
    serviceValue TRUSTSERVICE.&Value ({TrustServiceSet}{@serviceId}) }
```

```
TrustServiceSet TRUSTSERVICE ::=
    {   ts-foreignRoot
      | ts-renewedRoot
      | ts-ea
      | ts-aa
      | ts-distributionCenter
      | ts-otherTslPointer
      , ... }
```

```
TRUSTSERVICE ::= CLASS {
    &id ENUMERATED UNIQUE,
            &Value }
        WITH SYNTAX {
            SYNTAX &Value
            ID &id }
```

```
        ts-foreignRoot TRUSTSERVICE ::= {
            SYNTAX Certificate
            ID ServiceType:foreignRoot }
```

```
        ts-renewedRoot TRUSTSERVICE ::= {
            SYNTAX SEQUENCE {
                rootCertificate Certificate,
                linkRootCertificate Certificate }
            ID ServiceType:renewedRoot }
```

```
        ts-ea TRUSTSERVICE ::= {
            SYNTAX SEQUENCE {
                certificate Certificate,
                linkedCertificate Certificate OPTIONAL,
                accessPoint IA5STRING }
            ID ServiceType:ea }
```

```
        ts-aa TRUSTSERVICE ::= {
            SYNTAX SEQUENCE {
                certificate Certificate,
                accessPoint IA5STRING }
            ID ServiceType:aa }
```

```
        ts-distributionCenter TRUSTSERVICE ::= {
            SYNTAX IA5STRING
            ID ServiceType:distributionCenter }
```

```
        ts-otherTslPointer TRUSTSERVICE ::= {
            SYNTAX IA5STRING
            ID ServiceType:otherTslPointer }
```

```
        ServiceType ::= ENUMERATED {
            foreignRoot,
            renewedRoot,
            ea,
            aa,
            distributionCenter,
            otherTslPointer,
            ... }
```

ANNEX B – Cross-test requirements based on ETSI TS 103097 1.3.1 / TS 102 941 1.2.1

In this section the security requirements for the latest ETSI security formats are specified. In the same way as described in Annex A and depicted in Figure 6 cross tests should show the interoperability of different Root CA in scope of the C-ITS CP [3].
The objective also remains the same as described in Annex A to test whether the verification of message authentication is successful, including the validation of the trust chain as illustrated in Figure 7.

B1.1. Certificates formats

The certificates formats for CAs, ATs and ECs used for the C-Roads project are defined in ETSI TS 103 097 v1.3.1. Each ITS-S certificate is composed of several main fields:

- Version = 3,
- Signer Info = sha256AndDigest or certificate,
- CRA CA Id = 0x000000,
- CRL Series = 0,
- Validity start with duration,
- Assurance level = 0x00,
- App Permissions,
- Cert Issue Permissions, and
- Signature (NIST or Brainpool with 256 Bit = maximum 64 bytes).

The assurance level field shall contain the assurance level of the sender or certificate authority. A certificate shall contain an assurance level that is equal to or lower than the assurance level of the certificate referenced by the signer info. If the assurance level is unknown for the certificate, then the default assurance level 0 shall be used. In C-Roads Project, we set the values of both assurance level and confidence level in ITSS-certificates to 0.

The formats of used RCA-CTL and used CRLs are defined in ETSI TS 102 941 v1.2.1.

B1.2. Certificate validity

The CA certificate validity times are set to values as listed in Table 13.
This reduced time in contrast to the C-ITS CP [3] ensures that important PKI processes are performed within the pilot operation phase of C-Roads:

- Update of Root CA certificate with the help of link certificates
- Re-keying of EA and AA certificates
- Re-keying of EC certificates

Entity	Max. Private Key Usage period	Maximum Validity time
Root-CA	1y	2y
EA	6m	18m
AA	6m	1y
EC	1y	1y

Table 13: Validity periods of certificates in the pilot phase of C-Roads

B1.3. Cryptographic operations

There are different types of algorithms defined in ETSI Standard TS 103 097 v1.3.1 and the C-ITS CP [3], some used for signing, others for encryption. In C-Roads all these alrogithms are supported as summarized in the following:

- ECDSA_nistP256_with_SHA256
- ECDSA_brainpoolP256r1_with_SHA256
- ECDSA_brainpoolP384r1_with_SHA384
- ECIES_nistP256_with_AES128_CCM
- ECIES_brainpoolP256r1_with_AES128_CCM

B1.4. C-Roads ITS Application ID (ITS-AID)

The ITS-AID format used in C-Roads project is of type IntX (as described in ETSI TS 103 097 v1.3.1). Follwing [6], the ITS-AIDs chosen for the C-Roads project are listed in Table 4.

B1.5. Specific Service Permissions (SSPs)

The permissions of the root CA are listed in Table 14, the permissions of the EA in Table 15 and the permissions of the AA in Table 16.

The Service Specific Permission (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. For example, there may be an SSP value associated with the ITS-AID 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 value ‘x’ in the following tables may be set differently per country. For example the German country code is 0x94 according to ISO 14816 country code.

App Permissions		**sspValue (hex)**		**sspValue (binary)**	
624	CTL	0138		0000 0001 0011 1000	
622	CRL	01		0000 0001	
Issue Permissions		**sspValue (hex)**	**Bitmask (hex)**	**sspValue (binary)**	**Bitmask (binary)**
36	CAM	01FFFC	FF0000	0000 0001 1111 1111 1111 1100	1111 1111 0000 0000 0000 0011
37	DENM	01FFFFFF	FF000000	0000 0001 1111 1111 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000 0000 0000
137	TLM	01E8	FF07	0000 0001 1110 0000	1111 1111 0001 1111
138	RLT	01C0	FF1F	0000 0001 1100 0000	1111 1111 0011 1111
139	IVI	01xxx000FFF8	FF0000000007	0000 0001 xxxx xxxx xx00 0000 0000 0000 1111 1111 1111 1000	1111 1111 0000 0000 0000 0000 0000 0000 0000 0000 0000 0111
140	TLC	01FFFFE0	FF000001	0000 0001 1111 1111 1111 1111 1110 0000	1111 1111 0000 0000 0000 0000 0001 1111
141	GN_MGMT	00	FF	00000000	1111 1111
623	SC_MGMT	01FE	FF01	0000 0001 1111 1110	1111 1111 0000 0001

Table 14: Root CA permissions used in C-Roads

The value ‘x’ in Table 14 above shall contain the country code according to ISO 14816. A root CA with the permissions listed in Table 14 is permitted to issue sub CA certificates with all possible permissions.

App Permissions		**sspValue (hex)**		**sspValue (binary)**	
623	SC_MGMT	010E		0000 0001 0000 1110	
Issue Permissions		**sspValue (hex)**	**Bitmask (hex)**	**sspValue (binary)**	**Bitmask (binary)**
36	CAM	01FFFC	FF0000	0000 0001 1111 1111 1111 1100	1111 1111 0000 0000 0000 0011
37	DENM	01FFFFFF	FF000000	0000 0001 1111 1111 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000 0000 0000
137	TLM	01E8	FF07	0000 0001 1110 0000	1111 1111 0001 1111
138	RLT	01C0	FF1F	0000 0001 1100 0000	1111 1111 0011 1111
139	IVI	01xxx000FFF8	FF0000000007	0000 0001 xxxx xxxx xx00 0000 0000 0000 1111 1111 1111 1000	1111 1111 0000 0000 0000 0000 0000 0000 0000 0000 0000 0111
140	TLC	01FFFFE0	FF000001	0000 0001 1111 1111 1111 1111 1110 0000	1111 1111 0000 0000 0000 0000 0001 1111
141	GN_MGMT	00	FF	00000000	1111 1111
623	SC_MGMT	01C0	FF3F	0000 0001 1100 0000	1111 1111 0011 1111

Table 15: EA permissions used in C-Roads

The value ‘x’ in Table 15 above shall contain the country code according to ISO 14816. An EA with the permissions listed in Table 15 is permitted to issue EC certificates with all possible permissions.

App Permissions		sspValue (hex)		sspValue (binary)	
623	SC_MGMT	0132		0000 0001 0011 0010	
Issue Permissions		**sspValue (hex)**	**Bitmask (hex)**	**sspValue (binary)**	**Bitmask (binary)**
36	CAM	01FFFC	FF0000	0000 0001 1111 1111 1111 1100	1111 1111 0000 0000 0000 0011
37	DENM	01FFFFFF	FF000000	0000 0001 1111 1111 1111 1111 1111 1111	1111 1111 0000 0000 0000 0000 0000 0000
137	TLM	01E8	FF07	0000 0001 1110 0000	1111 1111 0001 1111
138	RLT	01C0	FF1F	0000 0001 1100 0000	1111 1111 0011 1111
139	IVI	01xxx000FFF8	FF0000000007	0000 0001 xxxx xxxx xx00 0000 0000 0000 1111 1111 1111 1000	1111 1111 0000 0000 0000 0000 0000 0000 0000 0000 0000 0111
140	TLC	01FFFFE0	FF000001	0000 0001 1111 1111 1111 1111 1110 0000	1111 1111 0000 0000 0000 0000 0001 1111
141	GN_MGMT	00	FF	00000000	1111 1111

Table 16: AA permissions used in C-Roads

The value ‘x’ in Table 16 above shall contain the country code according to ISO 14816. An AA with the permissions listed in Table 16 is permitted to issue AT certificates with all possible permissions.

App Permissions		sspValue (hex)	sspValue (binary)
36	CAM	01zzzz	0000 0001 zzzz zzzz zzzz zzzz
37	DENM	01zzzzzz	0000 0001 zzzz zzzz zzzz zzzz zzzz zzzz
137	TLM	01zz	0000 0001 zzzz z000
138	RLT	01z0	0000 0001 zzz0 0000
139	IVI	01xxxyyyzzzz	0000 0001 xxxx xxxx xxyy yyyy yyyy yyyy zzzz zzzz zzzz z000
140	TLC	01zzzzzz	0000 0001 zzzz zzzz zzzz zzzz zzzz zzz0
141	GN_MGMT	00	0000 0000
623	SC_MGMT	01C0	0000 0001 1100 0000

Table 17: EC permissions used in C-Roads

The value ‘x’ in Table 17 above shall contain the country code according to ISO 14816 and the value ‘y’ the provider ID which is defined in ETSI TS 103 301 but currently not assigned to specific values. The value ‘z’ can be set according to the station type.

App Permissions		sspValue (hex)	sspValue (binary)
36	CAM	01zzzz	0000 0001 zzzz zzzz zzzz zzzz
37	DENM	01zzzzzz	0000 0001 zzzz zzzz zzzz zzzz zzzz zzzz
137	TLM	01zz	0000 0001 zzzz z000
138	RLT	01z0	0000 0001 zzz0 0000
139	IVI	01xxxyyyzzzz	0000 0001 xxxx xxxx xxyy yyyy yyyy yyyy zzzz zzzz zzzz z000
140	TLC	01zzzzzz	0000 0001 zzzz zzzz zzzz zzzz zzzz zzz0
141	GN_MGMT	00	0000 0000

Table 18: AT permissions used in C-Roads

The value ‘x’ in Table 18 above shall contain the country code according to ISO 14816 and the value ‘y’ the provider ID which is defined in ETSI TS 103 301 but currently not assigned to specific values. The value ‘z’ can be set according to the station type.

B1.6. Secured Messages

Data Messages (CAM, DENM, SPAT, …) are signed following the guidelines of the standard ETSI 103 097 v1.3.1. Secured messages are built in Geonet layer and transmitted to the Security layer according to ETSI EN 302 636-4-1 v1.3.1.

B1.7. Verification of message signature

The present section describes the general process of the message's signature verification by using ECTL, RCA-CTL, and CRL.

B1.7.1. Pre-Conditions

For each native PKI system,

- The TLM certificate is provided to the ITS-S during the initialization phase.
- The ECTL is provided to the ITS-S during the initialization phase.
- The home RCA certificate or at least the ID of the home RCA is provided to the ITS-S during the initialization phase.
- The TLM certificate, ECTL, RCA certificate, RCA-CTL and CRL are assumed to be valid.
- The RCA-CTL is available in an RCA repository of each country.
- The CRL is available in the RCA repository of each country.
- The ITS-S shall verify that the ECTL is signed by the TLM.
- The ITS-S shall verify that the RCA-CTL and the CRL are signed by the home RCA.

B1.7.2. Verification steps

All RCA certificates containted 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.
- **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 AIDs list, time start and duration…). The AA certificate may be retrieved either from a V2X secured exchange.
- **Step (3)**: The ITS-S verifies that the AA certificate is issued by RCA.
- **Step (4)**: The ITS-S checks that the HashedID8 of AA certificate is not present in CRL.

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.

B1.7.3. 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.

B1.8. CA certificates details

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

B1.8.1. 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 463739060,
      duration hours : 17544
    },
    assuranceLevel '00'H,
    appPermissions {
      {
        psid 624,
        ssp bitmapSsp : '0138'H
      },
      {
        psid 622,
        ssp bitmapSsp : '01'H
      }
    },
    certIssuePermissions {
      {
        subjectPermissions explicit : {
          {
            psid 36,
            sspRange bitmapSspRange : {
              sspValue '01FFFF'H,
              sspBitmask 'FF0000'H
            }
          },
          {
            psid 37,
            sspRange bitmapSspRange : {
              sspValue '01FFFFFF'H,
              sspBitmask 'FF000000'H
            }
          },
          {
            psid 137,
            sspRange bitmapSspRange : {
              sspValue '01F8'H,
              sspBitmask 'FF07'H
            }
          },
          {
            psid 138,
            sspRange bitmapSspRange : {
              sspValue '01E0'H,
              sspBitmask 'FF1F'H
            }
          },
          {
            psid 139,
            sspRange bitmapSspRange : {
              sspValue '01940000FFF8'H,
              sspBitmask 'FF0000000007'H
            }
          },
          {
            psid 140,
            sspRange bitmapSspRange : {
              sspValue '01FFFFFE'H,
              sspBitmask 'FF000001'H
            }
          },
          {
            psid 141,
            sspRange bitmapSspRange : {
              sspValue '00'H,
              sspBitmask 'FF'H
            }
          },
          {
            psid 623,
            sspRange bitmapSspRange : {
              sspValue '01FE'H,
              sspBitmask 'FF01'H
            }
          }
        },
        minChainLength 2,
        eeType {app, enrol}
      }
    },
    verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'5D9B66F9884826D40859B2D4B7957BBC35EDAEAFC8095FBFC08BDC1592CC2077'H
  },
  signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'2EAA2DA6C65969D93D3D0E19DC345D255BE99F61718CECEF2E7BFC587EA5D657'H,
    sSig
'8602F86186CE3E2193CF76346B9EDA7CF84B533CEC12ACE59984948A2371257C'H
  }
}
```

B1.8.2. EA certificate

```
EtsiTs103097Certificate ::= {
   version 3,
   type explicit,
   issuer sha256AndDigest : '4343CC539698F7D9'H,
   toBeSigned {
     id name : "BSI V2X Pilot PKI EA",
     cracaId '000000'H,
     crlSeries 0,
     validityPeriod {
        start 463837260,
        duration hours : 14592
     },
     assuranceLevel '00'H,
     appPermissions {
        {
          psid 623,
          ssp bitmapSsp : '010E'H
        }
     },
     certIssuePermissions {
        {
          subjectPermissions explicit : {
             {
               psid 36,
               sspRange bitmapSspRange : {
                  sspValue '01FFFF'H,
                  sspBitmask 'FF0000'H
               }
             },
             {
               psid 37,
               sspRange bitmapSspRange : {
                  sspValue '01FFFFFF'H,
                  sspBitmask 'FF000000'H
               }
             },
             {
               psid 137,
               sspRange bitmapSspRange : {
                  sspValue '01F8'H,
                  sspBitmask 'FF07'H
               }
             },
             {
               psid 138,
                sspRange bitmapSspRange : {
                   sspValue '01E0'H,
                   sspBitmask 'FF1F'H
                }
              },
              {
                psid 139,
                sspRange bitmapSspRange : {
                   sspValue '01940000FFF8'H,
                   sspBitmask 'FF0000000007'H
                }
              },
              {
                psid 140,
                sspRange bitmapSspRange : {
                   sspValue '01FFFFFE'H,
                   sspBitmask 'FF000001'H
                }
              },
              {
                psid 141,
                sspRange bitmapSspRange : {
                   sspValue '00'H,
                   sspBitmask 'FF'H
                }
              },
              {
                psid 623,
                sspRange bitmapSspRange : {
                   sspValue '01C0'H,
                   sspBitmask 'FF3F'H
                }
              }
          },
          eeType {enrol}
        }
     },
     encryptionKey {
        supportedSymmAlg aes128Ccm,
        publicKey eciesBrainpoolP256r1 : compressed-y-1 :
'0F6B7102A287E454F83C24E8A36B1E907CF1D84D153B6EA50CA00BDF3F5E422E'H
     },
     verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'A707BEEC3AE3532F218EB021C223B669A7966E0B6AE2058746FB88A8545D7ACA'H
   },
   signature ecdsaBrainpoolP256r1Signature : {
     rSig x-only :
'0F5C28CA8775A484341A61AA3C29FCAF3BE516A4ECF345887F46DB6EB155BB85'H,
     sSig
'79F9795FBAA9E546D86B1551F3A51B38A3DFE8E8E28D9CBE2F3E9A16CF916F26'H
   }
```

```
}
```

B1.8.3. AA certificate

```
EtsiTs103097Certificate ::= {
   version 3,
   type explicit,
   issuer sha256AndDigest : '4343CC539698F7D9'H,
   toBeSigned {
     id name : "BSI V2X Pilot PKI AA",
     cracaId '000000'H,
     crlSeries 0,
     validityPeriod {
        start 463837456,
        duration hours : 8760
     },
     assuranceLevel '00'H,
     appPermissions {
        {
          psid 623,
          ssp bitmapSsp : '0132'H
        }
     },
     certIssuePermissions {
        {
          subjectPermissions explicit : {
             {
               psid 36,
               sspRange bitmapSspRange : {
                  sspValue '01FFFF'H,
                  sspBitmask 'FF0000'H
               }
             },
             {
               psid 37,
               sspRange bitmapSspRange : {
                  sspValue '01FFFFFF'H,
                  sspBitmask 'FF000000'H
               }
             },
             {
               psid 137,
               sspRange bitmapSspRange : {
                  sspValue '01F8'H,
                  sspBitmask 'FF07'H
               }
             },
             {
               psid 138,
               sspRange bitmapSspRange : {
                  sspValue '01E0'H,
                  sspBitmask 'FF1F'H
               }
             },
             {
               psid 139,
               sspRange bitmapSspRange : {
                  sspValue '01940000FFF8'H,
                  sspBitmask 'FF0000000007'H
               }
             },
             {
               psid 140,
               sspRange bitmapSspRange : {
                  sspValue '01FFFFFE'H,
                  sspBitmask 'FF000001'H
               }
             },
             {
               psid 141,
               sspRange bitmapSspRange : {
                  sspValue '00'H,
                  sspBitmask 'FF'H
               }
             }
          }
        }
    },
    encryptionKey {
        supportedSymmAlg aes128Ccm,
        publicKey eciesNistP256 : compressed-y-1 :
'8F712F01C6BB6B86FADECDF7D4AF6999AFABC2612E5DDF73E8C07343E96C1364'H
    },
    verifyKeyIndicator verificationKey : ecdsaNistP256 : compressed-y-1
: '6B022C47E20CE3DD3F86914B29EF3EFC7A14CD1FB4AC5E6299D51D330B131684'H
  },
  signature ecdsaBrainpoolP256r1Signature : {
    rSig x-only :
'4459ECB69048C27C51B129AA68522AA17AE85755CA14D04650A0AD66277CE311'H,
    sSig
'A7F85126D3EE013F3163ADE27E8C754020343CD57D0708FEAFC5FA3F9F685667'H
  }
}
```

B1.9. RCA-CTL details

```
value RcaCertificateTrustListMessage ::= {
  protocolVersion 3,
  content signedData : {
    hashId sha256,
    tbsData {
      payload {
        data {
          protocolVersion 3,
          content unsecuredData : CONTAINING {
            version v1,
            content certificateTrustListRca : {
              version v1,
              nextUpdate 471614485,
              isFullCtl TRUE,
              ctlSequence 0,
              ctlCommands {
                add : dc : {
                  url "http://bsi.v2x-pilot.escrypt.com/dc",
                  cert {}
                },
                add : ea : {
                  eaCertificate {
                    version 3,
                    type explicit,
                    issuer sha256AndDigest : '4343CC539698F7D9'H,
                    toBeSigned {
                      id name : "BSI V2X Pilot PKI EA",
                      cracaId '000000'H,
                      crlSeries 0,
                      validityPeriod {
                        start 463837260,
                        duration hours : 14592
                      },
                      assuranceLevel '00'H,
                      appPermissions {
                        {
                          psid 623,
                          ssp bitmapSsp : '010E'H
                        }
                      },
                      certIssuePermissions {
                        {
                          subjectPermissions explicit : {
                            {
                              psid 36,
                              sspRange bitmapSspRange : {
                                sspValue '01FFFF'H,
                                sspBitmask 'FF0000'H
                              }
                            },
    {
      psid 37,
      sspRange bitmapSspRange : {
        sspValue '01FFFFFF'H,
        sspBitmask 'FF000000'H
      }
    },
    {
      psid 137,
      sspRange bitmapSspRange : {
        sspValue '01F8'H,
        sspBitmask 'FF07'H
      }
    },
    {
      psid 138,
      sspRange bitmapSspRange : {
        sspValue '01E0'H,
        sspBitmask 'FF1F'H
      }
    },
    {
      psid 139,
      sspRange bitmapSspRange : {
        sspValue '01940000FFF8'H,
        sspBitmask 'FF0000000007'H
      }
    },
    {
      psid 140,
      sspRange bitmapSspRange : {
        sspValue '01FFFFFE'H,
        sspBitmask 'FF000001'H
      }
    },
    {
      psid 141,
      sspRange bitmapSspRange : {
        sspValue '00'H,
        sspBitmask 'FF'H
      }
    },
    {
      psid 623,
      sspRange bitmapSspRange : {
        sspValue '01C0'H,
        sspBitmask 'FF3F'H
      }
    }
  },
  eeType {enrol}
}
```

```
                      },
                      encryptionKey {
                        supportedSymmAlg aes128Ccm,
                        publicKey eciesBrainpoolP256r1 : compressed-y-1
: '0F6B7102A287E454F83C24E8A36B1E907CF1D84D153B6EA50CA00BDF3F5E422E'H
                      },
                      verifyKeyIndicator verificationKey :
ecdsaBrainpoolP256r1 : compressed-y-1 :
'A707BEEC3AE3532F218EB021C223B669A7966E0B6AE2058746FB88A8545D7ACA'H
                    },
                    signature ecdsaBrainpoolP256r1Signature : {
                      rSig x-only :
'0F5C28CA8775A484341A61AA3C29FCAF3BE516A4ECF345887F46DB6EB155BB85'H,
                      sSig
'79F9795FBAA9E546D86B1551F3A51B38A3DFE8E8E28D9CBE2F3E9A16CF916F26'H
                    }
                  },
                  aaAccessPoint "http://dockerv2xpilot_ea_1:8080/ea",
                  itsAccessPoint "http://bsi.v2x-pilot.escrypt.com/ea"
                },
                add : aa : {
                  aaCertificate {
                    version 3,
                    type explicit,
                    issuer sha256AndDigest : '4343CC539698F7D9'H,
                    toBeSigned {
                      id name : "BSI V2X Pilot PKI AA",
                      cracaId '000000'H,
                      crlSeries 0,
                      validityPeriod {
                        start 463837456,
                        duration hours : 8760
                      },
                      assuranceLevel '00'H,
                      appPermissions {
                        {
                          psid 623,
                          ssp bitmapSsp : '0132'H
                        }
                      },
                      certIssuePermissions {
                        {
                          subjectPermissions explicit : {
                            {
                              psid 36,
                              sspRange bitmapSspRange : {
                                sspValue '01FFFF'H,
                                sspBitmask 'FF0000'H
                              }
                            },
                            {
                              psid 37,
                              sspRange bitmapSspRange : {
                                sspValue '01FFFFFF'H,
                                sspBitmask 'FF000000'H
                              }
                            },
                            {
                              psid 137,
                              sspRange bitmapSspRange : {
                                sspValue '01F8'H,
                                sspBitmask 'FF07'H
                              }
                            },
                            {
                              psid 138,
                              sspRange bitmapSspRange : {
                                sspValue '01E0'H,
                                sspBitmask 'FF1F'H
                              }
                            },
                            {
                              psid 139,
                              sspRange bitmapSspRange : {
                                sspValue '01940000FFF8'H,
                                sspBitmask 'FF0000000007'H
                              }
                            },
                            {
                              psid 140,
                              sspRange bitmapSspRange : {
                                sspValue '01FFFFFE'H,
                                sspBitmask 'FF000001'H
                              }
                            },
                            {
                              psid 141,
                              sspRange bitmapSspRange : {
                                sspValue '00'H,
                                sspBitmask 'FF'H
                              }
                            }
                          }
                        }
                      },
                      encryptionKey {
                        supportedSymmAlg aes128Ccm,
                        publicKey eciesNistP256 : compressed-y-1 :
'8F712F01C6BB6B86FADECDF7D4AF6999AFABC2612E5DDF73E8C07343E96C1364'H
                      },
                      verifyKeyIndicator verificationKey : ecdsaNistP256
: compressed-y-1 :
'6B022C47E20CE3DD3F86914B29EF3EFC7A14CD1FB4AC5E6299D51D330B131684'H
                    },
                    signature ecdsaBrainpoolP256r1Signature : {
                      rSig x-only :
'4459ECB69048C27C51B129AA68522AA17AE85755CA14D04650A0AD66277CE311'H,
                      sSig
'A7F85126D3EE013F3163ADE27E8C754020343CD57D0708FEAFC5FA3F9F685667'H
                    }
                  },
                  accessPoint "http://bsi.v2x-pilot.escrypt.com/aa"
                }
              }
            }
          }
        }
      },
      headerInfo {
        psid 624,
        generationTime 463838485354000
      }
    },
    signer certificate : {
      {
        version 3,
        type explicit,
        issuer self : sha256,
        toBeSigned {
          id name : "BSI V2X Pilot PKI Root",
          cracaId '000000'H,
          crlSeries 0,
          validityPeriod {
            start 463739060,
            duration hours : 17544
          },
          assuranceLevel '00'H,
          appPermissions {
            {
              psid 624,
              ssp bitmapSsp : '0138'H
            },
            {
              psid 622,
              ssp bitmapSsp : '01'H
            }
          },
          certIssuePermissions {
            {
              subjectPermissions explicit : {
                {
                  psid 36,
                  sspRange bitmapSspRange : {
                    sspValue '01FFFF'H,
                    sspBitmask 'FF0000'H
                  }
    },
    {
      psid 37,
      sspRange bitmapSspRange : {
        sspValue '01FFFFFF'H,
        sspBitmask 'FF000000'H
      }
    },
    {
      psid 137,
      sspRange bitmapSspRange : {
        sspValue '01F8'H,
        sspBitmask 'FF07'H
      }
    },
    {
      psid 138,
      sspRange bitmapSspRange : {
        sspValue '01E0'H,
        sspBitmask 'FF1F'H
      }
    },
    {
      psid 139,
      sspRange bitmapSspRange : {
        sspValue '01940000FFF8'H,
        sspBitmask 'FF0000000007'H
      }
    },
    {
      psid 140,
      sspRange bitmapSspRange : {
        sspValue '01FFFFFE'H,
        sspBitmask 'FF000001'H
      }
    },
    {
      psid 141,
      sspRange bitmapSspRange : {
        sspValue '00'H,
        sspBitmask 'FF'H
      }
    },
    {
      psid 623,
      sspRange bitmapSspRange : {
        sspValue '01FE'H,
        sspBitmask 'FF01'H
      }
    }
  },
minChainLength 2,
              eeType {app, enrol}
            }
          },
          verifyKeyIndicator verificationKey : ecdsaBrainpoolP256r1 :
compressed-y-1 :
'5D9B66F9884826D40859B2D4B7957BBC35EDAEAFC8095FBFC08BDC1592CC2077'H
        },
        signature ecdsaBrainpoolP256r1Signature : {
          rSig x-only :
'2EAA2DA6C65969D93D3D0E19DC345D255BE99F61718CECEF2E7BFC587EA5D657'H,
          sSig
'8602F86186CE3E2193CF76346B9EDA7CF84B533CEC12ACE59984948A2371257C'H
        }
      }
    },
    signature ecdsaBrainpoolP256r1Signature : {
      rSig x-only :
'81C3209C1B16EE4B131CF7031C04CE5F0EA23D20CBA293A1F7A0FCFF9433FA35'H,
      sSig
'6107FB62B3184925E17AC4F1EDA5C1849040491CFFE0731019E92711F12DCFE9'H
    }
  }
}
```