



C-ITS Security & Governance

C-Roads platform, Working Group 2, Task Force 1

Version 2.2.0

28.05.2024

Table of Content

List of Figures	3
List of Tables	3
Document history	4
List of used abbreviations	5
1 Introduction	6
1.1 C-Roads platform for harmonisation of C-ITS deployment	6
1.2 Story board C-Roads C-ITS deployment documentation	7
1.3 Scope of this document	8
2 A secure European C-ITS System	9
2.1 Overview	9
2.2 Most relevant standards	11
2.3 A hybrid communication system	11
2.4 EU CCMS Levels and timeline	13
2.5 Basic security aspects for C-ITS	14
2.6 Concept of Service Specific Permissions (SSP)	16
3 C-Roads tests & non-production pilots (L0)	17
3.1 Security elements and governance	18
3.2 PKI operation	19
3.3 Security provisions of C-Roads pilots	19
3.4 Potential areas of cooperation and harmonization	23
4 C-Roads pilots regular operation (L1)	24
References	26

List of Figures

Figure 1: C-ITS Trust Model Architecture, see section 1.3.1 of the CP [1]	9
Figure 2: C-ITS Trust Model Information Flows, see section 1.3.1 of the CP [1]	10
Figure 3: C-ITS message embedded as payload – additional security layer outside of C-ITS message structure	12
Figure 4: Different levels of security and trust as foreseen by the European Commission.....	13
Figure 5: ECTL levels timeline	14
Figure 6: Concept of permissions in certificates - functionally required vs restricted SSPs	17

List of Tables

Table 1: Main Interoperability Requirements.....	11
Table 2: PKI systems (providing certificates based on ETSI TS 103 097) foreseen by the Member States and C-Roads pilots	20

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
0.5	17.10.2017	Chapter 4 input by M. Medina, comments M. Helene Badiali, IDnomic Chapter 3 input by A. Froetscher, Atech	Draft
0.6	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	Draft
0.8	20.12.2017	Update chapter 2, and comments Atech	Draft
0.9	Mar. 2018	Updated content in various chapters, including statements from C-Roads members, TF3 Eindhoven Meeting, changes discussed and accepted	Draft
1.0	Sep. 2018	UK comments and native speaker review	Draft
1.1	Sep. 2018	Annex B included, document updated 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	Draft
1.4	Jan. 2019	Reviewed Hungarian contribution updated	Approved (Annexes in Draft)
1.5	April 2019	Hybrid communication part updated, UK contribution added/updated, Annex B: Validation steps introduced, certificates updated	Draft
1.6	May 2019	VRO SSPs added	Draft
1.7	Aug. 2019	1.6 remarks considered, annex B updated	Draft
1.7.5	May 2020	Transfer of annexes A & B to TF1 Security requirements document	Draft
1.8.0	May 2020	Complete document overhaul and restructuring: one overview and governance part, separate technical specifications and requirements	Draft
1.8.1	June 2020	Feedback from all WG2 observation forms integrated as far as possible	Draft
1.8.2	July 2020	Inclusion of agreed modifications after WG2 review, insertion of common C-Roads introduction	Draft
1.8.5	Sept. 2020	Feedback from all WG2 observation forms	Draft
2.0.0	Aug. 2021	Editorial cleanup, reference updated, section 2.6 on SSP concept added	Draft
2.0.4	June 2022	Insertion of EU CCMS levels description and document restructuring accordingly	Approved
2.0.5	Aug./Sept. 202	Transfer of the delegation concept from the security requirements document, alignment of the documents, comment resolution in TF1	Draft
2.0.7	Mar. 2023	Update of the delegation section following dedicated workshops and WG2 meeting	Approved
2.2.0	May 2024	Update following the availability of the PP and the CP/SP update	Draft

List of used abbreviations

AA	Authorization Authority
AT	Authorization Ticket
API	Application Programming Interface
C2C-CC	Car to Car Communication Consortium
CA	Certificate Authority
C-ITS	Cooperative ITS
CCMS	C-ITS Security Credential Management System
CP	Certificate Policy
CPA	Certificate Policy Authority
CPS	Certificate Practice Statement
CPOC	C-ITS Point of Contact
CTL	Certificate Trust List
EA	Enrolment Authority
EC	Enrolment Certificate
EE	End Entity
ECTL	European Certificate Trust List
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
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 – Security Aspects
TLM	Trust List Manager
TLS	Transport Layer Security - Internet Engineering Task Force (IETF) RFC 8446
WG2	Working Group 2

1 Introduction

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

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

C-ITS enables vehicles to interact directly with each other and the surrounding road infrastructure. In road transport, C-ITS typically involves vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In order to enable an efficient and undisturbed exchange of information within these services as well as a cross-border implementation, harmonised C-ITS specifications are indispensable. The approach starts from a functional perspective, then requirements applicable to all implementations and then towards technology specifications of currently validated implementations (ITS-G5 for short range communication, IP based for long range cellular). In order to meet these challenges, the C-ROADS platform is divided into five Working Groups. The first Working Group is concerned with organisational tasks, the second with Technical Aspects and the third with Evaluation and Assessment. The fourth Working Group is about Urban C-ITS Harmonisation and Working Group 5 is about Digital Transport Infrastructure (DTI).

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

The Working Groups are installed as decision support for the Steering Committee to ensure proper decisions towards interoperable deployments. Individual experts participating in the single pilots work together in these Working Groups to prepare proposals and recommendations. Also, members of the single pilot activities as well as of the C-Roads-Working Groups actively contribute to the work of the EU-C-ITS-Platform.

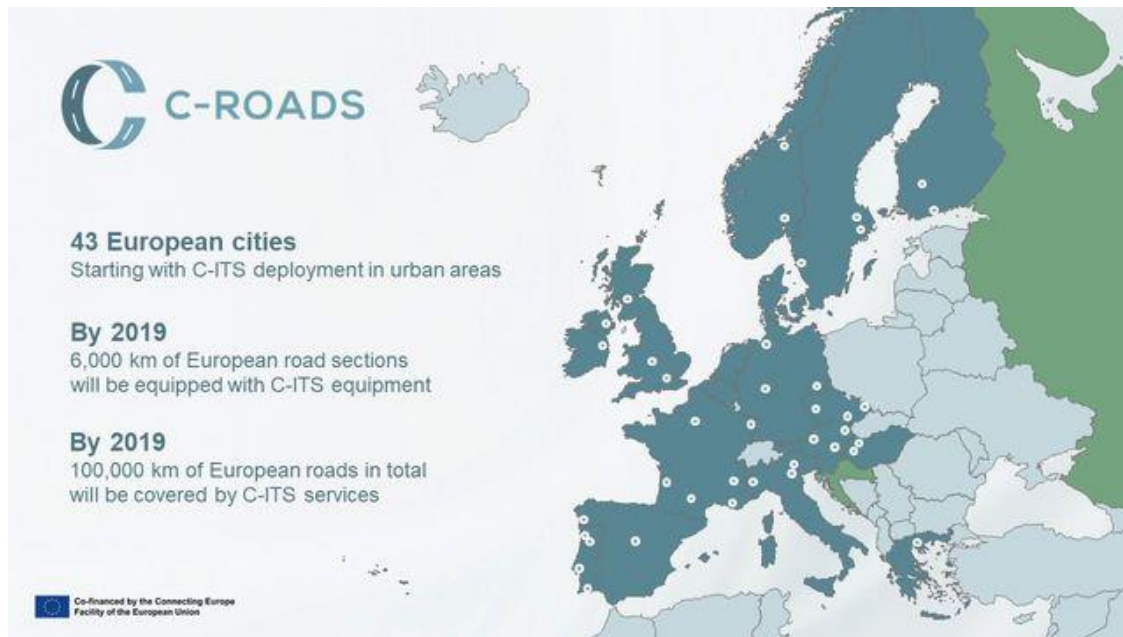


Figure 1: Overview of C-Roads coverage

1.2 Story board C-Roads C-ITS deployment documentation

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

A complete description of the story board of a C-ITS implementation project, the different stages and the related C-Roads documents is given in *Introduction to the C-Roads WG2 Deployment Documentation and Requirements*.

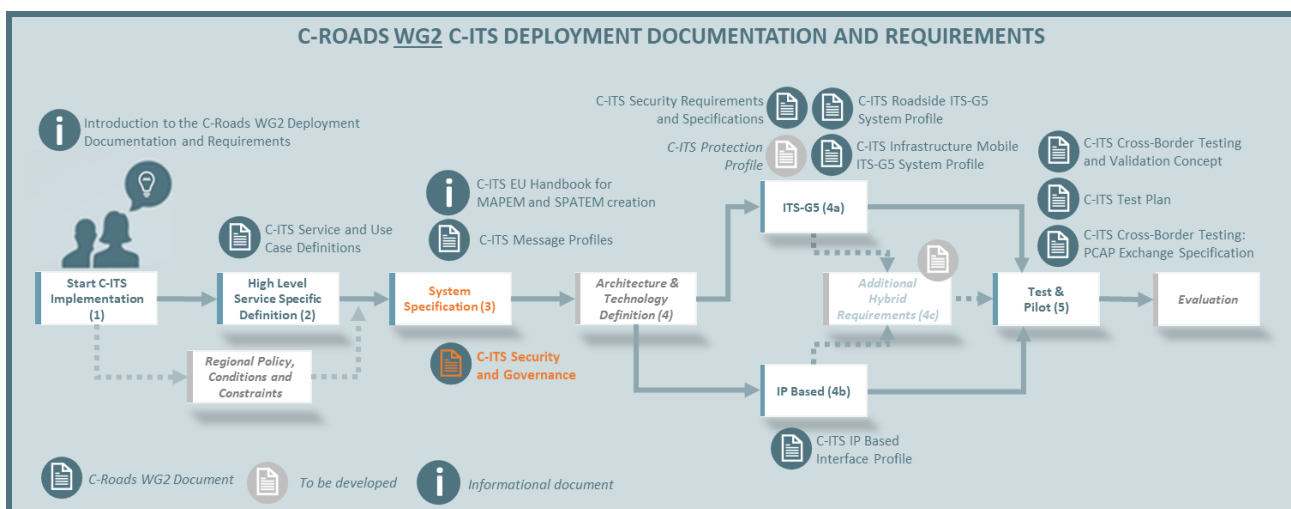


Figure 2: highlight of WG2 document in complete story board

The documents cover a wide range of aspects related to several stages as described in section 1.4 of *Introduction to the C-Roads WG2 Deployment Documentation and Requirements*. Starting with stage 3, generic requirements and the required governance are specified - those are applicable for all services, use cases and scenarios in a similar way. On stage 4a and 4b, the more detailed specifications are relevant - including service specific security requirements. Both levels, generic and specific requirements, have impact on the test cases derived on stage 5.

1.3 Scope of this document

This document provides an overall introduction to the common European trust model and builds on the European Certificate Policy for C-ITS, which is referring to the relevant ETSI standards for certificates and PKI management as the underlying technical basis. These provisions are valid for all services, use cases and scenarios harmonized within C-Roads. This document also describes common agreements that are important for C-Roads and other European C-ITS stakeholders, covering a level of developments and testing within and across different C-Roads pilots as well as the relation to the levels of regular and continuous operation.

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. This version also considers IP-based 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.

The C-ITS security aspects described within this document have initially been based on two documents that the EU C-ITS Platform had produced in 2017 and updated in 2019:

- CP – Certificate Policy [1]
- SP – Security Policy [2]

Further reference documents are ETSI and CEN/ISO standards that provide security requirements for the use of a PKI to secure V2X communications. Besides these agreed policy requirements and related standards, additional guidance and detailed protocol specifications have been elaborated.

This report concentrates on the C-ITS implementation in the C-Roads pilots according to the requirements derived from aforementioned policies. Following a general introduction in chapter 1, security aspects relevant for the European CCMS are presented in chapter 2. Chapter 3 and 4 complete this report with a set of governance recommendations for testing and pilots as well as the phase of regular operation of C-ITS systems and services in Europe.

Technical details and requirements as well as information related to security testing are specified in a separate TF1 document “C-ITS Security Requirements” [5].

In addition to these two documents, the “hardening” and respective security certification of C-ITS stations is a CP requirement to be considered by all C-ITS station operators. Therefore a “Protection Profile” [4] has been created according to Common Criteria, ISO/IEC 15408.

None of these reports/documents provide a comprehensive list containing *all* “cybersecurity aspects” of C-ITS stations and technical elements and the necessary provisions for preventing general IT security attacks. Out of scope are topics which are not (yet) included in the EU policy considerations. This includes: misbehaviour detection of single ITS stations; misuse of certificates; intrusion detection; security for the integration of C-ITS stations into other systems and secure operational processes beyond the requirements of the CP (i.e. ISMS); misuse of the entities within the EU Trust Model.

2 A secure European C-ITS System

C-Roads specifications detail various C-ITS aspects – e.g. service and use case definitions, message formats and their content – including essential security requirements.

In order to ensure authenticity and integrity of the exchanged C-ITS messages as well as the authorization of (previously unknown) senders, digital certificates are used. The respective public and private keys associated with these digital certificates allow users to sign and verify digital signatures, commonly known as public key cryptography.

2.1 Overview

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 Public Key Infrastructure comprising all C-ITS stations, vehicle-based ones and road infrastructure-based ones governed by one common CP - Certificate Policy. As the sum of all rules that need to be adhered to by all participants, the CP defines a common trust domain.

In C-Roads TF1, the classification and the definition of roles indicated in the CP and SP have been adopted. Definitions of all essential roles that are depicted in Figure 1 are provided in CP and SP as well. The governing body responsible for the maintenance and evolution of the CP is the CPA – Certificate Policy Authority, which also is responsible for checking the compliance of the members of the trust domain.

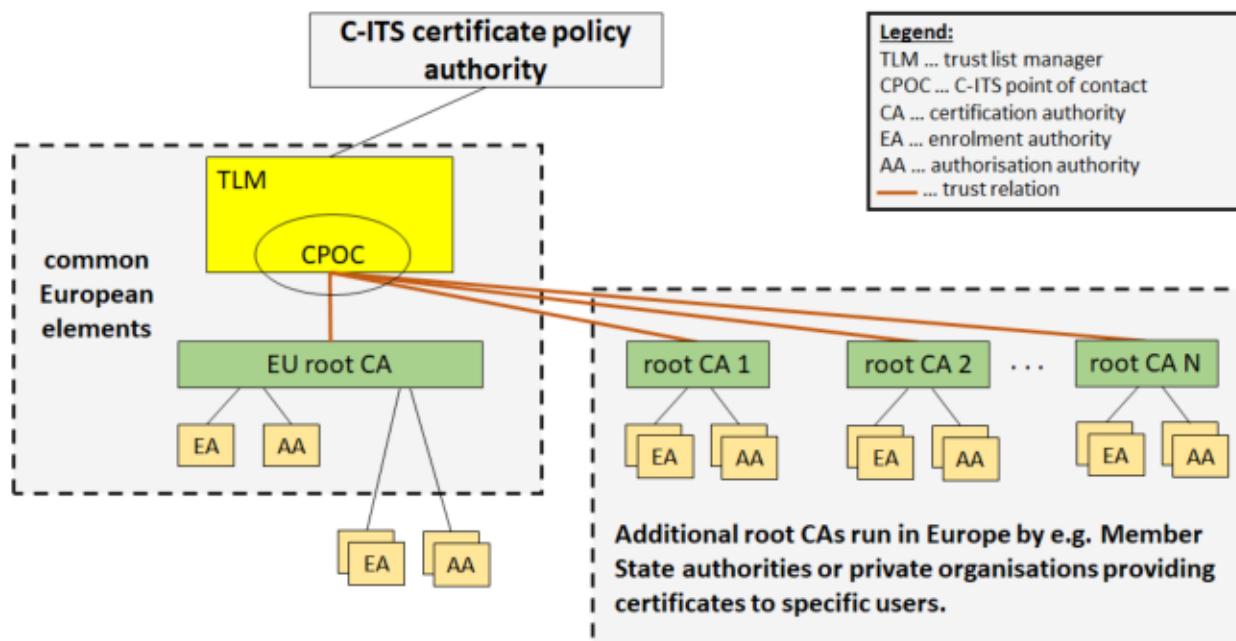


Figure 1: C-ITS Trust Model Architecture, see section 1.3.1 of the CP [1]

While the actual operation of the PKI systems might be under the control of individual Member States or industry players (“Root CA 1” to “Root CA N” in Figure 1) or under the control of the European Root CA, there are important central entities foreseen in CP and SP which need to be used commonly by all members of the common trust domain. In particular the following entities are to be used commonly and can not be run in separate instances:

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

Without the use of the following central entities, there is no mutual trust across the different PKI systems and therefore no common trust domain.

This also applies to all C-Roads pilots and partners.

As of May 2020, these central entities are ready to be provided by the European Commission and are to be used by all C-Roads partners. For a detailed explanation of possible trust levels that can be provided and used, see section 2.4.

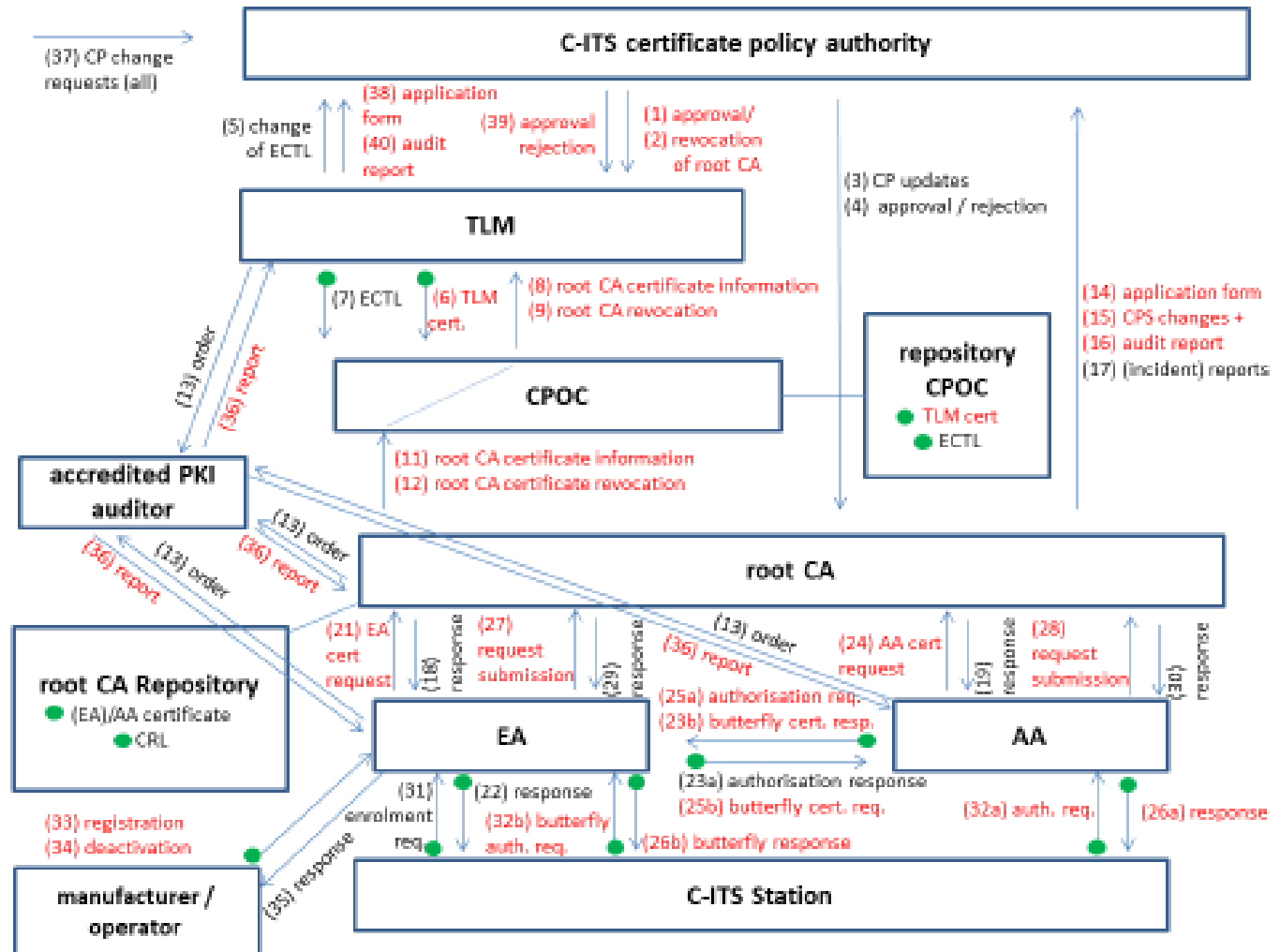


Figure 2: C-ITS Trust Model Information Flows, see section 1.3.1 of the CP [1]

This CP also describes the details of the security provisions including the responsibilities of the C-ITS station operators along the complete chain of trust via EA – Enrolment Authority, AA – Authorisation Authority and Root CA's to the central EU elements, CPOC – C-ITS Point of Contact and TLM - Trust List Manager. In the CP, also the process and communication steps between all entities are defined for the connection to other basic elements of the PKI, see Figure 2. In order to ensure the same level of security as applied within the PKI systems, also the communication links with external entities are properly defined by the CP, e.g. when transmitting authorisation tickets or enrolment certificates to a single C-ITS station, which is also depicted in Figure 2.

2.2 Most relevant standards

Within the context of TF1, a thorough analysis of the existing security standards has been conducted. The main interoperability requirements detailed in existing standards are summarized in the following Table 1.

Table 1: Main Interoperability Requirements

Specifications	Details
Governance	EU C-ITS Security Policy [2]
Trust Model	EU C-ITS Certificate Policy [1]
Certificate Data Structure	ETSI TS 103 097 [8]
Cryptographic Algorithms	ETSI TS 103 097 [8] NIST / Brainpool EU C-ITS Certificate Policy [1]
Download C-Roads CTL	ETSI TS 102 941 [9]
Download C-Roads CRL	
C-Roads CTL data structure	
C-Roads CRL data structure	
GeoNet - secured packets in C-ITS messages	ETSI EN 302 636-4-1 [10]

2.3 A hybrid communication system

Appropriate security mechanisms are required to assure that only trustworthy parties interact with each other, maintaining the trust in integrity and authenticity of all C-ITS messages. This applies for all C-ITS services, whether they are provided in broadcast scenarios or via IP-based communication with and between backend systems or a “hybrid” combination of these communication paths.

PLEASE NOTE

For evolving “hybrid” communication systems, it is useful to keep the following distinction in mind:

- The term “broadcast” currently refers to ETSI ITS G5 communication based on IEEE 802.11p in the 5.9 GHz band, but can also comprise short range communications features for evolving communication technologies.
- The term “IP-based” networks comprises wired (backend/cloud) systems and wireless (cellular) networks. Again, this includes existing (3G/4G) mobile networks as well as future (5G/6G) network generations.

The term “C-ITS station” is defined as the set of hardware and software components required to collect, store, process, receive and transmit secured and trusted messages in order to enable the provision of a C-ITS service. This includes personal, central, vehicle and roadside ITS stations as defined in EN 302 665 v 1.1.1.

This definition is not limited to a specific communication technology; hence it is applicable for broadcast systems as well as for IP-based communication networks. The referenced ETSI standard describes the ITS station architecture, including mandatory security interfaces, using digital certificates according to ETSI TS 103 097 to authenticate senders of C-ITS message. This security mechanism is relying on the networking layer of the ETSI station architecture (GeoNet).

The exchange of signed messages and the related digital certificates is sufficient for broadcast scenarios with unknown recipients, i.e. ETSI ITS G5.

For IP-based communication that needs to be secured by TLS, additional aspects need to be considered, which is done in C-Roads Task Force 4. Also additional header(s) and features like message routing/queuing come into play, which are required to efficiently distribute a C-ITS messages, which are embedded as payload, as shown in Figure 3.

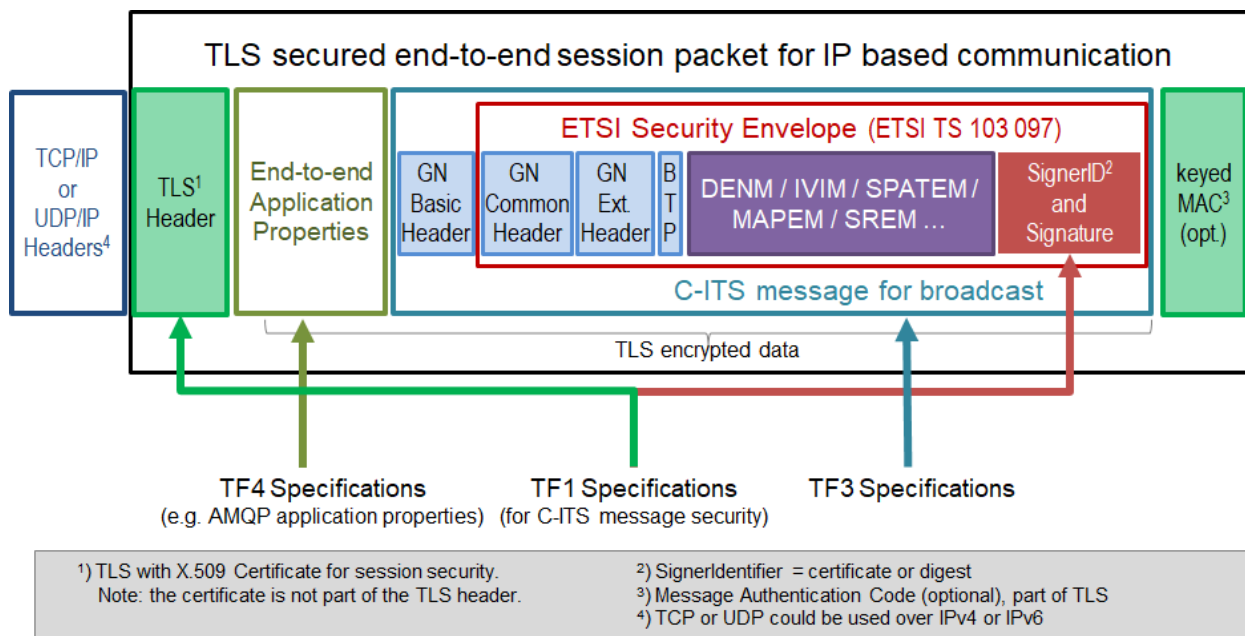


Figure 3: C-ITS message embedded as payload – additional security layer outside of C-ITS message structure

The current working assumption is that all security requirements are fulfilled by using TLS version 1.3 according to IETF RFC 8446 on top of the C-ITS security concept.

This means that in addition to C-ITS message signing and authentication with the use of certificates according to ETSI TS 103 097, IP-based communication will be secured by X.509 certificates according to IETF RFC 5280.

PLEASE NOTE

The exchange of “C-ITS messages” therefore implies that the GeoNet-layer needs to be implemented in every C-ITS station – even for communication only between backends.

This also implies that identifiers of C-ITS messages, which are required by the ETSI architecture, remain the same across various communication channels.

Additional security aspects might need to be implemented specifically for hybrid communication of C-ITS messages. The corresponding security requirements will be identified and specified as the architecture for hybrid communication evolves. This will be done in close collaboration with TF4. As standards for ITS communication between wide area connected ITS stations are evolving, these standards will have to be analyzed first in order to develop requirements for large scale deployments. At least the following standards and technical reports will need to be considered:

- ISO 21177-2019 enabling session security between ITS stations based on ITS certificates
- ETSI TR 103 630 prestandardization study on Facility layer security. In addition, ETSI TS 102 723-9 describes the interface between facility layer and security entity (standardization process for all involved standards is still ongoing)

2.4 EU CCMS Levels and timeline

A sub-group on Cooperative Intelligent Transport Systems (C-ITS) under the Commission Expert Group on Intelligent Transport Systems (E01941) has been established in 2020 to assist the Commission in working on the common EU-wide cybersecurity infrastructures and processes and to foster exchange of experience and good practice in the field of C-ITS.

3 levels of trust (hence compliance) have been defined to support deployment of Day 1 C-ITS services in Europe. They are described in the annex VIII of the CPOC Protocol [3].

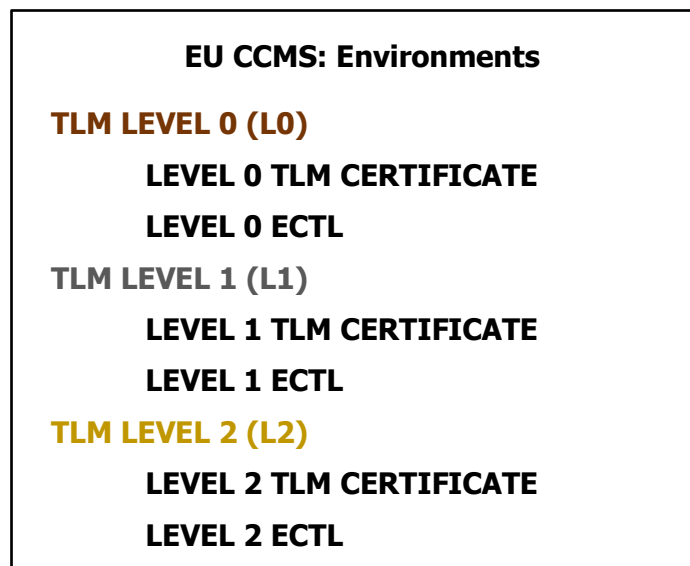


Figure 4: Different levels of security and trust as foreseen by the European Commission

- L0 (testing) is dedicated to competence-building towards standard & technical requirements conformity. It is made for limited in time basic tests (single stations or interoperability), or larger field tests and pilots. No CP/SP/CPOC compliance is required (hence no CPA approval). The correct format of the Root Certificate is however checked.
- L1 (Production) is a transition level during the ramp-up phase of C-ITS deployments. It is made for production environments. Full compliance to CP/SP/CPOC is required with specifically defined exceptions (cf. section 4 and section VIII.3.2 of [3]).
- L2 (Production) is for regular operations of large and distributed C-ITS networks. Full compliance to CP/SP/CPOC is required.

The following figure presents the ECTL levels timeline.

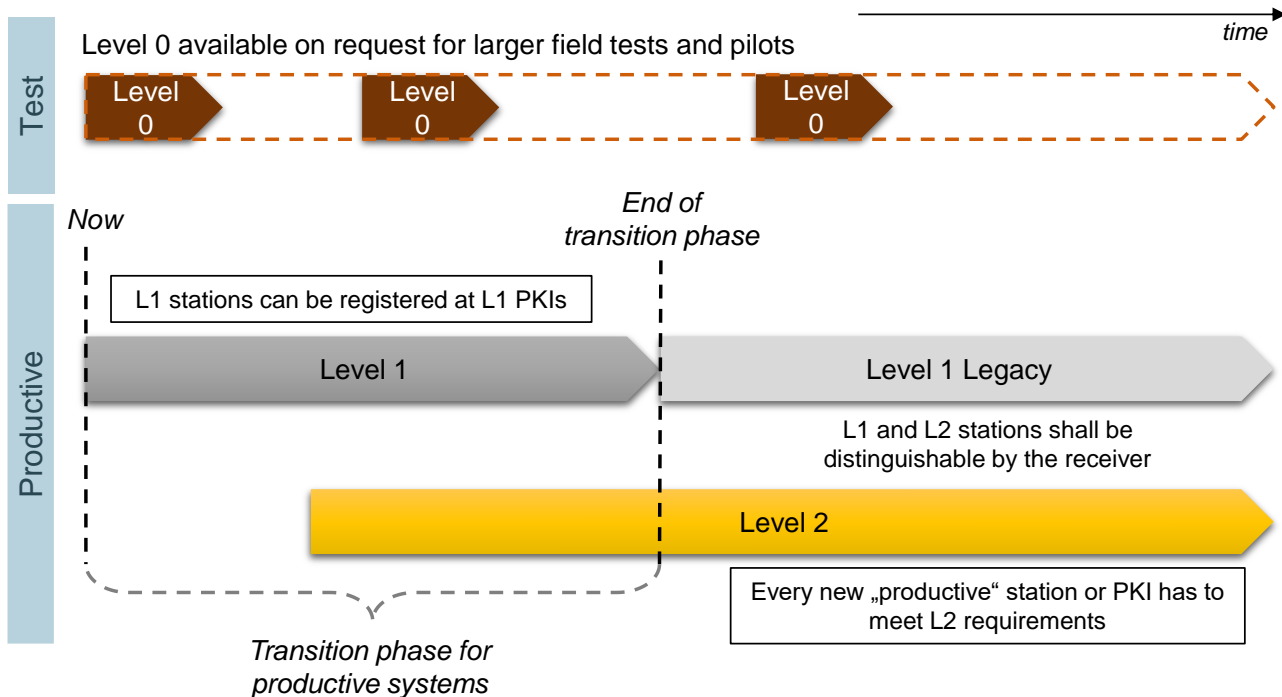


Figure 5: ECTL levels timeline

NOTES

- L1 stations may process L2 messages.
- L2 stations may process L1 messages (e.g. for information only), according to their individual risk analyses (considering that L1 compliance exceptions may imply a higher risk).
- Processing of messages across 2 levels (L1 & L2) requires the management of 2 ECTLs by the station.

2.5 Basic security aspects for C-ITS

Several security requirements are defined commonly for the whole group of “Day One C-ITS Services”, which can be summarized in the following way:

- 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 signed the certificate, is also included, so that the corresponding CA can also be validated. Following this so-called *chain of trust* up to the issuing Root CA and checking the currently valid ECTL – European Certificate Trust List, 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. The required level of trust is defined in the CP, including processes for all elements involved. In order to execute all actual verification steps, ensuring that messages are exchanged in a secure way, the information needs to be derived from the related standards. This work has been done by TF1 and the resulting (test) specification can be found in “C-ITS Security Requirements & Specifications”.

b. Data privacy:

One layer of privacy protection is defined in section 5.2.1 of the CP, by mandating technical and organisational separation of certain roles as 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. These potential privacy issues are one major difference regarding the various station types, 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 roadside stations or road operator vehicles or Central ITS stations signing and sending messages on their behalf, which is also reflected in the respective section 7.2.1 of the CP.

c. Data retention (affecting privacy and data protection regulation):

Data retention should be performed in accordance with the guidance provided in the CP/SP. Data retention periods might also be subject to local legislation (according to GDPR), and inconsistencies and repercussions should be investigated.

- For communications from roadside units and infrastructure ITS stations towards vehicles and road users, data privacy is not considered, since no personal data is being processed in I2V services.
- 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 operated by private users and the risk of being tracked as a user. This aspect is out of scope for C-Roads TF1, but the applied general principle for all V2I services 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 five minutes in order to achieve widest data anonymity.. More information on data protection and privacy can be obtained from C-Roads WG1, which is also conducting a series of privacy workshops and webinars.

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. For more information regarding the general principles, please refer to section 2.6, whereas detailed and use case specific SSP specifications can be found in the “C-ITS Service and Use Case Definitions” created by Task Force 2 within Working Group 2.

e. Revocation:

Regarding C-ITS stations, a revocation of single entities is currently not foreseen in the CP and by the current standards. 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 valid and therefore 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. According to the CP, preloading of ATs to individual C-ITS stations is limited to a maximum of 3 months, see section 7.2.1 of the CP.

This kind of passive revocation described above will be closely linked to the topic of misbehaviour detection. This concept is expected to be considered in updated standards and the future CP, it is still to be implemented in order to detect and report malfunctioning and/or malicious C-ITS stations.

Regarding PKI entities, a revocation of CA's is foreseen. If a single (Root)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 anymore. This requires a reliable, frequent distribution of the ECTL to all system operators using online access as appropriate, C-ITS stations have to check for updates of the ECTL at least weekly, see section 2.2 of the CP.

2.6 Concept of Service Specific Permissions (SSP)

One crucial aspect when using digital certificates to sign messages is the correct configuration of the respective permissions, stating that the certificate holder is actually entitled to deliver the specific C-ITS services as defined in C-Roads.

These permissions are to be checked against the actual type of message by the receiver upon reception of any message. If the respective permissions are not encoded in the certificate used to sign a specific message, the receiving station shall reject the message as invalid.

This concept is illustrated in the following figure: taking the warning message for roadworks as an example, which is functionally required for the depicted trailer, the SSP bit corresponding to the roadworks warning container in a DENM is set "1" (marked in red), meaning that the certificate holder is allowed to sign such a message. A receiving vehicle would receive the DENM containing the respective cause code and check the certificate for the permissions to (i) sign DENMs in general and (ii) sign specific roadworks warnings. (Other checks like validity times, issuing CA and others are to be checked as well, but not in the focus of this section. For more details, please refer to [5]). When validated correctly, the message can be processed.

On the right, there is an example given for a restricted permission – any undefined "future use" of the message type CAM shall not be allowed for the depicted trailer, therefore the respective bits are set to zero and such messages are to be rejected by receiving stations.

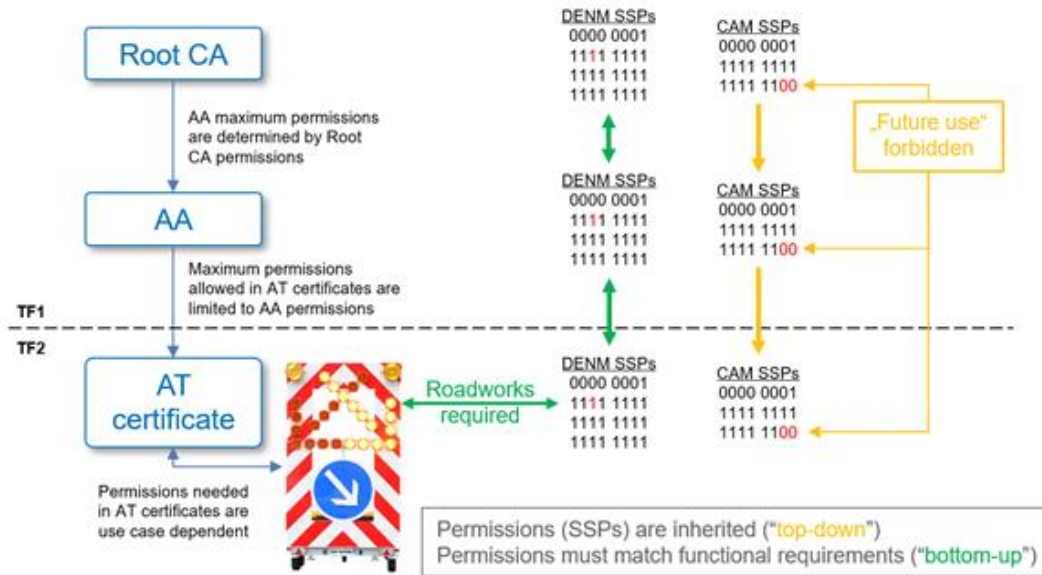


Figure 6: Concept of permissions in certificates - functionally required vs restricted SSPs

To give a few more examples illustrating the general concept:

Only emergency vehicles should be able to sign emergency vehicle warnings, while e.g. public transport vehicles should not. Road maintenance requires permissions different from those relevant for police cars, public transport priority should be restricted to respective stations and are different from signage applications, service related to traffic lights are to be kept separate from roadworks warnings and so on.

Another aspect shown on the previous figure is the relation to the PKI: Permissions to be issued in any AT certificate by an AA need to be in line with the permissions of the Root CA they belong to. The range of valid SSPs is always inherited in a "top-down" manner, and in the first place it is also part of the registration of a Root CA in the European trust model.

This setup of one or more Root CAs can be done in different ways:

- Either in one PKI branch comprising all types of SSPs relevant for the C-ITS services to be deployed, and a strict SSP management on subordinate layers.
- Strictly different PKI branches for different subsets of SSPs, e.g. police forces using a PKI separated from the PKI for road operators.
- Mixed setups, comprising elements of the two former approaches.

All of these setups can be deployed in line with [1], and a decision about the deployment model might depend on several factors. Since these aspects are more of an organisational nature, therefore an exchange between C-Roads Working Groups 1 and 2 has been initiated.

3 C-Roads tests & non-production pilots (L0)

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. Central-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.

The "Day One C-ITS services" as basically defined in the C-ITS Strategy [6] COM (2016) 766 and more detailed descriptions of TF2 as well as specifications elaborated in TF3, 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.

For the various C-Roads pilots starting from different levels of experience in C-ITS, some limitations and restricted requirements need to be considered as they are limited to non production operations. These are relevant for the governance level, since they have impact on Root CA operators and the involved stakeholders of the C-ITS network.

This chapter describes main elements for guaranteeing basic security for the communication in a C-ITS network, for **C-Roads tests and non production pilot phases**. This corresponds to the the level L0 defined by the European Comission (cf. section 2.4).

Additionally some aspects are listed in section 3.4 that, although not crucial for interoperability, are potential candidates for beneficial harmonisation across C-Roads pilots

3.1 Security elements and governance

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 ensure proper testing of specific security aspects, all functional requirements as well as putting first services into operation on public roads:

- For security specific tests, a dedicated TLM, CPOC and ECTL will be provided by the Czech C-Roads partners.
This testing environment will allow for analysis of verification steps and the detection/rejection of malformed and/or manipulated messages and certificates.
- For functional tests, the “Level 0” TLM, CPOC and ECTL as provided by the European Commission can be used.
This testing environment emulates a “normal operation” from a security point of view and serves the test cases relevant for the various services, use cases and scenarios as specified by TF2 and TF3.

The provision of certificates and certificate trust lists needs to be ensured by the respective PKI operator for the (potentially various) C-ITS station operators.

In terms of governance of the central entities, different cases need to be distinguished, depending on the intended use and the level of the respective system:

- The central entities for security tests operated by a Czech PKI provider company require no specific governance, TF1 and the central elements group within TF1 will take care of any required agreements.
The class of test cases is limited to lab situations and “on the table” test. The actual service, use case and scenario is not of utmost importance, the main focus is on correct detection of invalid signatures, outdated certificates, revoked certificates, outdated ECTLs and the like. Specific services may be tested only to check for (in)correct use of permissions within the certificates.
Invalid signatures and certificates on TLM, RCA, EA, AA and C-ITS Station level are to be expected in order to test if security controls are working as intended.
- The central entities for functional tests (“Level 0”) are governed by the European Commission. This governance comprises management of the CP and SP, authorization of PKI systems, updates and provision of the ECTL in a secure way.

The classes of test cases that are covered span from lab tests and “on the table” tests to on-road tests and potentially more complex test environments, dependent on the service, use case and scenario.

Valid certificates, signatures and ECTLs according to the standards, described processes and C-Roads specifications are to be expected at all times from all partners in order to test C-ITS services if they are working as intended.

3.2 PKI operation

For Pilots activities (beyond testing activities) running on Level 0, 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. 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.

Within such an approach the following is a list of examples that might not be in place for the L0 C-Roads pilot phase :

- 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 section 5.2.4.
- Personnel controls according to CP section 5.3 may not be implemented completely.
- Audit logging procedures according to CP section 5.4 may not be implemented completely.
- Records archival according to CP 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 1.5, section 4.1.2.1 and chapter 8 of the CP 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 1.5 and 4.1.2.3 of the CP.
- The operators may request a self-assessment of the ITS station manufacturer and the EA can request a self-assessment of the operator that registers the station.

Note: since May 2020, the EU Commission has open the L0 EU Root CA service available for any C-ITS actor.

3.3 Security provisions of C-Roads pilots

The following table provides an overview of the different C-Roads member states in terms of (planned) PKI operation.

Table 2: PKI systems (providing certificates based on ETSI TS 103 097) foreseen by the Member States and C-Roads pilots

C-Roads Member State	TLM	CPOC	Root CA	EA	AA	ITS station types	Pilot elements	Operational
Austria	EU	EU	Contract/TBD	Contract/TBD	Contract/TBD	ALL	TBD	TBD
Belgium (Flanders and Wallonia)	EU	EU	TBD	TBD	TBD	TBD		TBD
Czech Republic	EU	EU	National	National	National	ALL		2021
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
Greece	EU	EU						
Hungary	EU	EU	TBD	TBD	TBD	TBD	TBD	TBD
Ireland	EU	EU	EU RCA	EU RCA	EU RCA	ALL	TBD	TBD
Italy	EU	EU	Contract/EU	Contract/EU	Contract/EU	ALL		TBD
Netherlands	EU	EU	TBD	TBD	TBD	TBD	TBD	TBD
Norway	EU	EU	TBD	TBD	TBD	TBD		TBD
Portugal	EU	EU	TBD	TBD	TBD	TBD	TBD	TBD
Slovenia	EU	EU	National	TBD	TBD	TBD	TBD	TBD
Spain	EU	EU	National	National	National	All		TBD
Sweden	EU	EU	TBD	TBD	TBD	TBD		TBD
UK	EU	EU	TBD	TBD	TBD	TBD	TBD	TBD
EC DG JRC	EU	EU	EU	EU	EU	All	TBD	2020 TBC

For this table of the security provisions the column “ITS station types” may comprise Roadside ITS Stations – R-ITS-S, Vehicle ITS-Stations – V-ITS-S, Vro-ITS-S (for Road Operator Vehicles), as well as Central ITS Stations.

In some C-Roads pilots the security preparations are executed for all C-ITS Stations.

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.

In addition to public authorities 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 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 roadside ITS Stations involved directly from project partners. The Escrypt Pilot PKI for C-ROADS Pilot Austria is used in 2020 (and 2021). Usage of European Root-CA for the operational Austrian national C-ITS System currently being tendered could be envisioned.

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 NordicWay3 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trust 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 NordicWay3 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trust 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: For the piloting phase of C-Roads, authorities (Root CA, EAs and AAs) are offered by a Hungarian PKI provider for R-ITS-S and V-ITS-S stations. A feasibility study for longer term national deployments is planned in the future, but no decision has been taken yet.
9. Ireland: EU PKI for RCA, EA and AA during the pilot phase. Operational phase TBD.
10. Italy: C-Roads Italy 1 uses PKI by Contract and C-Roads Italy 2 will use European PKI (level 0) for the pilot..
11. 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.
12. Norway: The NordicWay3 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trust 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.
13. 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.
14. Slovenia: No decision taken yet.
15. 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.
16. Sweden: The NordicWay3 pilots, to which the Nordic countries participate, will use cellular communications. The backend will be in the EU Trust 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.
17. United Kingdom: The current pilot implementation is used for the A2M2 CVC project using a security solution that has been aligned with InterCor partners. A decision regarding the operational phase beyond the InterCor project has not been taken yet.

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 and then decide for the next steps, especially for the R-ITS-S and the central elements of the PKI.

3.4 Potential areas of cooperation and harmonization

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.
 - o EA and AA registration at the Root CA in order to request a Sub-CA certificate.
 - o Termination and transfer of EA and AA certificate at a specific Root CA.
 - o Revocation of EA or AA certificate at a specific Root CA.
 - o Registration including authentication of end-entity subscriber organizations (manufacturer / operator) according to the CP 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 an 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 Certificate Policy Authority (CPA) according to the CP.
 - o Root CA registration at the CPA 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.
 - o Termination of Root CA registration at the CPA in order to let the existing RCA certificate expire without an update of the ECTL.
 - o 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.
 - o Request for re-keying or key changeover of the Root CA certificate at the CPA in order to update the ECTL by the TLM and renew the ECTL at the CPOC.

4 C-Roads pilots regular operation (L1)

For operational units, the “Level 1” TLM, CPOC and ECTL as provided by the European Commission can be used if put into L1 production before end of L1 transition phase. This environment is not used for testing, but for production operation of the various services, use cases and scenarios as specified by TF2 and TF3.

These systems are to be used in actual operation on the road, covering various services, use cases and scenarios. Valid certificates, signatures and ECTLs according to the standards, described processes and C-Roads specifications as well as service implementations that are working as intended and producing correct messages are to be expected at all times in order to guarantee a smooth operation.

These central entities for operational units are governed by a CPA consisting of the European Commission supported by an expert group, see section 2.4. This governance comprises management of the CP and SP, authorization of PKI systems, updates and provision of the ECTL in a secure way.

In contrast to previous discussions and assumptions being made throughout 2019, a separate governance role comparable to a CPA will not be needed within C-Roads anymore.

As defined by the European Commission, access to L1 requires full compliance to the regulation with defined exceptions. C-Roads pilots going to regular operation are required to comply with these requirements.

The exceptions defined in the CPOC Protocol [3] are summarized here.

For C-ITS stations

According to Annex VIII, table 17 of [3], the following exceptions from the CP are acceptable for C-ITS stations:

- Common Criteria certification can be replaced by a positive evaluation report from a SOG-IS recognized test lab, ensuring protection against an attacker with basic attack potential (CC Part 3 Level 1 evaluation).
- Validation of a TLM certificate can be done centrally prior to a secure transfer to the station (no CC certification required for this alternative process).
- Enrolment and Authorization protocols can comply with versions of ETSI TS 102 941 newer than v1.4.1.

Important: exceptions on L1 Legacy remain the same for stations of types/models placed on the market before the end of the transition phase.

For C-ITS station's crypto modules

According to Annex VIII, table 17 of [3], Common Criteria certification can be replaced for crypto modules only either:

- By a CC EAL 4 certified hardware & firmware from an ISO 27001 certified manufacturer (*same exception for stations of types/models placed on the market before the end of the transition phase*)

Or

- An ongoing CC certification process started (attested every 6 months by the contracted accredited lab) to be finished before the end of the transition phase (*no exception on L1 Legacy after the end of the transition phase*)

For C-ITS station operators

- If an ISMS according to ISO 27001 is not available, a comparable security management processes shall be operated (e.g. CSMS)
- Compliance to the Security Policy can be declared through a self-assessment report

Important: no exceptions on L1 Legacy after the end of the transition phase assuming that the Security Policy will reference additional security management systems (e.g. CSMS according to UNECE R155).

For PKI operators

The insertion in the L1 ECTL requires the Root CA to be successfully audited according to the CP. If the audit can not be performed, the CPA may grant access to L1 if the following elements are fulfilled:

- The PKI is serving well-identified European production C-ITS services
- The PKI operator presents relevant certificates for the C-ITS PKI service (ISO 27001 and/or applicable CP audit report covering all part of the service, e.g. involved infrastructure, key management procedures and service operation processes & team)
- The PKI operator demonstrates service security to guarantee that valid certificates cannot be delivered to unauthorized entities:
 - Key management is compliant to the CP with an accredited auditor report (naming of certificates may not comply with the CPOC rules)
 - A process is defined to authenticate and authorize organisations/subscribers including the verification of stations' compliance (cf. exceptions for stations)

Important: no exceptions on L1 Legacy after the end of the transition phase.

References

- [1] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). EU C-ITS Certificate Policy - Release 3.0 – May 2024
https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf
- [2] Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). EU C-ITS Security Policy - Release 3.0 September 2023.
https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0_20230916.pdf
- [3] C-ITS Point of Contact (CPOC) Protocol in the EU C-ITS Security Credential Management System (EU CCMS).
https://cpoc.jrc.ec.europa.eu/data/documents/e01941_CPOC_Protocol_v3.0_20240206.pdf
- [4] Protection Profile for a Roadside ITS Station Gateway. Version 1.0. Certification-ID: BSI-CC-PP-0122
- [5] “C-ITS Security Requirements & Specifications” v2.2.0
- [6] 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
- [7] ETSI TS 103 301: Facilities layer protocols and communication requirements for infrastructure services;
- [8] ETSI TS 103 097 V1.4.1 - Security header and certificate formats
- [9] ETSI TS 102 941 V1.4.1 - Trust and Privacy Management
- [10] ETSI EN 302 636-4-1 V1.4.1 - Vehicular Communications; GeoNetworking