C-ITS Security & Governance

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

Version 1.9

12th May 2020

Co-financed by the European Union
Connecting Europe Facility

Table of Content

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	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
0.83	15.02.2018	Update chapter 3, including statements from C-Roads members	Draft
0.85		Updated content in various chapters	Draft
0.90	March 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 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	August 2019	1.6 remarks considered, annex B updated	Draft
1.8	May 2020	Transfer of annexes A & B to TF1 Security requirements document	Draft
1.9	May 2020	Complete document overhaul and restructuring: one overview and governance part, separate technical specifications and requirements	Draft

List of used abbreviations

AA	Authorization Authority
AT	Authorization Ticket
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
EC	Enrolment Certificate
EE	End Entity
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 – Security Aspects
TLM	Trust List Manager
TLS	Transport Layer Security - Internet Engineering Task Force (IETF) RFC 8446
WG2	Working Group 2

Scope of this 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 pilots and 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 updated version of this report 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.

Introduction

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, Within C-Roads, TF1 as the security task force of Working Group 2, 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 have initially been based on two documents that the EU C-ITS Platform had produced in 2017:

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

In the course of 2019, the core ideas of these documents have been included in the proposed Delegated Regulation on C-ITS.

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 [3]

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, governance aspects as well as organisational requirements in chapter 2 are the core elements of this report. Chapter 3 completes this report with a set of recommendations.

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

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 TF1 is also creating a “Protection Profile” 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.

1 A secure European C-ITS System

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, main focus is therefore on C-ITS services involving and/or relating to road infrastructure (e.g. hazardous locations, signage applications, road condition).

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, 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.

1.1 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, see section 2.2.

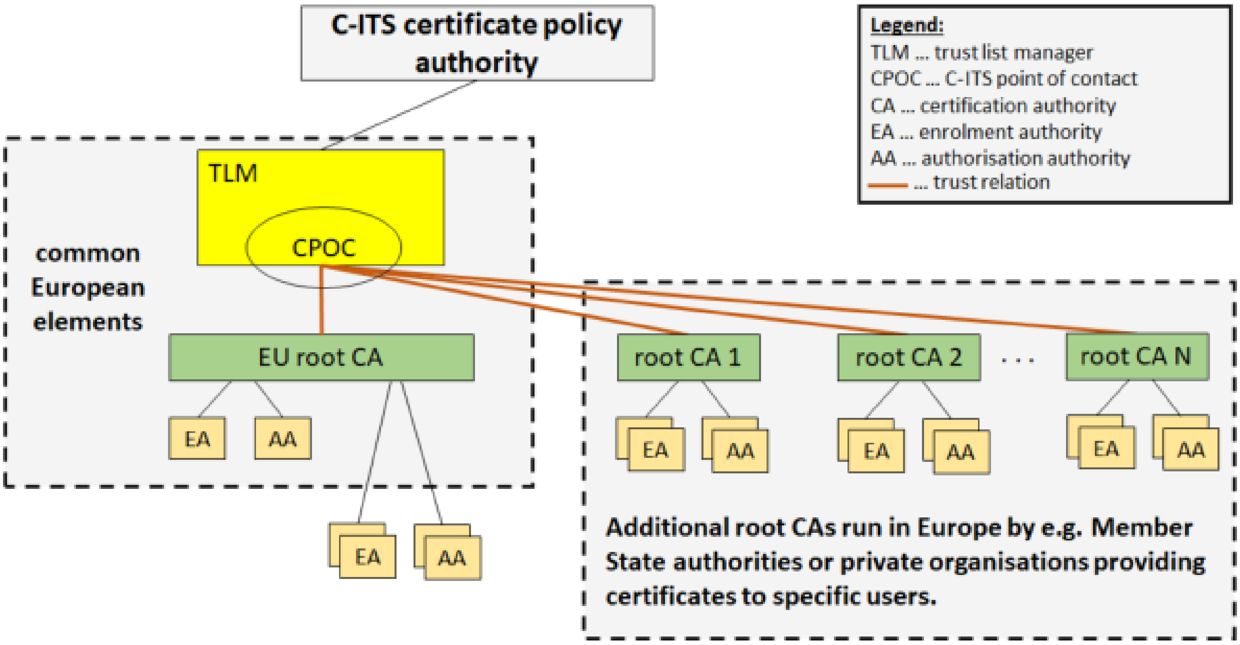

C-ITS certificate policy authority
Legend:
TLM ... trust list manager
CPOC ... C-ITS point of contact
CA ... certification authority
EA ... enrolment authority
AA ... authorisation authority
... trust relation
TLM
CPOC
common European elements
EU root CA
EA
AA
EA
AA
root CA 1
root CA 2
. . .
root CA 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 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 (“rootCA 1” to “rootCA 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 2.2.

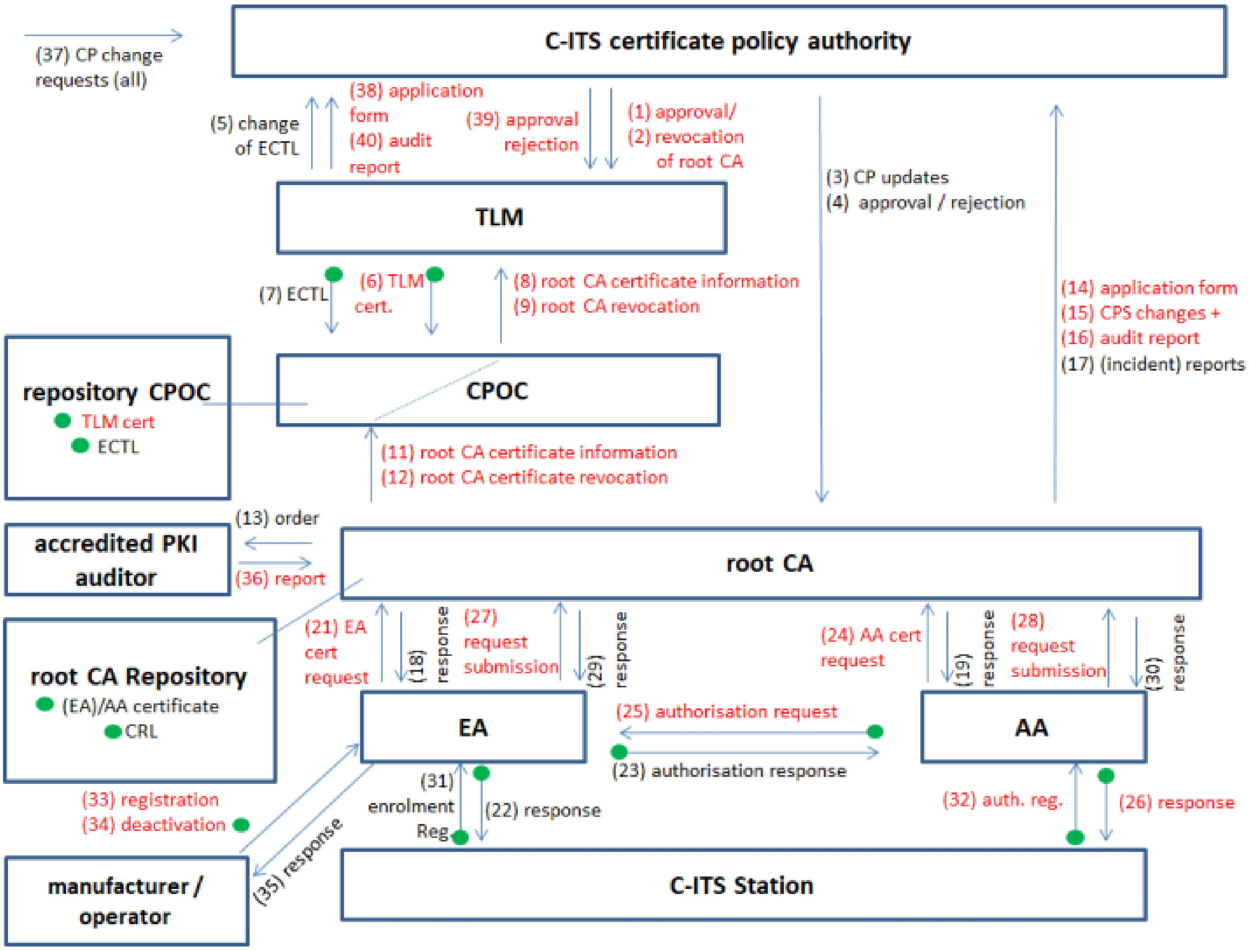


Figure 2: C-ITS Trust Model Information Flows, see section 1.3.1 of the CP [1]

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 be 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.

1.2 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. A full list of TF1 standards is provided in [3].

Table 1: Main Interoperability Requirements

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

** This report is based on the latest version of the standard. The Assumption is made here that the CPA will update the current reference in the CP to the more recent standards, which had not been available at the time of the CP's publication.*

1.3 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 will most likely include evolving communication technologies like C-V2X or 5G-New Radio in the future.
> - 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 in the proposed Delegated Regulation on C-ITS 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), as indicated in a schematic representation in Figure 3.

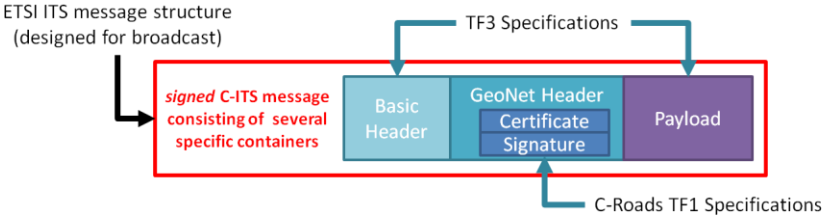

ETSI ITS message structure
(designed for broadcast)
TF3 Specifications
signed C-ITS message consisting of several specific containers
Basic Header
GeoNet Header
Certificate
Signature
Payload
C-Roads TF1 Specifications

Figure 3: (Simplified) C-ITS message structure - security is part of the GeoNet-layer

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 4.

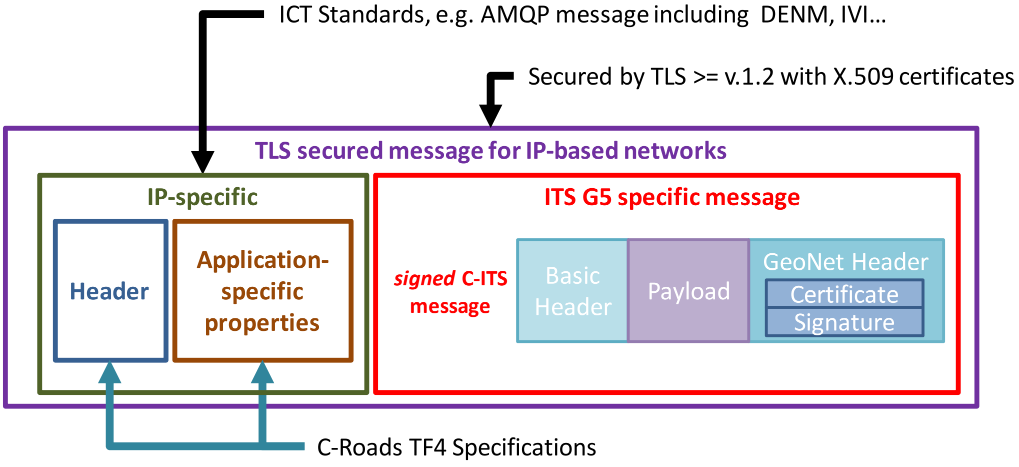

ICT Standards, e.g. AMQP message including DENM, IVI...
Secured by TLS >= v.1.2 with X.509 certificates
TLS secured message for IP-based networks
IP-specific
Header
Application-specific properties
ITS G5 specific message
signed C-ITS message
Basic Header
Payload
GeoNet Header
Certificate
Signature
C-Roads TF4 Specifications

Figure 4: 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.

2 PKI operation and governance for C-Roads tests

This chapter describes main elements for guaranteeing basic security for the communication in a C-ITS network, during the lifetime of C-Roads and beyond.

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.

The “Day One C-ITS services” as basically defined in the C-ITS Strategy [4] 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.

2.1 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:

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 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, 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. This upper limit is defined in section 1.6.2.2, table 5 in the CP. 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. The detailed SSP specifications can be found in the “C-ITS Security Requirements & Specifications”.

e. Revocation:
   Revocation of single C-ITS stations is currently 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 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 section7.2.1 of the CP.

   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.

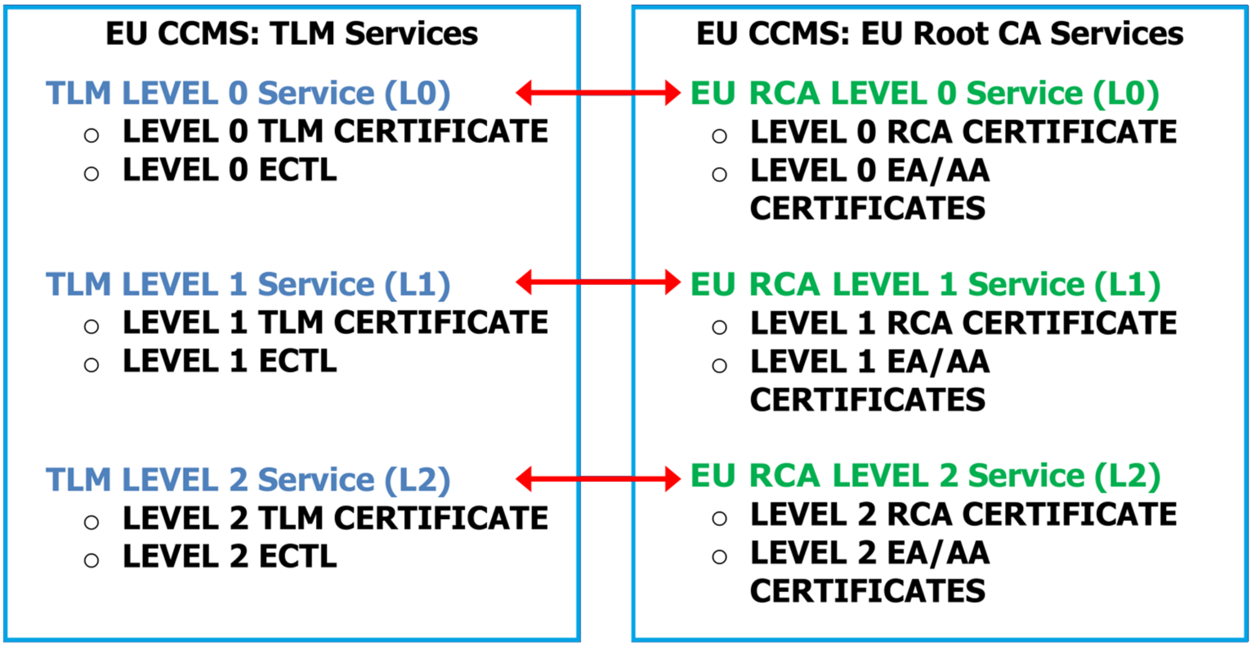
Co-financed by the European Union
Connecting Europe Facility

2.2 Security compliance levels

According to the security requirements from the European CP, Common Criteria (ISO/IEC 15408) and the international SOG-IS agreement provides the security framework to be used for the assessment/certification of all C-ITS stations. In order to prepare road operators and authorities for regular operation, TF1 has intensified the efforts to create a “Protection Profile” according to Common Criteria, ISO/IEC 15408 until the end of 2020.

The availability of certified C-ITS stations is covering the CP requirement in terms of logical and physical hardening of end entities. Another aspect to be covered is the secure operation of the required PKI systems. Besides technical requirements, e.g. using certified hardware, certificate validity times etc., also organisational requirements need to be met, e.g. access restrictions, redundant data centers etc., and the whole PKI operation needs to be audited.

Both factors play an important role when it comes to the definition of the various trust levels that are depicted Figure 5. Technical aspects are only one aspect to be addresses, the governance also needs to be elaborated and agreed on. For that purpose, the European Commission is planning to establish the CPA – Certificate Policy Authority and has recently launched a “call for experts”, which will then form a sub-group to the so-called ITS Committee and discuss and advise on CP related matters



EU CCMS: TLM Services

TLM LEVEL 0 Service (L0)
- LEVEL 0 TLM CERTIFICATE
- LEVEL 0 ECTL

TLM LEVEL 1 Service (L1)
- LEVEL 1 TLM CERTIFICATE
- LEVEL 1 ECTL

TLM LEVEL 2 Service (L2)
- LEVEL 2 TLM CERTIFICATE
- LEVEL 2 ECTL

EU CCMS: EU Root CA Services

EU RCA LEVEL 0 Service (L0)
- LEVEL 0 RCA CERTIFICATE
- LEVEL 0 EA/AA CERTIFICATES

EU RCA LEVEL 1 Service (L1)
- LEVEL 1 RCA CERTIFICATE
- LEVEL 1 EA/AA CERTIFICATES

EU RCA LEVEL 2 Service (L2)
- LEVEL 2 RCA CERTIFICATE
- LEVEL 2 EA/AA CERTIFICATES

Figure 5: Different levels of security and trust as foreseen by the European Commission

- For first pilot activities and the initial setup phase (the so-called “Level 0”), all types of (uncertified) C-ITS stations, even without any specific crypto-hardware (HSM – Hardware Security Module), may be used.
  As of May 2020, a separate TLM/CPOC environment is provided by the European Commission for development and testing, as well as corresponding RootCA, EA and AA on a European level.
  This test level is expected to be operated continuously. In the future, all potential changes and future developments will always require testing before updating operational systems in a coordinated way.

- Self-assessments of operators of C-ITS stations may only be acceptable during the first phase of operation, up to the so-called “Level 1”. Stations are expected to meet certain requirements, e.g. use of a dedicated HSM, even though a Common Criteria certification of the C-ITS stations and/or audited PKI systems might still be missing.
  As of May 2020, a separate TLM/CPOC environment as well as corresponding RootCA, EA and AA on a European level are expected to be provided by the European Commission for first operational deployments by Q3/2020.
  This level is expected to be operated only as an intermediate solution. As of May 2020, there are no fully CP compliant stations and PKI systems in operation that have already been audited and certified, still there is the need to separate first operational units from tests and development environments.
- Regular operation with full compliance to all CP requirements, including certification of C-ITS stations and audits of the PKI systems, will be summarized as the so-called “Level 2”.
  As of May 2020, a separate TLM/CPOC environment as well as corresponding RootCA, EA and AA on a European level are expected to be provided by the European Commission for continued regular operation from Q4/2020 on.

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 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 (i.e. Teska labs).
  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.
- For first operational units, the “Level 1” TLM, CPOC and ECTL as provided by the European Commission can be used.
  This environment is not used for testing, but for operation of the various services, use cases and scenarios as specified by TF2 and TF3.

2.4 C-Roads Pilots and test - operation and governance

Depending on the intended use of C-ITS stations, it is within the responsibility of the PKI operators to register in the according trust domain for security testing, functional testing or operation as outlined in section 2.3, and to ensure the required compliance according to the desired level.

In any case, 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 Teska Labs 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.
- The central entities for operational units ("Level 1") are governed by a CPA consisting of the European Commission supported by an expert group, see section 2.2. This governance comprises management of the CP and SP, authorization of PKI systems, updates and provision of the ECTL in a secure way.
  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.

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.

2.5 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 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	Contract	Contract	ALL	SSP´s	Open, decision by 2019
Belgium (Flanders and Wallonia)	EU	EU	TBD	TBD	TBD	TBD		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	TBD	TBD	TBD	TBD	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	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 C-ITS stations are divided into Roadside ITS Stations – R-ITS-S and Vehicle ITS-Stations – V-ITS-S and Vro-ITS-S (for Road Operator Vehicles), 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 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. 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 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 NordicWay2 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

Co-financed by the European Union
Connecting Europe Facility

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, national authorities (Root CA, EAs and AAs) planned to be set up for the Hungarian pilot sites, a feasibility study is planned in Q1-Q2/2019, but no decision has been 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 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.
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 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.
16. 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 Recommendations for C-Roads Pilots

For the various C-Roads pilots starting from different levels of experience in C-ITS, some limitations and restricted requirements need to be considered. These are relevant for the governance level, since they have impact on root CA operators and the involved stakeholders of the C-ITS network. Therefore, the recommendations in section 3.1 are made with respect to how the C-Roads pilots may be assessed against the SP and CP and are dependent on the intended “level of trust” as outlined in section 2.2.

Additionally some aspects are listed in section 3.2 that, although not crucial for interoperability, are potential candidates for beneficial harmonisation across C-Roads pilots

It can be expected that, for large-scale deployments and regular operation beyond 2020, most of these aspects will be resolved in the future.

3.1 PKI operation within C-Roads Pilots (until 2020/2021)

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 need to be verified by an accredited PKI auditor, see section 2.2. A full audit is not recommended for initial C-Roads deployments and tests (comprising “Level 0” and potentially “Level 1” systems), since a full compliance is virtually impossible without certified hardware and C-ITS stations in use a(s of May 2020).

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. 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 C-Roads 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 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 1.7.5, 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 1.7.5 and 4.1.2.3 of the CP.
- 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.

3.2 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:

- THIS LIST IS TO BE UPDATED
- Processes under control of the Root CA according to the CP.
    - 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 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.

References

[1]: Certificate Policy (ANNEX 3 to the Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems) – March 2019

[2]: Security Policy (ANNEX 4 to the Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems) – March 2019

[3]: C_Roads_WG2_TForce1_Reference_Documentation_List_v1.0_01042018

[4]: 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

List of Figure and Tables

Co-financed by the European Union
Connecting Europe Facility