Guide for C-ITS standards conformity

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). The Consortium members represent worldwide major vehicle manufactures, equipment suppliers and research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium and its members work in close cooperation with the European and international standardisation organisations.

Disclaimer

Document information

Number:	2310	**Version:**	n.a	**Date:**	2024-07-12
Title:	White Paper on self-certification and testing			**Document Type:**	WP
Part of release	1.6.6				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last release

Date	Changes	Edited by	Approved
2024-07-12	Initial release	Release Management	Steering Committee

Table 2: Changes since last release

Table of contents

List of tables

List of figures

Abbreviations

Commonly used abbreviations are defined in the C2C-CC Glossary, see [RD-1][RD-3]. Additionally used abbreviations are defined in the following list.

Abbreviation	Description
IUT	Implementation under Test
CPOC	C-ITS Point of Contact
ECTL	European Certificate Trust Lists
VSP	Vehicle C-ITS Station Profile
RCA	Root Certificate Authority
EA	Enrolment Authority
CC	Common Criteria
CSMS	Automotive Cybersecurity Management System
ISMS	Information Security Management System
CPA	Certificate Policy Authority

1 Introduction

C-ITS forms an ecosystem consisting of numerous, diverse C-ITS-Ss provided by various suppliers and vendors. These C-ITS-Ss share data, necessitating a level of trust in the information shared by others. This becomes particularly crucial when the C-ITS-Ss are operated or introduced to the market by different entities.

Addressing this issue involves a two-fold approach. Firstly, interoperability requirements for the C-ITS-Ss are established to ensure a common 'language,' facilitating effective communication. Secondly, this issue is managed through the implementation of a Public Key Infrastructure (PKI). In this system, each C-ITS-S possesses a unique set of certificates - public and private key pairs also known as Authorization Tickets (ATs). These are used to sign their messages.

The message's application payload is shared along with its signature with other C-ITS-Ss. This allows the receiving C-ITS-Ss to verify the signature of received messages. Through this process of signature verification, a receiver can validate not only the integrity of a message, but also confirm that it was signed by a trusted entity.

These Authorization Tickets (ATs) are indirectly issued by Root Certificate Authorities (RCA) via an intermediate entity known as the Authorization Authority (AA). Please refer to chapters 1 and 2 of [RD-3] for a comprehensive overview of the C-ITS security architecture. Within the C-ITS ecosystem, multiple RCAs can exist, each potentially operated by different entities. To establish trust among these various RCAs, a PKI necessitates a collectively accepted set of trust anchors - these are the trusted RCAs. This group of trusted anchors is provided through the European Certificate Trust List (ECTL), which is managed and maintained by the EU.

The EU has established a "C-ITS Point of Contact" (CPOC) as the entry point for an RCA desiring inclusion in the ECTL. The standard procedure for becoming part of the ECTL is detailed in the CPOC protocol (refer to [RD-3]). This process incorporates additional specifications pertinent to particular aspects of C-ITS and outlines the necessary input items for initiation. These items form the basis for ensuring that deployed and operated C-ITS-Ss achieve a minimum level of maturity. The maturity level must be demonstrated in various ways, contingent on the referenced specifications. To ensure interoperability among C-ITS-Ss, the CPOC protocol mandates a self-declaration of conformity to a defined set of standards and profiles. This self-declaration is a procedure where the manufacturer of a C-ITS-S asserts, under their own responsibility, full implementation of all relevant requirements. While this declaration does not necessarily need validation by an independent third party (e.g., a conformity assessment body), it can be verified if desired.

While the CPOC protocol provides a general framework for integrating into the C-ITS trust domain, certain details remain open and require further discussion. As such, the first part of this document should be considered a simplified abstraction of the CPOC protocol process aiming to address unresolved issues and questions.

The second part of this document pertains to the testing efforts required for the self-declaration of conformity. Although a comprehensive set of requirements exists currently, we lack a complete set of test cases. Manufacturers are responsible for developing these tests. This document offers guidelines regarding the necessary scope for testing to ensure more comparable results across different manufacturers.

2 Process for self-testing and self-declaration of conformity

2.1 Self-testing and Self-declaration of conformity to standards and specifications

As introduced in the previous chapter, C-ITS is a rapidly evolving field, which necessitates strict adherence to compliance protocols for all stakeholders. One of the key aspects of compliance assessment according to the CPOC protocol involves self-declaration for conformity to a set of relevant interoperability specifications and standards.

The Car 2 Car Communication Consortium Basic System Profile (for vehicle C-ITS stations), as well as the C-ROADS Harmonised C-ITS specifications (for road side C-ITS stations and road operator vehicles) build the basis for functional interoperability and hence are an anchor point for functional conformity. Among other relevant standards, these detailed specifications outline pivotal guidelines that must be addressed during self-declaration, thereby ensuring seamless intercommunication and efficient operation within the C-ITS framework. Standards that these specifications refer to shall be part of the conformity declaration, too.

Another essential resource in this context is the ETSI TR 101 607 list of standards. Despite not all listed standards being explicitly relevant for interoperability, it acts as a guide, supporting the identification of standards that need to be considered.

However, simply adhering to some version of these standards is not enough. It is equally important that the versions of these standards indicated in the self-declaration are consistent with each other and align with those stated in the supported profile. Discrepancies can lead to operational inefficiencies, impairing system performance, and potentially jeopardizing road safety in the futures. It is the responsibility of the declaring organization to ensure this consistency of the indicated versions.

In declaring conformity with the relevant standards as mentioned above, the declaring organization assumes responsibility to ensure this conformity. This applies not only one-time on initial testing and enrolment, but also over time. This is relevant for updates over the air and also C-ITS Services that are reconfigured over time (e.g. a roadworks trailer assuming different use cases on different days). While this version of the document provides some first guidelines to address questions like these, some questions remain open and will be addressed in future versions (see chapter 4.1).

2.2 Becoming listed on the European Certificate Trust List (ECTL)

The ECTL was briefly described in chapter 1. With the CPOC protocol, the EU has established a guard for accessing the ECTL to ensure that all C-ITS-Ss in the trust domain fulfil the same set of minimum requirements. These requirements are the key to enable interoperable and harmonized C-ITS in Europe, see Figure 1.

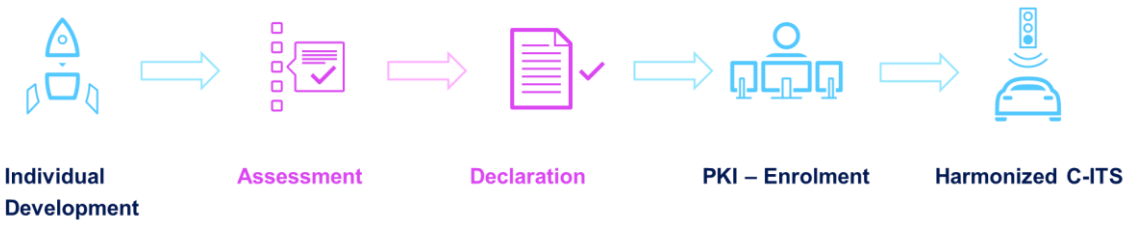

Figure 1: General process from development to operation of a C-ITS-S.

At this point it is also worth to note that the ECTL contains only trusted RCA certificates. This list does not represent a collection of “permitted C-ITS operators”. In some cases, the RCA certificates can be linked directly to an operator (if the operator of the C-ITS-Ss is also a PKI operator), but in other cases, an RCA certificate can represent a PKI operator only, who offers a service to C-ITS Station operators for “becoming part of the C-ITS trust domain”. These PKI operators take the burden of operating and maintaining RCA certificates. The PKI operators in turn provide access to EAs and AAs, which are issued by their trusted RCA certificate, to interested C-ITS participants under certain conditions, but they also “hide” the real-world C-ITS-S operators that uses the ECTL.

Before diving deeper into “how to become a part of the ECTL”, the three existing levels / instances of the ECTL should be introduced. Each of the instances is designed for a different purpose and there are different access criteria for each of the instances.

- L0: “*shall be used for competence-building towards C-ITS security standards and technical requirements conformity of C-ITS station and PKI implementations.*” ([RD-3], section VIII.2.2) In other words, this instance is designed for testing of existing and future C-ITS services and applications.
- L1: “*shall be used to align C-ITS implementation to the CP/SP and CPOC protocol processes and approach full compliance.*” ([RD-3], section VIII.2.3) This instance is used in a transition phase where the early day-1 C-ITS-Ss do not fulfil all requirements, but an operation of the C-ITS-Ss shall become possible. Therefore, the trust domain for these C-ITS-Ss has to be separated from the trust domain of L0. This instance might be terminated in the future and the deployed C-ITS-Ss might have to move to L2.
- L2: “*shall be used for certified production operation of C-ITS station and PKI implementations*”. ([RD-3], section VIII.2.4) This instance is the “productive” version that is used by all the C-ITS-Ss placed on the market to trust each other.

These 3 levels and their description indicate already that different access criteria are necessary with increasing severity of the requirements. While L0 can accept a set of deviations from the requirements to access the ECTL, L2 cannot. L1 is placed in between L0 and L2 and allows only a well-defined number of exceptions from the access criteria of L2.

Furthermore, it shall be noted that there are different “entry points” to the ECTL and the C-ITS trust domain:

- C-ITS Station manufacturers that operate their own PKI have to add their RCA certificate directly to the ECTL via the CPOC. Such constructs can be considered as a closed eco-system because they probably will not add C-ITS-Ss to their PKI that

exist outside of their company's scope (e.g. operated by somebody else). They have full control over their PKI and their usage. As they are "not open for the public", they are a less interesting case to study in this WhitePaper.

- A PKI operator has to add its own RCA certificate to the ECTL. This initial process is their own business. After being listed on the ECTL, the PKI operator will offer a service to the public where other companies can use an EA and AA that is provided by the PKI operator. These PKI operators are another entry point for Station operators, especially for small and medium organisations and a relevant to study in this WhitePaper. These C-ITS Station operators (who are in fact the customers of the PKI operator) would use the EA and AA to provision ATs to their C-ITS-Ss if the C-ITS-Ss fulfil a set of requirements.

In the following, only the second case is studied, where a Station operator wants to take part in the C-ITS trust domain via a PKI operator. The full list of access criteria can be found in [RD-3], section VIII.3. It must be emphasised that these requirements have to be fulfilled as well by Station manufacturers that operate their own PKI.

Note: section VIII.3 of [RD-3] lists all requirements to cover also for cases where an own PKI or a subset (EA / AA under foreign root certificate) shall be operated.

2.2.1 Accessing L0

The full list of details and explanations can be found in [RD-3], section VIII.3, Table 15.

The criteria to fulfil that are required for a C-ITS-S to access the EA or AA in an L0 environment are:

- *Legal existence of station operator*.
  The legal existence of a station operator can be proven by submitting an official company registry document to the PKI service provider, which contains the official data of the station operator company (e.g. name of the company, address, company registration number)

- *Self-declaration of standards conformity*
  This means that full conformity with all relevant standards for interoperability and respective system profiles of stations (self-declaration) is achieved, i.e. that full conformity to either the C2C-CC Profile in Release 1.6.0 (or newer) or to the C-Roads Release 2.0 (or newer) is declared.
  The CPOC Protocol states that at Level 0, there might be exceptions from conformity to standards and profiles, but they are limited to "*exceptions from conformity to standards and profiles can be made on Level 0 only to allow testing of new message types*" ([RD-3], table 15). So, even at Level 0, C-ITS-Ss shall be, in principle, fully conformant to relevant standards and profiles, but exceptions can be made by Station Operators & Manufacturers in their self-declaration of conformity.

- No CP/SP audit and certification is needed for C-ITS stations to access the L0 Environment.

2.2.2 Accessing L1

As mentioned, the L1 instance accepts certain exceptions from the criteria of the L2 instance (see clause 2.2.3). All of these exceptions are limited to the "*Certification of compliance to the Security Policy*". No exception for the "*Self-declaration of standards conformity*" have been defined. Depending on the applicable exceptions for a specific type of C-ITS-S of a specific manufacturer / operator, alternative or further documents have to be provided. Additional details and explanations can be found in [RD-3], section VIII.3, Table 16T.

The following exceptions of the L2 criteria are defined:

- Exception #1 with regards to the CC certification of the C-ITS-S itself.
  For the original requirement (25) of the Security Policy [RD-7]:
  "To support the security requirements of confidentiality, integrity and availability (…), C-ITS station operators shall operate C-ITS stations that have been assessed and certified using security assessment criteria against a certified protection profile as specified in the 'common criteria'[2] / ISO 15408 and approved by the CPA. (…)"

  The CPOC Protocol defines the following exception (Table 16 of [RD-3]):

  "*An evaluation of the C-ITS station shall be performed by a SOG-IS recognized test lab. The test lab shall evaluate that the C-ITS station is protected against an attacker with basic attack potential and therefore perform at least the Level 1 Evaluation Tasks in Section* VIII.3.2.1*. A positive evaluation report shall be provided by the station operator to the EA for registration."*
  This means that instead of the originally mandated CC certification for the C-ITS-S, an alternative is possible with the lowest evaluation level for a specific subset of validation-items for a C-ITS-S, which has to be proven by a SOG-IS recognized test lab. For example, this exception can be used if no PP for a specific station type is published yet.

- Exception #2 with regards to the CC certification of the Cryptographic Module / Secure Element.
  For the original requirement (324) of the Certificate Policy [RD-4]:
  "The cryptographic module shall be protected against unauthorised removal, replacement and modification. All PPs and related documents applicable for the security certification of the cryptographic module shall be evaluated, validated and certified in accordance with ISO 15408, applying the Mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS), or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity legislation. "

  The CPOC Protocol defines the following two exceptions (Table 16 of [RD-3]):

  - *"2a) The manufacturer of the secure element shall be certified according to ISO 27001. The hardware platform of the secure element shall have achieved Common Criteria certification. According to certified protection profiles of at least EAL level 4. This comprises the hardware as well as the on-chip software (firmware). Additional software (on top of the certified scope) and/or modifications in the software part from the certified state shall be developed*

following the same processes as other comparable Common Criteria certified products of the same manufacturer."

- *"2b) A SOG-IS MRA accredited certification lab was contracted. A declaration from the certification lab shall be provided by the manufacturer/operator that the corresponding Secure element certification process shall be completed before end of transition phase. During transition phase, periodic (at least six-monthly) progress reports from the accredited lab shall be submitted and assessed by the CPA in order to maintain L1 enrolment of the Secure element."*

Option 2a) replaces the requirements for CC certification of the Secure Element with i) an ISO 27001 certification of the manufacturer of the Secure Element, ii) the CC certification of the chip within the Secure Element, and iii) similar development processes for the addition SW part of the Secure Element, while option 2b) allows the usage of the uncertified Secure Element if the certification process has been started and is ongoing. **In both cases, the applicable documents have to be submitted to the PKI operator to get access to the L1 instance.**

- Exception #3 with regards to the validation of the TLM Certificate within an C-ITS-S.
  For the original requirement as given in section I.6.2.1 of the CPOC Protocol [RD-3]: *"The PKI participants can physically travel to Ispra and receive the current version of the TLM Certificate and corresponding TLM Link Certificate out of band directly from the CPOC. In any case, all PKI participants (including the C-ITS Station) shall verify the TLM Link Certificate using their current TLM Certificate before they actually change/update their trust anchor (TLM Certificate). "*

  The CPOC Protocol defines the following exception (Table 16 of [RD-3]):

  "*The update of the TLM Certificate in C-ITS stations may deviate from the process specified in Section I.6.2.1 of the CPOC protocol if the validation is done by a backend service and the submission to the C-ITS station is performed through a secured channel."*

  This exception allows the use of a (centralized) backend service that validates the TLM Certificate(s) once and distributing it via a secured channel instead of doing this validation in each C-ITS-S individually. A manufacturer that operates its own PKI may make use of this exception. Whether a C-ITS-S operator using a third-party PKI provider can use this exception or not depends as well on his architecture and the PKI provider.

- Exception #4 with regards to the enrolment and authorization management of C-ITS-Ss.
  By default, the process and message flow for enrolment of C-ITS-Ss and their authorization management is specified in ETSI TS 102 941.

  The CPOC Protocol defines the following exception (Table 16 of [RD-2]):

  "*Exceptions on the implemented protocol for enrolment and authorization management for C-ITS stations as well as authorization validation may be granted if the following is ensured:*

- *The same level of security and privacy has been certified by an accredited auditor. The certificate has to be presented to the CPA.*
- *The interoperability with other PKIs and C-ITS stations is ensured by adhering to the certificate profiles specified for RCA, AA, and AT certificates in ETSI TS 103 097."*

This exception is likely to be used by manufacturers that operate their own PKI and to allow them to use an alternative approach under the conditions above. Whether or not such an approach would also be possible when PKI access is purchased via a third party, is open but less likely.

If this option is used, the certificate to guarantee the "*same level of security and privacy*" has to be attached in addition to the other documents.

It is worth to be noted that if the self-declaration of standards and profile conformity claims conformance to TS 102 941, this exception cannot be used.

- Exception #5 with regards to the operation of an ISMS by the C-ITS-S operator.
  For the original requirement (1) of the Security Policy [RD-7]:
  "C-ITS station operators shall operate a certified information security management system according to ISO-27001 [7] that ensures the security of all of their C-ITS stations and the processed data. Instead of the ISMS [7], vehicle C-ITS stations may be covered by a CSMS that is certified in accordance with UN Regulation 155 [8] and EU Regulation 2022/1398 [9]. Systems and infrastructure that are not covered by the CSMS (including all interfaces) and that process data from C-ITS trust model elements [1] shall be certified against ISO-27001 [7]. C-ITS Station operators that operate an essential road transport service according to the NIS [10] or NIS 2 [11] Directives may apply the security measures and security requirements defined by the national transposition of the NIS [10] or NIS 2 [11] Directives instead. "

  The CPOC Protocol defines the following exception (Table 16 of [RD-3]):

  "If a security management system according to requirement (1) of the Security Policy is not available, a comparable security management process shall be operated (e.g. national standard or equivalent to ISO 27001)*"*

- Exception #6 with regards to the Security Policy Audit of the C-ITS-S operator.
  The original requirements (31), (32) and (33) of the Security Policy [RD-7] require a periodic audit by an accredited auditor for Station operators to maintain a valid certification for compliance with this policy.

  The CPOC Protocol defines the following exception (Table 16 of [RD-3]):

  "*The compliance audit for the Security Policy may be conducted internally by the C-ITS station operator which shall be confirmed by a self-issued statement of compliance. This statement does not shift responsibility from C-ITS station operator to the PKI operator."*

  This exception allows access to the L1 instance, even if an "official" audit is outstanding but an internal audit was made instead. **The confirmation of the self-audit has to be submitted to the PKI operator to get access to the L1 instance.**

Table 16 of [RD-3] lists two more exceptions but they are only applicable for PKI operators themselves. A C-ITS-Ss operator that utilises a PKI operator to become part of the C-ITS trust domain does not need to consider them for their C-ITS-Ss.

It is worth to be noted, that *Legal existence of station operator* also applies for L1 instance and shall be proved by the Station operator to the PKI provider.

2.2.3 Accessing L2

The L2 instance is the final instance to use for productive C-ITS-Ss. L2 has the highest access criteria but these can be summarized rather quickly. As the L1 instance defines exceptions from the L2 criteria, the L1 instance is thus discussed in the next chapter after the general criteria has been presented. Additional details and explanations for L2 can be found in [RD-3], section VIII.3, Table 15~~clause 19.3~~.

The criteria to fulfil that are required for a C-ITS-S to access the EA or AA in an L2 environment are:

- *Certification of compliance to the Security Policy*
  The certification of compliance to the Security Policy is proven via an audit by an accredited auditor according to ISO/IEC 27001. ISO/IEC 27002 is also applicable. The compliance to the Security Policy requires - among others - the following two items:
  - A common criteria certification (see ISO 15408) of the Cryptographic Module / Secure Element that is part of the C-ITS-S. This is based on point (28) of the Security Policy, which states that "*C-ITS stations shall comply with the applicable requirements of the Certificate Policy (…)",* e.g. with paragraph (324). One applicable Protection Profile (PP) for this process was developed by C2C-CC, see [RD-5], and can be used as entry point for the common criteria certification.
  - A common criteria certification (see ISO 15408) of the C-ITS-S itself. The requirements for the C-ITS-S itself are a little less stringent that the requirements for the Cryptographic Module. Applicable PPs for a C-ITS-S are usually station type specific. For the majority of station types the PPs are still under development by C2C-CC and C-Roads but for Roadworks Warning Trailers there is already a published version, see [RD-6].
- *Self-declaration of standards conformity*
  This means that full conformity with all relevant standards for interoperability and respective system profiles of stations (self-declaration) is achieved, i.e. that full conformity to either the C2C-CC Profile in Release 1.6.0 (or newer) or to the C-Roads Release 2.0 (or newer) is declared. Some details on the process on ensuring conformity are still to be clarified, see chapter 4.1.

It is worth to be noted, that *Legal existence of station operator* also applies for L2 instance and shall be proved by the Station operator to the PKI provider, based on Section VIII 3.3 of the CPOC protocol.

2.2.4 An example of the enrollment process

This section discusses a fictional scenario where a C-ITS-S shall be enrolled to become part of the C-ITS trust domain (the L2 instance). This example aims to guide the reader through the required steps, clarifying who needs to interact with whom, and identifying necessary documents or artifacts for each step.

Note: A real-world scenario can be more complex and involve additional actors, components and documents than the described scenario has. This scenario focuses on the most important parts. [RD-3] and [RD-4] serve as entry point for any questions about details of the process.

2.2.4.1 The Scenario

For this scenario, there are 3 main actors:

- A company *Company A* is manufacturing C-ITS-Ss that can be integrated into vehicles but the C-ITS-Ss requires some input from its host-vehicles. *Company A* is developing and maintaining the C-ITS-Ss and bringing them into the market.
- The C-ITS-Ss are bought by another company *Operator A*. *Operator A* is the operator of a fleet of public transport vehicles and integrates the C-ITS-Ss into their vehicles. *Operator A* wants his vehicles to be a part of the C-ITS trust domain and has to enrol the C-ITS-Ss, but *Operator A* does not maintain its own PKI.
- The PKI in this scenario is provided and operated by the company *PKI provider A*. *PKI provider A* owns a root certificate / RCA, but it is not yet part of the ECTL. *PKI provider A* also has created an endpoint for an Authorization Authority (AA) and another endpoint for an Enrolment Authority (EA). These endpoints can be considered as webservers. The AA and EA certificate have been created based on the root certificate and *PKI provider A* provides access to the EA and AA endpoints to *Operator A*.

2.2.4.2 The registration of *PKI provider A* at the ECTL

Before any enrolled C-ITS-Ss of *Operator A* would be trusted by other, exiting C-ITS-Ss, the root certificate of *PKI provider A* has to be added to the ECTL. This is a task to be done by *PKI provider A*. They have to create the root certificate and create the derived EA and AA certificates. The infrastructure provided by *PKI provider A* and their processes have to be audited to ensure full compliance to the Certificate Policy. Then, *PKI provider A* can submit an “RCA Enrolment Form” to the Certificate Policy Authority (CPA) – the entity that manages the ECTL – with the following items:

- the RCA Enrolment Form according to the CPOC Protocol template
- the audit report summary

other documents (e.g. Certificate of authorisation of the representative person of PKI provider A)Details for that process can be found in [RD-3], section 3.2. For this example, we assume that the RCA Enrolment is accepted, and a unique CPA-ID is assigned by the CPA to the *PKI provider A*.

Using the unique CPA-ID the *PKI provider A* is able to issue the Root CA certificate and then to submit the “RCA Application Form” to the CPA containing all detailed data of the RCA certificate. Details for that process can be found in [RD-3], section 3.2.

For this example, we assume that the RCA Application Form is accepted, and that *PKI provider A*’s root certificate is added to the ECTL. Then, other users of the ECTL will trust the root certificate of *PKI provider A*.

Note: As *PKI provider A* does not operate any C-ITS-Ss directly, *PKI provider A* does not have to declare compliance to standards and profiles.

2.2.4.3 The challenges before an enrollment can be done

The objective of *Operator A*, as operator of C-ITS-Ss, is to bring physical devices into the market to connect them with other C-ITS-Ss to benefit from that communication. The first step is the purchasing of the C-ITS-Ss from *Company A* and to integrate these devices into the vehicle fleet. These purchased C-ITS-Ss have to be enrolled into the C-ITS trust domain before they are trusted by others and this enrolment has to be done by *Operator A*.

For the enrolment, *Operator A* contracts *PKI provider A* to get access to the necessary security-infrastructure (EA and AA). *PKI provider A* has already done an audit to testify that they comply to the Certificate Policy and thus *PKI provider A* has to follow the rules defined in the Certificate Policy. This means that *PKI provider A* is requesting the following information from *Operator A* before any enrolment can be done:

- certification of compliance to the Security Policy
- declaration of standards conformity
- official company registration document proving legal existence of *Operator A*

2.2.4.4 Getting certificate of compliance to the Security Policy

Operator A contracts an auditor company that is accredited to perform ISO/IEC 27001 audits. The auditor company performs the compliance assessment to certify that *Operator A* and its Stations comply to all requirements of the Security Policy (including certified ISMS system, CC certification of the C-ITS-Ss, CC certification of the Secure Element of the C-ITS-Ss). The findings of this compliance assessment are recorded in the audit report and if all requirements are meet, the auditor issues a certificate of compliance to *Operator A.*

Note: it is recommended that this audit be carried out by *Operator A* before signing the contract with the *PKI provider A*.

2.2.4.5 Getting the declaration of standards conformity

For the declaration of standards conformity, the C-ITS-S operator (Operator A) and the C-ITS-S manufacturer (Company A) need to work together. *Company A* performs all the tests with their C-ITS-S and documents the results using the excel file [RD-9].However, their C-ITS-S requires some input signal from the host vehicle. For example, the current speed and driving direction for all types of vehicles or the status of the lightbar for special vehicles or the status of the doors for public transport vehicles. As a result, *Company A* can only do the tests under the assumptions that for the required signals valid information are provided (this assumption is valid because the C-ITS-S only reads the values and does not modify them).

Both entities, *Operator A* and *Company A*, have to cooperate to test and ensure that the assumptions made by *Company A* are not violated. Tests of the requirements relying on input signals from the host vehicle are in the responsibility of Operator A. Based on the comprehensive test results (including both the manufacturer's tests and the operator's tests), Operator A declares compliance using the self-declaration template [RD-8]. *Operator A* can then use this declaration for the enrolment.

Note: In their contract, Operator A and Company A can agree that Company A has to sign a self-declaration of compliance under the aforementioned assumptions. This declaration however is only relevant within their bilateral agreement. The self-declaration to be provided for enrolment needs to be done by the operator.

Note: it is recommended that the self-assessment and the declaration on standards conformity be carried out before signing the contract with the *PKI provider A.*

Further details on corresponding testing procedures as well as the further proceeding with the self-declaration are still open and will be addressed in future versions of this WhitePaper (see chapter 4.3).

2.3 Processes for product-evolutions

Once the compliance for a specific C-ITS Station type is declared, the devices enter the "operational" phase of their life cycle. This means *Operator A* may enrol these C-ITS-Ss in the EA of *PKI provider A*.

In this operational phase, a continuous monitoring should be established to ensure that the devices continue to comply with the requirements. For example, paragraph (323) of the Certificate Policy states that "*The security of the cryptographic module shall be continuously monitored and maintained as described in the ISMS/CSMS required by the Security Policy. In addition to that, the station operator shall ensure that all vulnerabilities discovered will be addressed (e. g. recorded, mitigated or fixed)".* This is especially relevant following updates in software or hardware but also for stations and services that are regularly reconfigured (e.g. roadworks trailers being deployed in different locations for different use cases). The misbehaviour itself can have different reasons, e.g., misinterpretation of requirements, the outage of a sensor or a malicious attack on C-ITS. Whatever is the reason, misbehaving entities can cause undesired behaviour on other C-ITS-Ss and the misbehaving stations should excluded from the trust zone as soon as possible. The misbehaviour-activities in ETSI are addressing that topic and it is likely that misbehaviour detection and assessment of detected misbehaviour by a misbehaviour authority will become a mandatory feature of C-ITS in the future. At the time of writing this document (beginning of 2024), the misbehaviour assessment is in the specification phase and not operational.

For this operational phase of a C-ITS station, the question arises whether a regular re-assessment is needed, under which conditions it is needed and how it is executed. The following sections provided insides to specific situations and actions that have an impact on standards conformity and in consequence may require a reassessment.

Note: in addition to the stations, also the *Operator A* shall maintain a valid certification compliance with the Security Policy in this operational phase.

2.3.1.1 Situations and their impact on a conformity declaration

Detected misbehaviour can be one out of many reasons to update an enrolled C-ITS-S. An update of the C-ITS-S can affect the former conformity declaration, depending on the scope of the update. In the following some examples are discussed together with the resulting impact on the existing conformity declaration.

- **Situation**: A vehicle-ITS is updated with a newer version of the HMI, i.e., the way how received C-ITS information are displayed to the driver.

  Impact: Neither C2C-CC nor ETSI specify the user experience at the application level in the OSI layer model. Both define requirements for the transmitting side and some requirements on the processing of the received data, e.g. with regards to security.

  Takeaway: If the change is out of scope of the C2C-CC or ETSI requirements, the existing conformity declaration is not impacted. A re-assessment is not necessary.

- **Situation**: The service that provides the absolute position of a vehicle-ITS has to be updated. This service is located on another device within the vehicle than the ITS-stack, but the position data is forwarded to the ITS-stack via an in-vehicle network. This position information is used to generate C-ITS messages.

  Impact: The update is made on an “auxiliary component” that delivers input for the C-ITS-S. C2C-CC has defined requirements on position-information that have to be met by the vehicle-ITS. The vehicle is considered “as a whole” by C2C-CC as no in-vehicle architecture is specified. This gives the OEMs the freedom to design their cars as they want to with the consequence that the vehicle as a complete unit has to fulfil the requirements. If the updated positioning-service delivers data in a significant lower quality, the applicability of the update should be discussed before enrolling it to the vehicle as the fulfilment of the position requirements is under risk.

  Takeaway: If an auxiliary component is changed, it should be ensured that the requirements are still met with that change. Compliance of the position-information to the C2C-CC requirements are a part of the conformity assessment. As that exemplary change does not affect all C2C-CC requirements, a re-assessment of the affected items should be made.

  This takeaway would also be applicable if an existing C-ITS component of one vehicle-type would be integrated into another vehicle-type but the other vehicle-type uses a different in-vehicle-architecture.

- **Situation**: An aftermarket device receives vehicle dynamic information via an interface from an external sensor of the host vehicle. This aftermarket device is developed further and now supports an additional input interface for dynamic information (e.g. speed). The host vehicle’s sensor still delivers data with the same quality, only the way how the information is shared with the ITS-stack is changed. This additional interface can be used as alternative to the existing interface. The existing interface was already in the scope of the conformity declaration.

  Impact: Even if the sensor in the host vehicle and the software of the ITS-stack in the aftermarket device are unchanged (and both fulfils the C2C-CC requirements), this new interface modifies the connection between those two.

Takeaway: If the connection in a distributed system is changed, it should be ensured that the new connection does not modify the data and thus does not impact the assessed components in a negative way. A re-assessment of the affected items should be made.

- **Situation**: The supplier of a C-ITS-Ss identified a software bug in its GeoNetworking implementation. For this and previous software-version the conformity was already declared.

  Impact: GeoNetworking is a mandatory feature of the C2C-CC BSP. Changes in the GeoNetworking can have an impact on the message dissemination behaviour and result in changes on the channel utilization. Depending on the type of bug, a bug (or a wrong fix of the bug) could also impact the forwarding behaviour of another C-ITS-Ss.

  Takeaway: For every bugfix in a component that is covered by the C2C-CC BSP a re-assessment of the affected parts should be carried out. The scope of the assessment should be identified carefully. With the GeoNetworking example it could be necessary to validate not only some of the GeoNetworking requirements again but also some of the triggering condition requirements that uses the underlying GeoNetworking features.

- **Situation**: The supplier of a C-ITS-S releases a new version of its implementation, i.e., a C-ITS-stack in version 2.0 that has been heavily refactored. The implementation aims for compliance to the same C2C-CC release as the previous version.

  Impact: A new major version comes hand in hand with major changes. Comparability of that version with older versions is not necessarily given. This new version has to show that it is compliant to all the requirements.

  Takeaway: After major changes in the software or hardware of an existing implementation, a full assessment should be carried out similar to the initial release of the previous version.

- **Situation**: The supplier of a C-ITS-updates the existing implementation to comply with a new C2C-CC release.

  Impact: The conformity declaration is only valid for one specific release. Future versions of the C2C-CC specification can change existing requirements because of different reasons, for example to fix bugs or to revise the phrasing to eliminate a maybe existing ambiguity. This means that devices that comply to an older version of the C2C-CC specification does not automatically comply to newer versions.

  Takeaway: For updating an implementation to comply with a new release a detailed change analysis should be made. Parts of the new C2C-CC release could be unchanged and these parts does not have to be validated in detail again. An example could be where the position of a vehicle-ITS is taken from another component within the vehicle and the position requirements have not been changed at all. This position information can still be considered as “compliant”. The changed parts however should be validated in detail again.

If the existing implementation is updated to a new major version of the C2C-CC specification, a full assessment is recommended.

- **Situation**: An aftermarket device uses external information from the host vehicle (e.g. speed). Under the assumption that the provided information of the host vehicle complies with the requirements from C2C-CC, the aftermarket device is declared as compliant to all requirements. This type of aftermarket devices is already integrated into one type of host vehicles and should now be integrated into another type of host-vehicle of a different brand.

  Impact: The new type of host vehicles maybe not fulfil the C2C-CC requirements and an aftermarket device that uses this “insufficient” data could be considered as not compliant.

  Takeaway: If a conformity declaration is made with assumptions, it should be validated if the assumptions are still valid if the device is integrated into another environment. This task is mainly at the operator-side of the devices, the aftermarket supplier should clearly state any assumption that was taken to declare conformity.

This list of situations is not conclusive. Other situations that need to be addressed include e.g. updates or additions to new C-ITS message formats for a new or existing use case. In addition, all security related changes (e.g. patches that fix a security gap) heavily affect conformity and need to be considered when defining processes and requirements for re-assessment.

2.3.1.2 The process of re-assessment

The re-assessment is a process where an already existing assessment (conformity declaration) is used as a basis and only parts of the implementation are assessed again. Usually, this re-assessment is carried out when only small parts of the implementation have been changed itself or are affected by changes in other components (e.g., provided input data from used sensors). A re-assessment is helpful to transfer an existing conformity declaration to a newer version of the implementation while keeping the required effort small. A full, new assessment for some bugfixes is also possible but not an efficient use of resources.

As a first step, the scope of the re-assessment has to be identified. There are different ways, depending on the changes. One way could be comparing documents with each other (e.g. for updating the implementation to a new C2C-CC release). Another way is to perform an effect-analysis, to identify the affected requirements item (e.g., when a used sensor is changed or updated).

This list defines the reduced scope of the re-assessment. The list contains the affected requirements and can be used to identify and select the related validation procedures to carry out. Only for those items new test results have to be generated.

The new set of results can be transferred into a new version of the C2C-CC “Self-Assessment-Sheet” [RD-9]. This sheet can be prefilled with the results of the already existing requirements (takeover of results) and is then completed with the test results of the validation activities for the re-assessment. For traceability and transparency, it is recommended to provide the following information in sheet:

- that a re-assessment was made,
- what was the basis for the re-assessment (i.e., identify the previous version of the Self-Assessment-Sheet),
- what was the scope of the assessment (e.g., list the affected requirements),
- provide information why the supplier assumes that existing results can be taken over.

After the re-assessment was conducted successfully, further details maybe have to be discussed with the responsible PKI operator in order to add C-ITS-Ss with this updated implementation to the trust domain (see chapter 4.4).

2.3.1.3 Final remarks on self-assessment and re-assessment in C-ITS

For a self-assessment the responsibility for being compliant remains first and foremost with the entity that declares compliance. This entity has the freedom to ask third parties, e.g., a conformity assessment body, to do parts of the job but the final responsibility stays with the entity. With that being said, it is also the responsibility of the entity to identify the scope of any changes and the affected requirements correctly to conduct a re-assessment. If affected items are not identified correctly and thus are not tested, the conformity declaration is no longer valid if those items are violated.

It should also be noted that C-ITS is very open system and requires trust between C-ITS-Ss of different manufacturers to provide a benefit. One part of this trust is the early identification of misbehaving entities and a quick exclusion of them from the trust domain. Doing so, the impact of misbehaving or even malicious devices can be limited. This requires an operational misbehaviour detection & reporting functionality. As soon as this is established, every unit can continuously monitor every other unit in its vicinity and check it for misbehaviour. Thus, it is not only the supplier of the device that does validation before the production is started, but instead deployed devices are also tested continuously along their operational phase (at least to a certain level). It can be assumed that the first version of misbehaviour detection algorithm will start with quite relaxed requirement validations, but future version maybe also validate more stringent for the requirements. Updates of existing stations, where one bug was fixed but another one was created, could be quickly identified by the C-ITS-Ss in the field.

A re-assessment would be made “on demand” when changes have been introduced to an existing implementation of a supplier. Today (2023), there is no requirement to repeat this re-assessment on a periodic basis. However, future system that are progressively connected will have an increased demand to stay secure. As a result, those systems are continuously updated and at least supplied with security patches. It has to be discussed if such patches are a sufficient change to justify a limited re-assessment (since the underlying software configuration has changed). If so, this could result in a process of continuous improvement of the implementation and of a continuous re-assessment-process.

3 Guidelines for self-testing

Since standard compliance is declared by the operators and manufacturers, they need to have proper procedures in place to test their implementations and C-ITS stations for compliance. This chapter provides first basic guidelines and principles for this self-testing.

Detailed recommendations will evolve over future versions of this WhitePaper (see chapter 4.5).

3.1 Testing for compliance to C2C-CC specifications

For the IUT a verification has to be carried out for all triggering conditions [C2CCC tc Docs] that are implemented. The verification should comprise at least the following:

- The DENM content should be verified for a full cycle of the triggering condition. This includes:
    - the detection of the event
    - at least one update-cycle
    - at least one termination cycle

  Some triggering conditions do not specify an update or termination cycle. In those cases, only the applicable cycles have to be validated. A full cycle refers to the initial detection / update / terminate DENM and the following repetitions of the DENM. Within such a full cycle, the content of each single message should be validated against all applicable requirements, i.e., the DENM content as specified by the triggering condition document as well as the content required by the VSP [C2CCC BSP].

  For example: A new DEMM for a “Stationary vehicle warning – stopped vehicle” [C2CCC tcStVe] is repeated for 15 s. Every 15 s the DENM is updated and repeated for 15 s. The termination DENM is also repeated for 15 s. A full cycle for this use case would at least cover 45 s.

- Each specified path in the triggering condition should be validated at least once. The correct behaviour for each path should be validated but each path does **not** have to be validated with a full cycle (see point above). This is applicable to all specified detection, update and termination paths.

  For example: The “Stationary vehicle warning – stopped vehicle” [C2CCC tcStVe] defines the detection-conditions a) – h) (see RS_tcStVe_120). Each of the conditions should be validated once. In addition, according to RS_tcStVe_121, the following validations should be done:

    - Check that the same condition is only considered once for the timer-reduction.
    - Check that two different conditions reduce the timer correctly. The two conditions can be either of the group a) – d) or the first condition is one of the group a) – d) and the second one is one of the group e) – h).

Detailed guidelines for testing compliance to the VSP will be given in future versions of this WhitePaper (for basic considerations, see chapter 4.6).

3.2 Testing for compliance to ETSI specifications

The C2C-CC VSP contains references to several ETSI documents. The conformity to these documents is also part of a full self-declaration of conformity towards the C2C-CC specifications. The C2C-CC “Self-Assessment Sheet” [RD-9] for such a conformity declaration supports also link to additional documents. Those links can be used point to the related “Protocol conformance test report Proforma” which is specified by ETSI. The Proforma-statement can be created after conducting all the related ETSI tests. The C2C-CC “Self-Assessment Sheet” would then only link to the Proformas and enables an easy tracking of additional third-party documents.

With regards to testing of ETSI specifications, it is recommended to use the existing tests and test procedures specified by ETSI. A list of the most relevant documents is (not comprehensive):

- ETSI TS 102 868-x
- ETSI TS 102 869-x
- ETSI TS 102 871-x
- ETSI TS 102 917-x
- ETSI TS 103 096-x

Note: The “x” is a placeholder. Each item represents a series of documents, each with 3 parts.

The listed documents have been created and are maintained by ETSI ITS to test the related functional standards. The first step to a full conformity to the functional standards is conducting all the validations listed in these test-documents. However, as the functional standards are under continuous development / improvement via change requests, the test-specification are not necessarily always up to date. The approved change requests of ETSI ITS are an obligatory extension of the main document and usually they improve only the functional standards. The related test-documents are not in all cases updated accordingly by change requests. As a result, for some parts of the functional documents the related tests could be missing.

For the entity that declares conformity, this is an additional burden. The entity would have to check which change requests are approved and how the related tests are affected or if new tests have to be created to cover the new / changed functionality. Those tests should be conducted in addition to the tests of the related test-document and added to the C2C-CC “Self-Assessment Sheet”.

3.3 Handling of ambiguities

There can be cases where the functional specification or a test is not clear. For example, there can be different interpretations of a requirement, the description of the test procedure is not detailed enough on how a step have to be performed exactly, the results is not clearly

specified or an implicit dependency between items is not visible and thus leads to different results than expected. As there is no guarantee that the specification is free of errors, the entity that declares conformity should approach the responsible standardization body in such cases.

If the entity is a member of C2C-CC, the issue can be reported directly via C2C-CC's issue-tracker and then be discussed with the C2C-CC expert groups. If the entity is not a member of C2C-CC, the entity can submit the issue via [RD-2] and receive a response on that issue.

4 Open questions

This chapter documents open topics that are not yet finally discussed in the consortium that will be addressed in future versions of this White Paper.

4.1 Self Testing and Self Declaration

For the responsibility assumed by the manufacturing and operating organizations, especially questions regarding re-assessment following software updates or on reconfiguration of a C-ITS Service need to be finalized.

A probable approach for this is that Once the devices were bought by the Operator A, this company is responsible to perform the re-assessment tests. It may contract the manufacture for re-testing, but the overall responsibility to keep devices in a „secure mode" is in the Station operator company's responsibility.

Depending on the changes made in an update, it is sensible not to do a full assessment again. This means however that someone (whose responsibility is this) will have to determine the required extent of a reassessment. How much risk for assessment gaps is the responsible organization or the C-ITS in general willing to take? How can this remaining risk be properly addressed through misbehaviour detection?

4.2 Standards conformity

When it comes to the standards conformity necessary for L1 and L2 as per the CPOC protocol, the methodology to ensure that transmitted messages comply with interoperability standards and specifications is not yet explicitly defined. This overarching topic gives rise to more nuanced questions. For instance, we need to consider how the integration of central components within the road infrastructure system should be represented in the compliance assessment for C-ITS messages.

4.3 Processing of the self-declaration

As described in section 2.2.4.5 the operator and manufacturer of a C-ITS-S have joint responsibility to declare conformity with the standards. As of the current understanding this self-declaration is provided to the PKI operator in order to get enrolled in the PKI.

Some topics with regards to the processing of the self-declaration by the PKI operator however remain open. E.g., it still needs to be clarified if, how, by whom and on which basis the self-declaration is further validated (regarding correct test procedures, consistency and completeness of the declared conformity).

4.4 Re-assessment and PKI operator

After executing a re-assessment as discussed in section 2.3.1.2, the result needs to be discussed and communicated at least with the responsible PKI operator. The details and required extent for this interaction still need to be clarified.

4.5 Self-Testing

The guidelines we've delineated for self-testing in Chapter 3 require further refinement and expansion. This will entail a deeper dive into the specifics of the testing procedures that need to be conducted. For instance, we should provide detailed recommendations on the deployment of Software-in-the-Loop (SiL) and Hardware-in-the-Loop (HiL) environments, as well as the use of real-world data. We also need to address the parameters required to establish a statistically valid basis.

In addition to these points, expanded guidelines must account for determining the optimal length and setting minimum requirements for real-world test drives. These considerations are crucial, for example when validating e.g., the correct implementation of Cooperative Awareness Message (CAM) generation rules. The scope of this includes but is not restricted to ensuring adequate length for covering AT change steps. Test rides should also be sufficiently long to cover the concepts for pathHistory generation and ensure the coverage of different driving environments—urban, rural, and highway settings alike.

4.6 Self-testing compliance with the VSP

Testing of compliance with the VSP is by nature more focused on system related aspects. Considerations for further guidelines will include recommendations on adequate data sets for testing Position and Timing requirements. Other aspects to be considered will be hopping of messages as well as lifetime-considerations in the GeoNetworking.

4.7 Misbehaviour detection

Misbehaviour detection is a topic that is still being worked on in standardization. As soon as the general concepts are harmonized and clarified, this concept can play an important role in ensuring compliance in the operational phase of C-ITS-Ss.

5 Appendix A – Related documents and references

In addition to the documents listed below, some of the documents are references by their symbol as defined in the Release Overview (C2CCC_TR_2000). Those items can be recognized by text that is enclosed in "[" and "]".

[RD-1] Glossary - CAR 2 CAR Communication Consortium, https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.2/C2CCC_TR_2053_Glossary.pdf

[RD-2] C2C-CC First Point of Contact, https://www.car-2-car.org/first-point-of-contact, accessed 10.01.2022

[RD-3] C-ITS Point of Contact (CPOC) Protocol , https://cpoc.jrc.ec.europa.eu/data/documents/E01941_CPOC_Protocol_Release-3.1_20240627.pdf, accessed 05.07.2024

[RD-4] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf, accessed 05.06.2024

[RD-5] Protection Profile V2X Hardware Security Module, https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.0/C2CCC_PP_2056_HSM_V1.0.pdf, accessed 27.11.2023

[RD-6] Protection Profile for a Roadworks Warning Unit Version 1.1, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html, accessed 27.11.2023

[RD-7] Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf, accessed 05.06.2024

[RD-8] Template for the declaration on C-ITS standards conformity – CAR 2 CAR Communication Consortium, https://www.car-2-car.org/documents/basic-system-profile

[RD-9] Self Assessment Sheet – CAR 2 CAR Communication Consortium, https://www.car-2-car.org/documents/basic-system-profile