



C-ITS DELEGATION MECHANISM

23.09.2025



Co-funded by
the European Union

Table of Contents

1.	Introduction.....	4
1.1	C-Roads platform for harmonisation of C-ITS deployment.....	4
1.2	C-ITS services.....	5
1.3	Purpose of a reading guide to the WG2 C-Roads documentation.....	6
1.4	Story board C-Roads C-ITS deployment documentation.....	7
1.5	C-ITS documentation release and version overview.....	11
2.	Motivation and Concept.....	13
3.	Delegations Requirements.....	16

Table of Figures

Figure 1:	Overview of C-Roads coverage.....	5
Figure 2:	Overview of C-Roads Working Groups.....	8
Figure 3:	Story board and C-Roads documentation.....	8
Figure 4:	IVIM signature verification.....	13
Figure 5:	IVIM without delegation.....	14
Figure 6:	IVIM with delegation.....	15

Document history

Version	Date	Description, updates, and changes	Status
1.0	Mar. 2023	First proposition by the C-Roads platform (WG2 – TF1)	Draft
1.0.1	Apr. 2023	Review by C-Roads members	Draft
1.1	Jun. 2023	Additional remarks by C-Roads members	Draft
1.2	Dec. 2023	Update following CP editing team review	Draft
2.2.0	May 2024	Finalisation for C-Roads publication	Draft
3.0.0	September 2025	Update of introduction and references	Approved

List of used abbreviations

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

References

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

1. Introduction

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

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

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

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

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



Figure 1: Overview of C-Roads coverage

1.2 C-ITS services

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

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

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

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

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

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

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

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

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

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

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

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

1.4 Story board C-Roads C-ITS deployment documentation

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

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

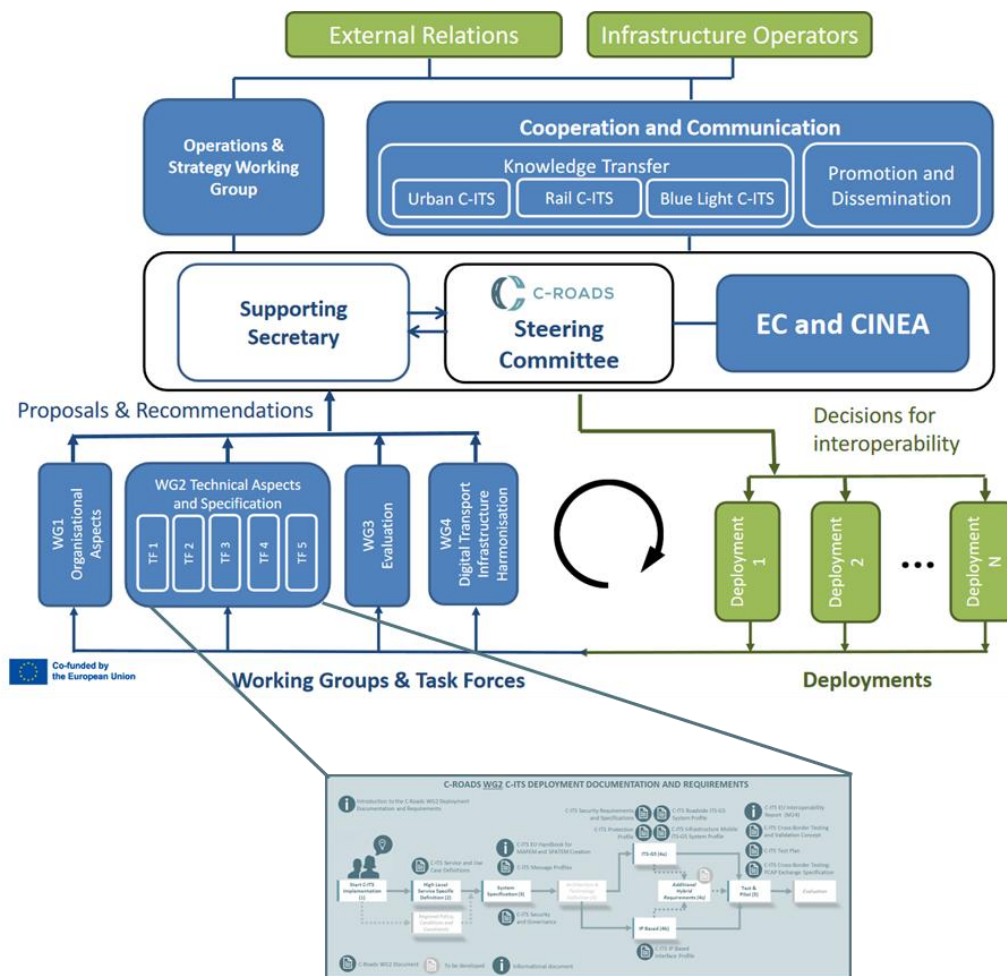


Figure 2: Overview of C-Roads Working Groups

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

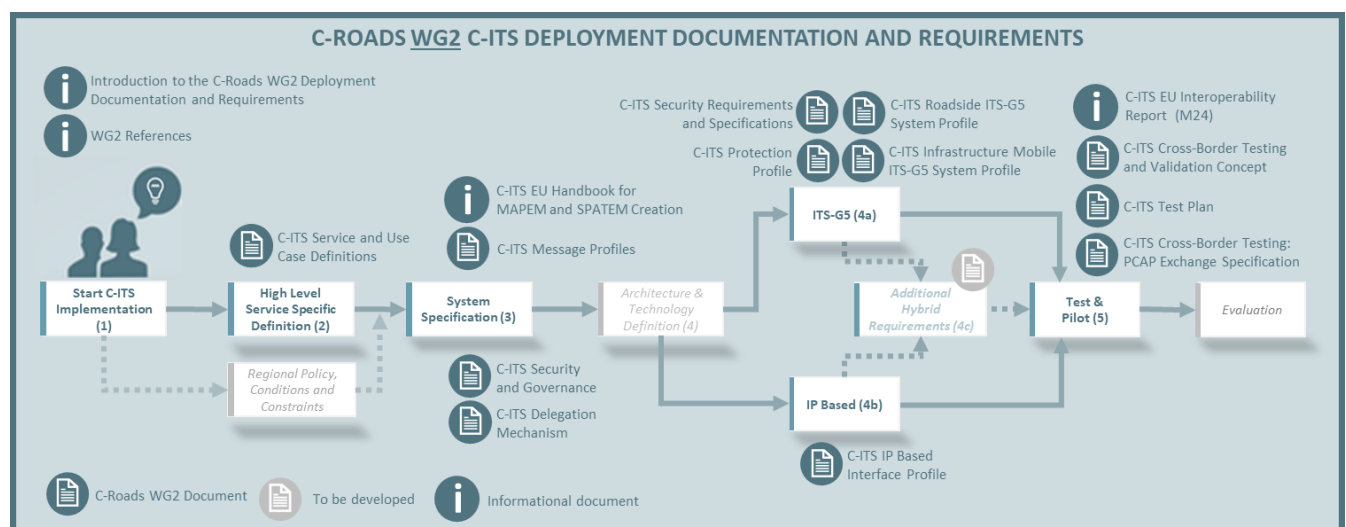


Figure 3: Story board and C-Roads documentation

Stage 1: Start C-ITS Implementation

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

Associated C-Roads document(s):

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

Stage 2: High Level Service Specific Definitions

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

Associated C-Roads document(s):

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

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

Stage 3: System Specification

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

Associated C-Roads documents:

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

Stage 4: Architecture & Technology Definition

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

Stage 4a: ITS-G5

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

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

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

Associated C-Roads document(s):

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

Stage 4b: IP-Based

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

Associated C-Roads document(s):

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

Stage 4a and 4b:

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

Stage 4c: Hybrid

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

Stage 5: Test & Pilot

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

Associated C-Roads document(s):

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

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

1.5 C-ITS documentation release and version overview

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

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

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

2. Motivation and Concept

This section introduces the “delegation”, which conceptually describes an approach to handle IVI messages consistently across different road operators, or IVI service providers in broader terms.

The delegation is restricted to IVI ServiceProviderID that is the identifier of the C-ITS station Operator. The C-ITS standards and regulation as defined in the EU [EU C-ITS SP] and in the [EU C-ITS CP] remain applicable, in particular to the delegator and delegate and their C-ITS stations. The delegation is strictly limited to the use of ServiceProviderID SSPs.

In order to correctly use the IVI service, the IVI PSID requires to include the Service Provider ID in its respective SSP bits [ETSI TS 103 301]. As required by [ETSI TS 103 301], the receiving station verifies for any incoming IVI message that the Service Provider ID within the message matches with the Service Provider ID within the AT of the sender that signed the IVI message, see Figure 4.

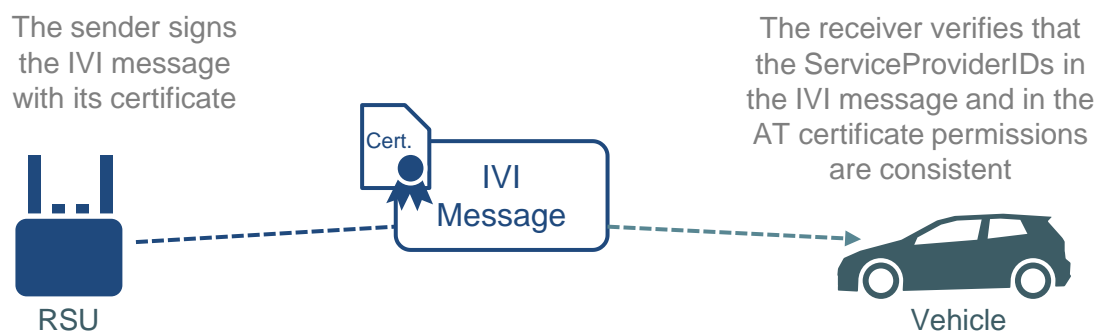


Figure 4: IVIM signature verification

The content provider (i.e. service provider or road operator) of IVI message is required to include its own Service Provider ID as part of the content, as well the message ID. In case another station with a different Service Provider ID is encoding, signing and sending the IVI message with a content of this provider, it is crucial to ensure the use of correct Service Provider IDs for trusted distribution of IVI messages.

When signing and sending IVI messages with a content of a different provider, it might lead to a mismatch of Service Provider IDs present in the content of the IVI message and in the AT certificate used to sign the message delivered to the end receiver, see Figure 5.

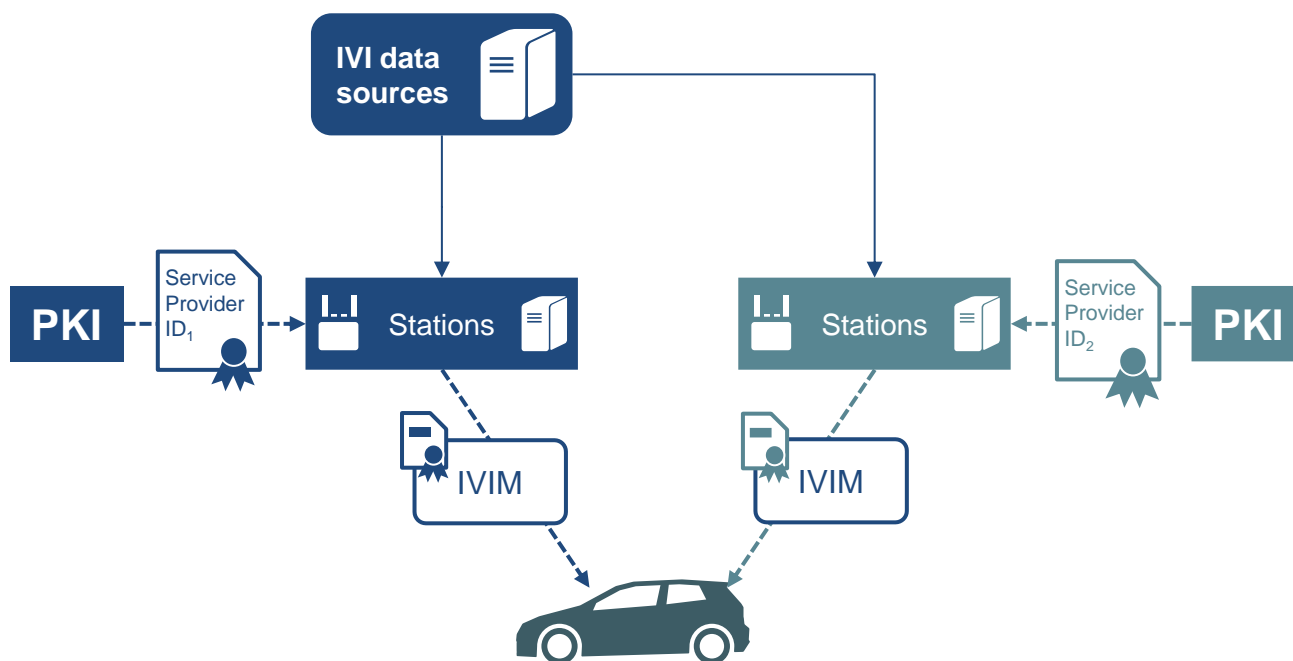


Figure 5: IVIM without delegation

The permissions delegation mechanism consists of a Service Provider (*Delegator* - *ServiceProviderID₁*) authorizing an ITS station of another Service Provider (*Delegate* – *ServiceProviderID₂*) to use certificates suitable to sign IVI messages with the content of the delegator.

As a consequence, the delegation concept requires operators of C-ITS stations that sign and send IVI messages with content received from other service providers or road operators to have obtained consent from the respective service providers or the road operators (i.e., the content providers) to obtain and use AT certificates with the Service Provider IDs of the content providers.

Please note: The underlying standard IEEE 1609.2 does not allow an AT to contain multiple SSP values for a given PSID. Hence the different Service Provider IDs have to be handled in separate parallel ATs (i.e. number of ATs containing a specific pair of ITS-AID, SSP) as laid down in section 7.2 of the [EU C-ITS CP].

This way, the Service Provider IDs in the message and the certificate can be matched by receivers as part of the verification process of the validity of the message, see Figure 6.

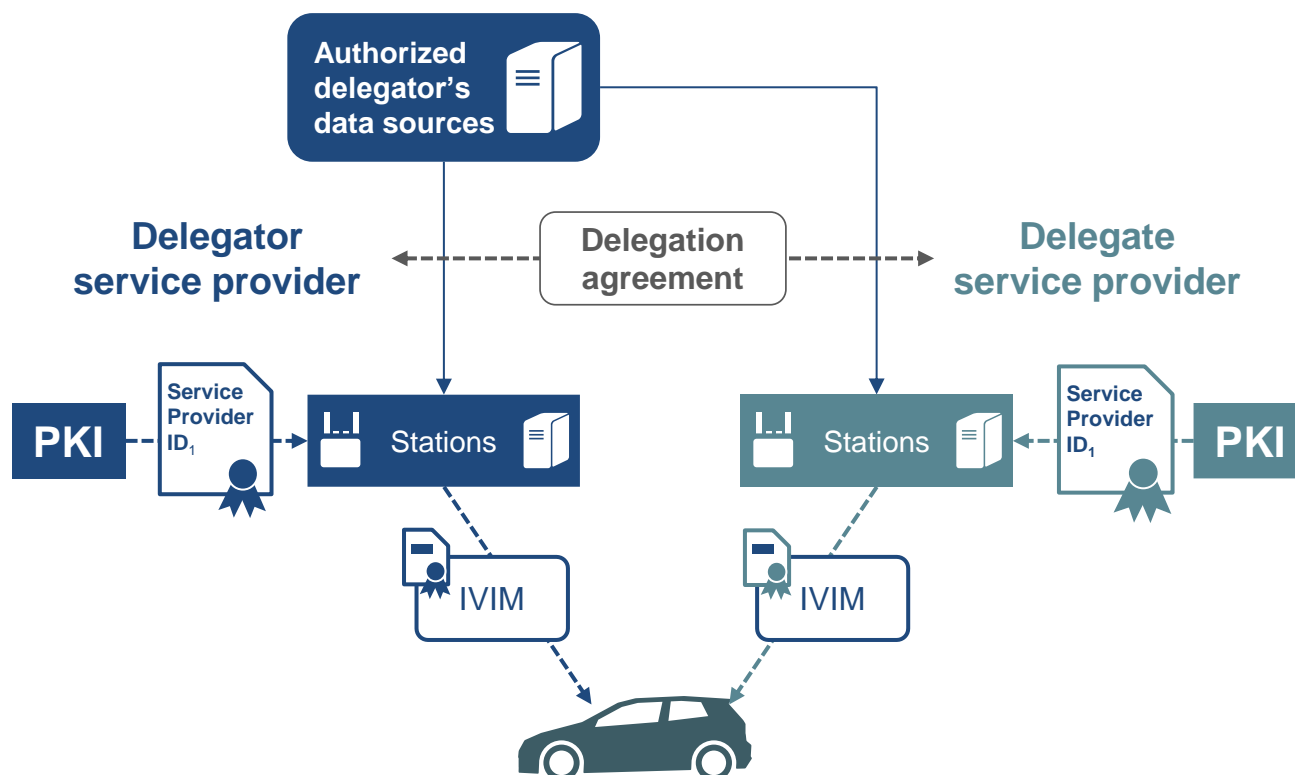


Figure 6: IVIM with delegation

Notes:

- The operators of the delegate ITS station may be a road authority, a private independent actor or a legal national entity.
- Content of the IVI message may be provided by the delegator through different sources.

3. Delegations Requirements

In the following section, requirements reflecting the current state of discussions are presented.

- The delegation of permissions shall only be granted for a period limited to the compliance validity (cf. [EU C-ITS CP]) of the delegate and delegator
- PKI operators have to be informed about all delegation agreements that are in place between the subscribed C-ITS actors (delegator and/or delegate)
- PKI operators shall ensure that stations registered in their PKI get IVI permissions for agreed IVI messages, with valid Service Provider ID SSPs (i.e. own or delegated Service Provider ID – if delegated, the Delegation Agreement document should be provided by the station operator)
- The IVI message encoded, signed and sent by the delegate shall only contain data coming from the delegator's authorized system(s)

The following steps have been identified as necessary to formally set up the delegation process. The sequence given here is indicative, the final delegation agreement being the official proof of delegation.

- The delegator sends a delegation request to the delegate including:
 - The identity of the organisation and registration information (name, address, legal proof of registration, contact info)
 - The type of messages / data concerned
 - The corresponding list of SSPs to be delegated
 - The needed period of delegation
- The delegate shall determine that the delegator organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation.

The delegate shall confirm that the delegator organisation has authorised the delegation and that the contact submitting the request on behalf of the delegator is authorised to do so.

- After the verification and validation of the delegator request, the delegate shall send to the delegator the following documents:
 - Identification information of the ITS station(s) that will sign IVI messages with the content of the delegator using the Service Provider ID of the delegator, along with the name of the Root CA that will provide the certificates
 - Identification information of the servers (e.g. traffic manager) that the delegator authorizes as IVI data sources to the delegate.
 - A proof of security/compliance of this(these) ITS station(s) shall be provided to the delegator (e.g. audit report proving the compliance to [EU C-ITS CP] and [EU C-ITS SP])
 - Delegation Agreement (contract) with the needed information (identification of the parties, IVI permissions, period of the agreement) and any other information considered useful. This agreement is signed by the contact of the delegate
- The delegator shall verify the documents provided. In particular:
 - Verify that the ITS station(s) that will sign IVI messages are compliant to [EU C-ITS CP] and [EU C-ITS SP]

- Verify that the Root CA certificate is present in the ECTL
- Verify that the delegate organisation has authorised the delegation and that the contact who signed the delegation agreement on behalf of the delegate is authorised to do so.

In return, the delegator countersigns the Delegation Agreement.

- The delegate shall provide this Delegation Agreement to its PKI operator to prove the right to request IVI permissions of the delegator.
- The delegate's PKI Operator (EA) shall verify the Delegation Agreement and if (and only if) accepted, it shall support the issuing of the requested IVI Permissions.
- The PKI operator verifies all the delegation requirements and documents and accepts or rejects the delegation request and corresponding certificate requests.
- The PKI operator may need to generate a new AA certificate to cover the delegator Service Provider ID SSPs.

Any change in the compliance status of the delegate or its PKI provider shall be promptly notified to the delegator.

IMPORTANT: This delegation mechanism described above might be one possibility among others to solve the issue of an ITS station IVI managing messages from multiple service providers. The potential security and legal questions and implications raised by such solution should be carefully analysed before implementing it.

Without delegation, C-ITS stations from a Service Provider should not request certificates containing other ServiceProviderID than the one assigned by the national registration administrator and available in the national registry according to EN ISO 14816.