



C-ITS DELEGATION MECHANISM

04.11.2025



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	Story board C-Roads C-ITS deployment documentation.....	5
1.3	Scope of this document.....	6
2.	Motivation and Concept.....	7
3.	Delegations Requirements	10

Table of Figures

Figure 1: Overview of C-Roads coverage.....	5
Figure 2: Highlight of WG2 document in complete story board	6
Figure 3: IVIM signature verification	7
Figure 4: IVIM without delegation.....	8
Figure 5: IVIM with delegation	9

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 references	Approved
3.1.0	November 2025	Update of introduction	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 3.0.0 (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. In order to enable an efficient and undisturbed exchange of information within these services as well as a cross-border implementation, harmonised C-ITS specifications are indispensable. The approach starts from a functional perspective, then requirements applicable to all implementations and then towards technology specifications of currently validated implementations (ITS-G5 for short range communication, IP based for long range cellular). In order to meet these challenges, the C-ROADS platform is divided into four Working Groups. The first Working Group is concerned with organisational tasks, the second with Technical Aspects and the third with Evaluation and Assessment. The fourth Working Group is about 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 last working group Strategy and Operations 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.

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.

The content of the WG2 documentation is based on input from actual implementations and was harmonised in C-Roads task forces and working group. Specifications of additional implementations can be provided to C-Roads and will be incorporated into the document through the harmonisation process.



Figure 1: Overview of C-Roads coverage

1.2 Story board C-Roads C-ITS deployment documentation

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

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

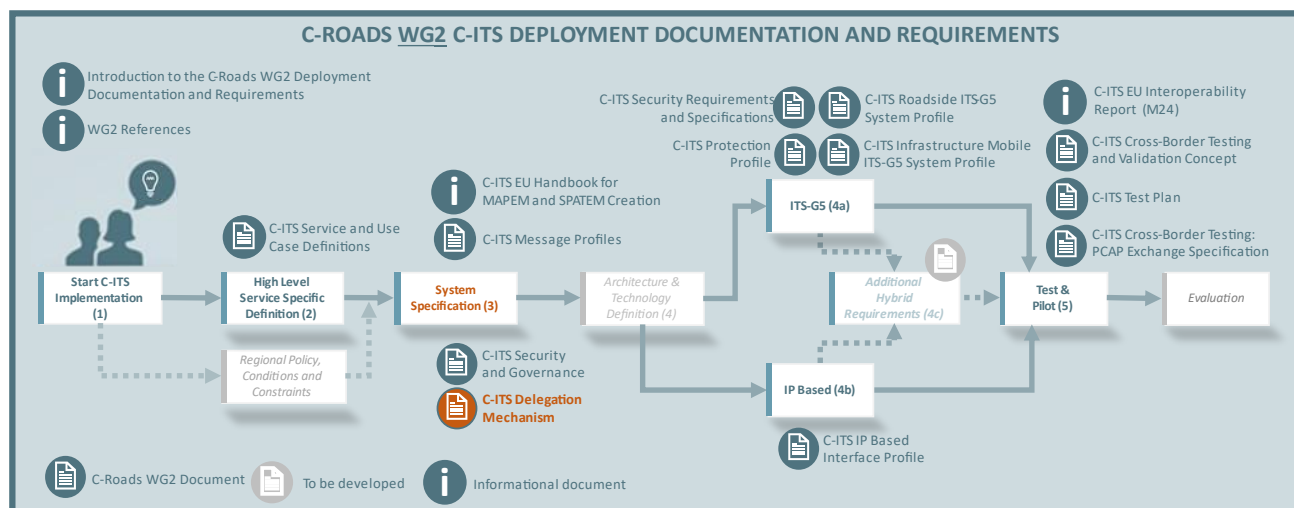


Figure 2: Highlight of WG2 document in complete storyboard

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

1.3 Scope of this document

This document describes a proposition to manage the delegation of IVIM's ServiceProviderID.

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 3.

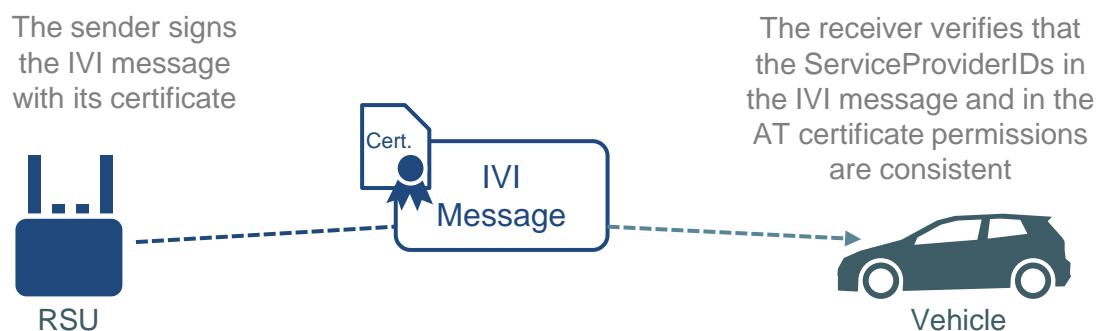


Figure 3: IVIM signature verification

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 4.

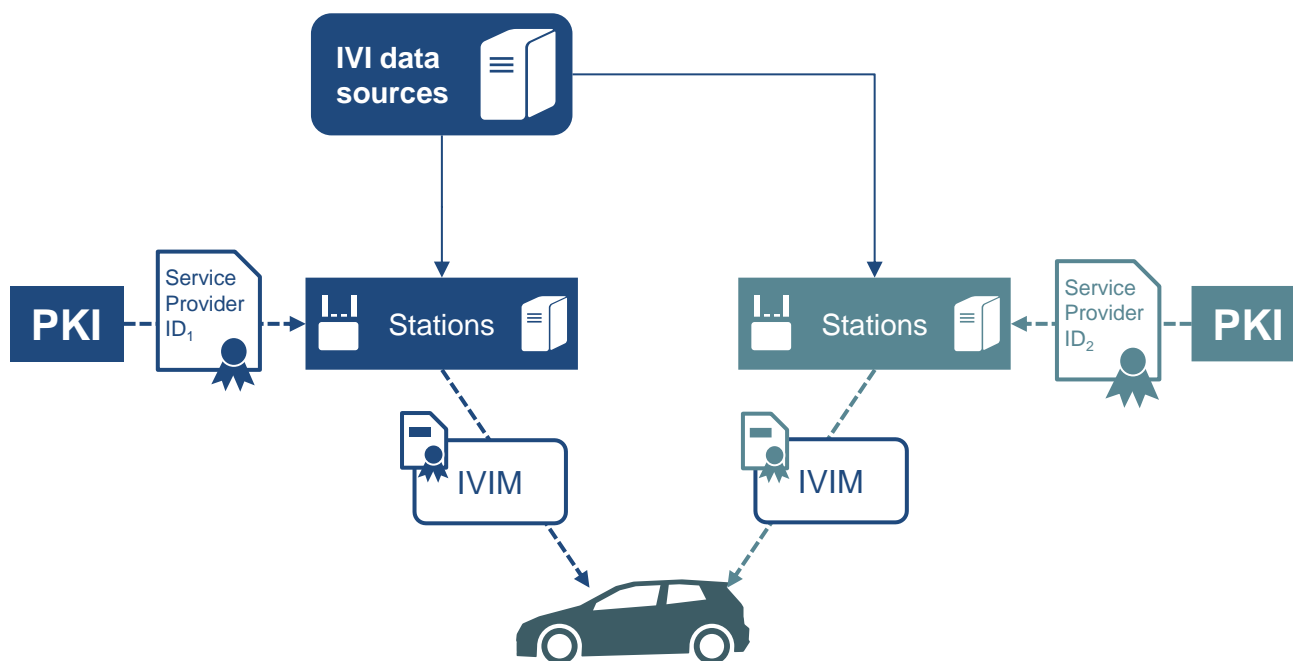


Figure 4: IVIM without delegation

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 5.

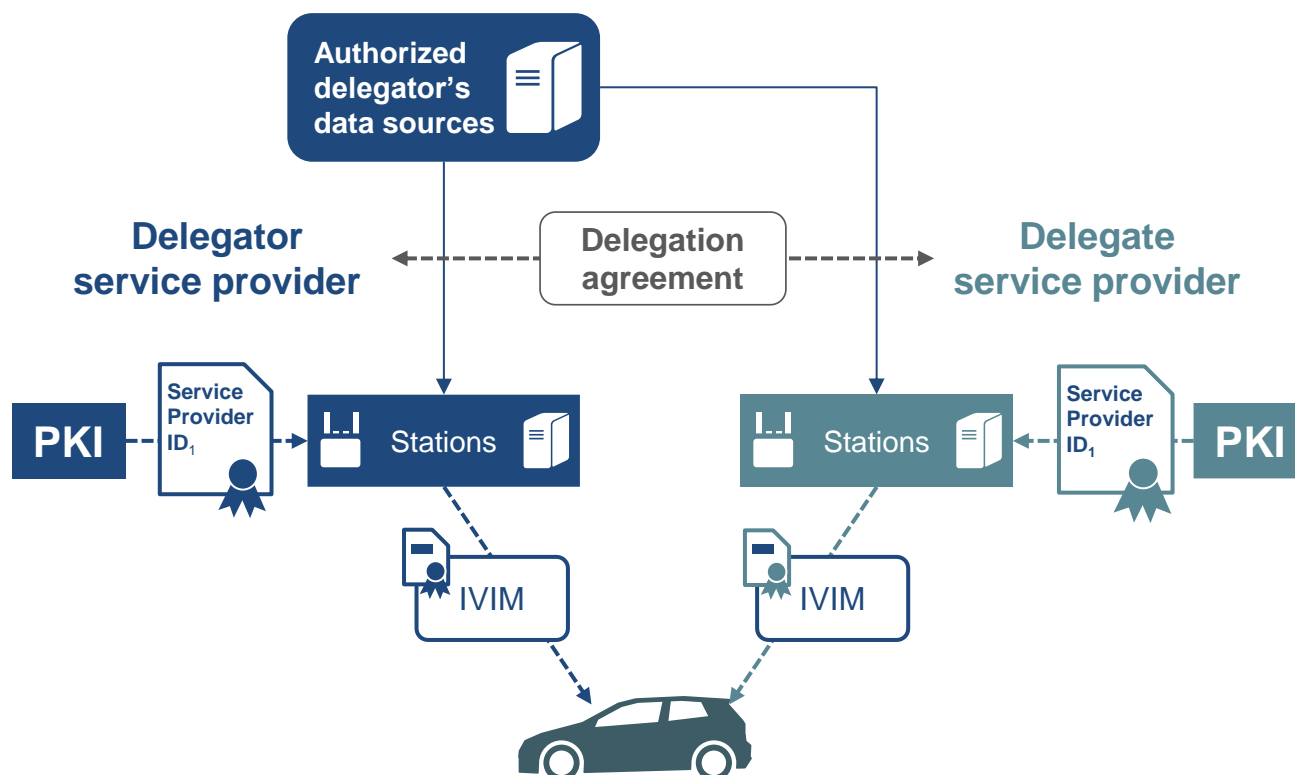


Figure 5: IVIM with delegation

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.