



# **C-ITS IP Based Interface Profile**

## **Version 2.0.8**

C-Roads Platform

Working Group 2 Technical Aspects

Taskforce 4 Hybrid Communication

## Revision information and document handling

Version	Date	Description	Status
1.0	19.06.2019	Draft for approval by Steering Committee	Draft
1.5	02.07.2019	Based on SC meeting on 02-07-2019: Release 1.5 is accepted for C-ROADS deployment by all member states	Final
1.6	17.12.2019	Based on SC meeting on 17.12.2019 Release 1.6 is accepted for C-ROADS deployment by all member states	Final
1.7.0	24.06.2020	Based on SC meeting on 24.06.2020 Release 1.7.0 is accepted for C-ROADS deployment by all member states	Final
1.7.1	6.10.2020	Draft for release 1.7.1 for approval by Steering Committee This is fourth version of the document which means that all changed and new requirements have /4.	Draft Internal -
1.8	16.12.2020	Based on SC meeting on 16.12.2020 Release 1.8 is accepted for C-ROADS deployment by all member states. This is fifth version of the document which means that all changed and new requirements have /5. Changes compared to 1.7.1 <ul style="list-style-type: none"> <li>- Informative text and additional information added, mostly on bilateral agreements for BI-BI testing</li> <li>- Two new technical requirements related to information management</li> </ul>	Final
2.0	29.06.2021	Based on SC meeting on 29.06.2021 Release 2.0 is accepted for C-ROADS deployment by all member states. This is sixth version of the document which means that all changed and new requirements have /6. Changes compared to 1.8 <ul style="list-style-type: none"> <li>- Description of Central C-ITS architecture added</li> <li>- Chapter 5 (Session level security) has been reworked and updated</li> <li>- Appendix A has been updated with a Quadtree common algorithm specification</li> <li>- New Appendix E now includes a description of the technical solution for a Governing Body and the different trust domains</li> </ul>	Final
2.0.1	7.10.2021	Based on SC meeting on 7.10.2021	Final

		<p>Release 2.0.1 is accepted for C-ROADS deployment by all member states. This is the seventh version of the document which means that all changed and new requirements have /7.</p> <p>Changes compared to 2.0</p> <ul style="list-style-type: none"> <li>- New requirements on logging to facilitate trouble-shooting and cross-border testing</li> </ul> <p><b>Possibility to have more than one broker</b></p>	
2.0.2	16.12.2021	<p>Based on SC meeting on 16.12.2021 Release 2.0.2 is accepted for C-ROADS deployment by all member states. This is eighth version of the document which means that all changed and new requirements have /8</p> <p>Changes compared to 2.0.1</p> <ul style="list-style-type: none"> <li>- Minor updates related to corrections and terminology to align to AMQP specification</li> </ul>	Final
2.0.4	15.06.2022	<p>Based on SC meeting on 15.06.2022 Release 2.0.4 is accepted for C-ROADS deployment by all member states. This is ninth version of the document which means that all changed and new requirements have /9.</p> <p>Changes compared to 2.0.2 (Note: Version 2.0.3 does not exist)</p> <ul style="list-style-type: none"> <li>- Table for filtering on CAM is added</li> <li>- Improvements and corrections to specification based upon feedback from testing and deployments</li> </ul>	Final
2.0.5	4.10.2022	<p>Based on SC meeting on 4.10.2022 Release 2.0.5 is accepted for C-ROADS deployment by all member states. This is tenth version of the document which means that all changed and new requirements have /10</p> <p>Changes compared to 2.0.4</p> <ul style="list-style-type: none"> <li>- Type for CauseCode and subCauseCode in Table 2 and Table 7 is changed from string to integer</li> <li>- Improvements and corrections to specification based upon feedback from testing and deployments</li> </ul>	Final
2.0.6	13.12.2022	<p>Based on Steering Committee meeting on 13.12.2022 release 2.0.6 is accepted for C-ROADS deployment by all member states.</p>	Final

		<p>This is the eleventh version of the document which means that all changed and new requirements have /11</p> <p>Changes compared to 2.0.5</p> <ul style="list-style-type: none"> <li>- Improvements to specification based upon feedback from testing and deployments</li> <li>- A new function called “Sharding” introduced which will allow for horizontal scaling (adding more capacity) and still guarantee in-order delivery of C-ITS messages</li> </ul>	
2.0.8	20.06.2023	<p>Based on Steering Committee meeting on 20.06.2023 release 2.0.8 is accepted for C-ROADS deployment by all member states.</p> <p>This is the twelfth version of the document which means that all changed and new requirements have /12</p> <p>Changes compared to 2.0.6 (Note: Version 2.0.7 does not exist)</p> <ul style="list-style-type: none"> <li>- Improvements on hybrid system monitoring and data-logging procedures</li> <li>- TTL (TimeToLive) requirement have been updated</li> <li>- Namespacing requirements have been added</li> <li>- Redirect policy requirements have been added</li> </ul>	Final

## Table of Contents

1	Introduction.....	9
1.1	C-Roads platform for harmonization of C-ITS deployment .....	9
1.2	Story board C-Roads C-ITS deployment documentation .....	10
1.3	Scope of this document.....	11
1.4	Verbal forms of the expression of provisions .....	11
1.5	Definitions .....	12
1.6	References .....	13
1.7	Numbering and version handling of requirements .....	14
2	Overview of C-ITS communication.....	14
3	Basic Interface - IP based interface for backend communication .....	15
3.1	Introduction .....	15
3.1.1	Central C-ITS station architecture for Basic Interface .....	16
3.2	Functional requirements.....	18
3.3	BI protocol specification .....	21
3.3.1	Payload requirements .....	22
3.3.2	Filtering mechanism .....	23
3.3.3	Configuration parameters.....	29
3.3.4	Location specification .....	30
3.3.5	Application requirements.....	31
4	Improved Interface - IP based interface for backend communication .....	32

4.1	Introduction .....	32
4.2	Functional requirements.....	33
4.3	Improved Interface protocol specification .....	35
4.3.1	Certificates .....	36
4.3.2	DNS configuration.....	36
4.3.3	Interchange discovery .....	37
4.3.4	Control channel establishment .....	37
4.3.5	Capabilities exchange .....	38
4.3.6	Subscription exchange .....	42
5	Session level security .....	51
5.1	Introduction .....	51
5.2	Common TLS profile .....	52
5.3	BI – BI TLS profile.....	52
5.4	BI / II TLS profile .....	53
6	Appendix A – Quadtree .....	53
7	Appendix B – Deployment Models.....	56
8	Appendix C – Capabilities exchange JSON format.....	57
9	Appendix D – Subscription exchange JSON format.....	59
10	Appendix E – Session level security and governance.....	62
11	Appendix F – Pilot testing information.....	64
11.1	Basic Interface Registry .....	64
11.2	BI Bilateral pilot testing.....	64
11.3	II Pilot Governance .....	64
11.4	Test logging format .....	64
12	Appendix G – Sharding.....	65
13	Appendix H – Deleted requirements .....	68

## Acronyms/explanations

AMQP	Advanced Message Queueing Protocol
APACHE	The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software, released under the terms of Apache License2.0.
avc	automated vehicle container
BI	Basic Interface
C-ITS	Cooperative Intelligent Transport Systems
CAM	Cooperative Awareness Message
CRL	In cryptography, a Certificate Revocation List (or CRL) is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.
DENM	Decentralized Environmental Notification Message
ETSI	European Telecommunications Standards Institute
EU	European Union
GHz	Gigahertz
GIS	Geographical Information System: is a system designed to capture, store, manipulate, analyze, manage, and present spatial or geographic data.
GNSS	Global Navigation Satellite System, system used for positioning.
HLN-RLX	Hazardous Location Notification - Railway Level Crossing
hop	In computer networking, including the Internet, a hop occurs when a packet is passed from one network segment to the next. Data packets pass through routers as they travel between source and destination. The hop count refers to the number of intermediate devices through which data must pass between source and destination. Since store and forward and other latencies are incurred through each hop, a large number of hops between source and destination implies lower real-time performance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IEC	International Electrotechnical Commission
IEEE 802.11	See IEEE 802.11P
IEEE 802.11p	IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication system. It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure, so called V2X communication, in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz).
IP	Internet Protocol
IPv4	Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet. IPv4 is described in IETF publication RFC 791.

IPv6	Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). IPv6 is intended to replace IPv4.
ISO	International Organisation for Standardization
IETF	Internet Engineering Task Force is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). It has no formal membership or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.
II	Improved Interface
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). ITS-G5 uses the approved amendment of the IEEE 802.11 (standard IEEE 802.11p). This technology (possibly others) uses the 5.9 GHz frequency band to support safety- and non-safety ITS applications.
IVI	Infrastructure to Vehicle Information
IVIM	Infrastructure to Vehicle Information Message
KB	Kilobyte
MAPEM	MAP (topology) Extended Message
m	Metre
ms	Milliseconds
MS	Member State
OCSP	The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP.
OEM	Original Equipment Manufacturer
OV	Organization Validated
PKI	A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
rcc	RoadConfigurationContainer
RFC	Request For Comments
RO	Road Operator
RTA	Road Traffic Authority
RSP	Roadside ITS-G5 System Profile (short also Roadside System Profile)
SPATEM	Signal Phase and Timing Extended Message
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message

SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.
TTL	Time to live (TTL) or hop limit is a mechanism that limits the lifespan or lifetime of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded or revalidated.
V2I	Vehicle-to-Infrastructure Communication; Information exchange between vehicles and infrastructure.
V2V	Vehicle to Vehicle Communication; information exchange between vehicles.
V2X	Vehicle-to-any communication; X is either infrastructure or car; Including communication between vehicles as well as between vehicles and infrastructure.
WAVE	Wireless Access in Vehicular Environments
WG2	Workgroup 2
WGS84	World Geodetic System is a standard used in cartography
Wi-Fi	Wi-Fi is a family of radio technologies commonly used for wireless local area networking (WLAN) of devices. It is based on the IEEE 802.11 family of standards.
WLAN	Wireless Local Area Network
X.509	In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.

e.g.	In Latin “exempli gratia” which stands for: “For Example”
i.e.	In Latin “id est” which stands for “In other words”
w.r.t.	With respect to

## List of Figures

Figure 1 Overview of C-Roads coverage .....	10
Figure 2 Highlight of WG2 document in complete story board .....	10
Figure 3 Overview of C-ITS communication.....	14
Figure 4 Basic IP interface for C-ITS message exchange .....	15



Figure 5 BI sequence overview .....	16
Figure 6 Central C-ITS station architecture for Basic Interface.....	17
Figure 7 Basic Interface sequence diagram .....	22
Figure 8 Evolved architecture for country/region information sharing .....	32
Figure 9 Sequence overview.....	33
Figure 10 Improved Interface procedure overview .....	36
Figure 11 Capabilities exchange sequence.....	38
Figure 12 Subscription exchange sequence .....	44
Figure 13 Deployment models .....	57
Figure 14 Session level PKI hierarchy .....	63
Figure 15 Examples of trust domain interactions .....	63

# 1 Introduction

## 1.1 C-Roads platform for harmonization of C-ITS deployment

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

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

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

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



Figure 1 Overview of C-Roads coverage

## 1.2 Story board C-Roads C-ITS deployment documentation

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

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

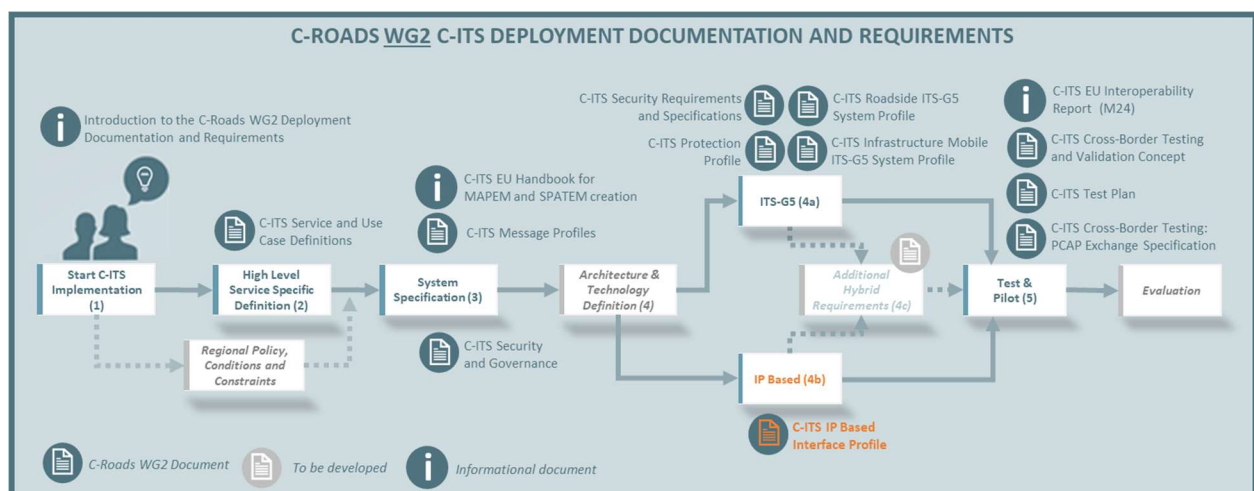


Figure 2 Highlight of WG2 document in complete story board

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

### 1.3 Scope of this document

This document covers 4b from C-Roads workflow in section 1.2. This document provides a description of the functionality and interface profiles which are needed to provide interconnection of backend systems to allow sharing of C-ITS information.

This document specifies the following:

#### Basic Interface - IP based interface for backend communication:

- Functional requirements
- Basic Interface protocol specification
- Filtering mechanism
- Configuration parameters
- Location specification
- Application requirements

#### Improved Interface - IP based interface for backend communication:

- Functional requirements
- Improved Interface protocol specification

#### Transport layer security

- Transport Layer Security profile
- Transport Layer Security Certificates

This document does not cover the payload content, i.e. the C-ITS message contents.

### 1.4 Verbal forms of the expression of provisions

In this document, the following verbal forms are used to indicate mandatory requirements:

Shall / Shall not

Recommendations shall be indicated by the verbal forms:

Should / Should not

Permissions shall be indicated by the verbal forms:

May / May not

Possibility and capability shall be indicated by the verbal forms:

Can / Cannot

Inevitability used to describe behavior of systems beyond of the scope of this deliverable shall be indicated by:

Will / Will not

Facts shall be indicated by the verbal forms:  
Is / Is not

## 1.5 Definitions

**C-ITS Actors** – entities or organisations which operate C-ITS stations and/or provide C-ITS services based on high quality traffic information. C-ITS actors have the responsibility to update their published and supported C-ITS messages.

**AMQP** (Advanced Message Queuing Protocol) – AMQP is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.

**AMQP broker** – An AMQP message broker is an architectural pattern for message routing. It mediates communication among applications, minimizing the mutual awareness that applications should have of each other in order to be able to exchange messages, effectively implementing decoupling. In this specification, an AMQP broker is used to route C-ITS messages.

**AMQP client** is an AMQP component configured as initiating the communication and receiving, and/or sending messages

**BI client** is an AMQP client configured to implement the BI interface

**Basic Interface (BI)** is the data communication interface used for real time exchange of C-ITS messages in the backend communication.

**Improved Interface (II)** – Provides a control plane between interchange entities for automation of discovery, subscription handling and to federate exchange of information between countries/regions.

**Deployment Model** is how a group of C-ITS actors decides to establish the information-sharing network, e.g. using a central AMQP broker(s) which interconnects multiple C-ITS actors, alternatively; information sharing between C-ITS actors can be based on multiple logical point-to-point connections directly between the C-ITS actors.

**Hybrid C-ITS** – Hybrid communication covers for transmission of C-ITS messages potentially using multiple communication channels; availability of such communication channels may vary depending on policy, location and requirements set.

**C-ITS messages** – signed messages defined by ETSI and ISO and profiled in the C-ROADS C-ITS Message Profiles.

**Third parties** – any organization which is contracted by a C-ITS Actor.

**Interchange entity** – Central hub in a C-ITS messaging network, implementing the Basic Interface (BI) and Improved Interface (II). It integrates an AMQP broker and an AMQP client.

**Capabilities** – Description of available data sets.

**Data sets** – Available information and meta-data

**Governing Body** – Trusted party responsible for the trust chain and registration of active entities (e.g. DNS registration). Organisational aspects are not covered by this specification

**Trusted Domain name** – Trusted registry of interchange entities approved by the relevant governing body.

**Endpoint** – The entry point to a service, a process, or a AMQP destination in service-oriented architecture

**BI repetition** – The repetition of AMQP message distribution over the BI

**GeoNetworking repetition** – The repetition of short-range C-ITS messages as indicated in the GeoNetworking layer of the message

**AMQP destination** – A destination is an object (a queue or a topic) that represents the target of messages that the client produces and the source of messages that the client consumes.

## 1.6 References

[1]	AMQP ISO/IEC 19464:2014
[2]	C-Roads C-ITS Message Profiles
[3]	C-Roads Roadside ITS G5 System Profile
[4]	AMQP Apache-filters-chapter 2: Java Message Service Support
[5]	RFC 8446 Transport Layer Security Protocol Version 1.3
[6]	RFC 6066 Transport Layer Security Extensions
[7]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[8]	ISO 3166-1:2013 alpha-2 Country Codes
[9]	ISO 14816:2005 Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure
[10]	ISO 14823:2017 Intelligent transport systems – Graphic data dictionary
[11]	ISO/TS 19321:2015 Intelligent transport systems – Cooperative ITS – Dictionary of in-vehicle information (IVI) data structures
[12]	ETSI EN 302 637-3 V1.3.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
[13]	ETSI TS 103 301 V1.3.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
[14]	RFC 2616 Hypertext Transfer Protocol – HTTP/1.1
[15]	RFC 2818 HTTP over TLS (HTTPS)
[16]	C-Roads Common C-ITS Service and Use Case Definitions





Upper left part shows the solution area related to the communication of C-ITS messages between backend entities, addressed by this document. Following this part, all types of backend entities are connected by communication links.

Lower left part shows the solution area related to communication between a backend entity and the end-user application and this communication can be performed following different commercial/national strategies.

Upper right shows road operators network implementation choices to realize C-ITS services in ITS-G5 [3].

Lower right shows the ITS-G5 communication [3].

## 3 Basic Interface - IP based interface for backend communication

### 3.1 Introduction

The C-ITS actors typically operate in one country/region and share information to/from clients. They connect to entities in the relevant country to consume and provide information. To allow information sharing, an Interface/protocol named **BI (Basic Interface)** is specified between C-ITS actors (and their potential third parties), see figure 4.

BI is independent of any deployment model that Member States or C-ITS actors choose to deploy.

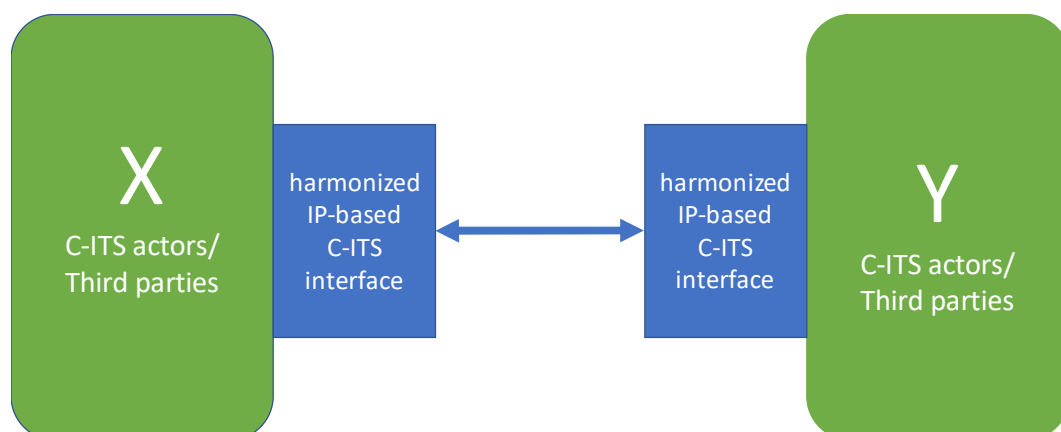


Figure 4 Basic IP interface for C-ITS message exchange



Figure 5 illustrates the flow of the BI implementation, further details on the procedures can be found in this chapter. Further details on deployment models can be found in appendix B.

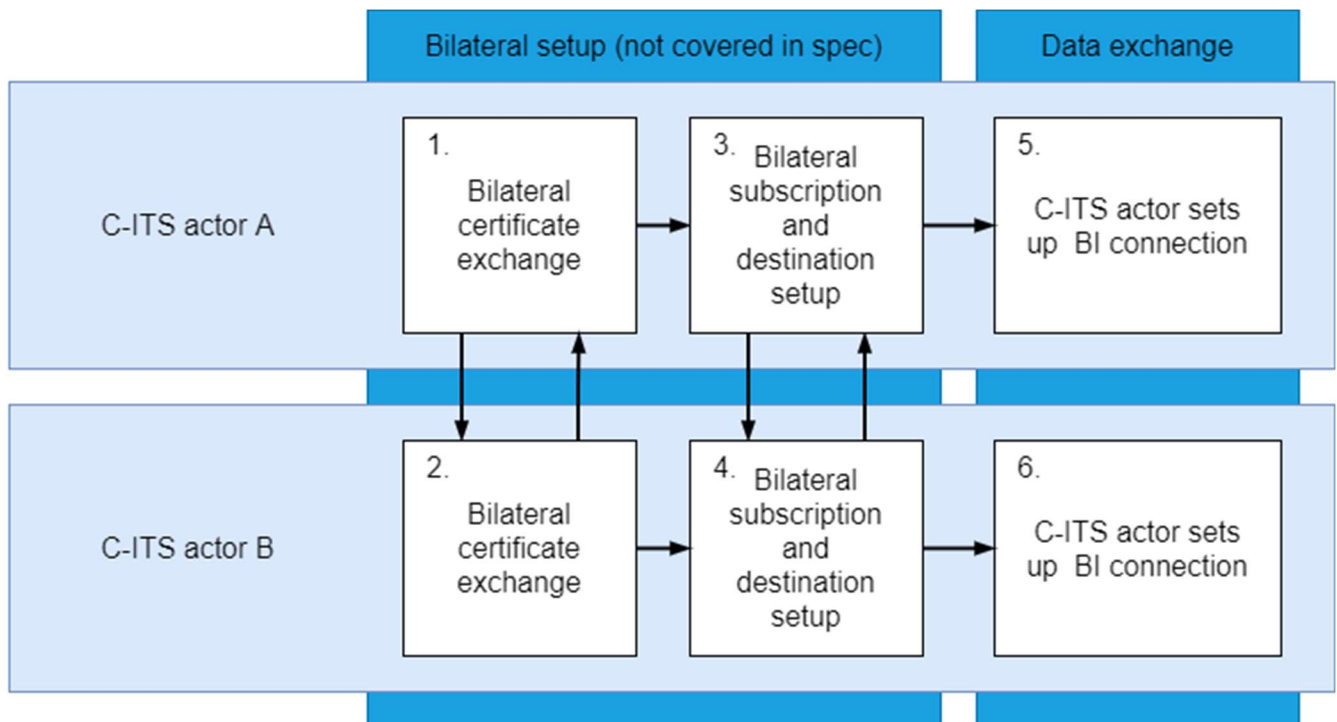


Figure 5 BI sequence overview

Additional information:

The above BI set up between any two C-ITS actors can be achieved via manual configuration. To set up BI manually, the C-ITS actors need to bilaterally agree on the following minimum information:

- TLS certificates to use for BI
- AMQP endpoints information (e.g. URL, IP-address)
- Use-case specific information to be exchanged (e.g. message types, protocol versions)
- Geographic coverage (e.g. Quadtree information)

BI Registry template available in appendix F.

### 3.1.1 Central C-ITS station architecture for Basic Interface

This section provides an overview of the C-ITS station architecture with an integrated BI client for backend communication. It especially describes the API between a Central C-ITS station and a BI client for backend communication. It defines the details of the harmonised IP-based C-ITS interface from figure 4.

# Central C-ITS station architecture for Basic Interface

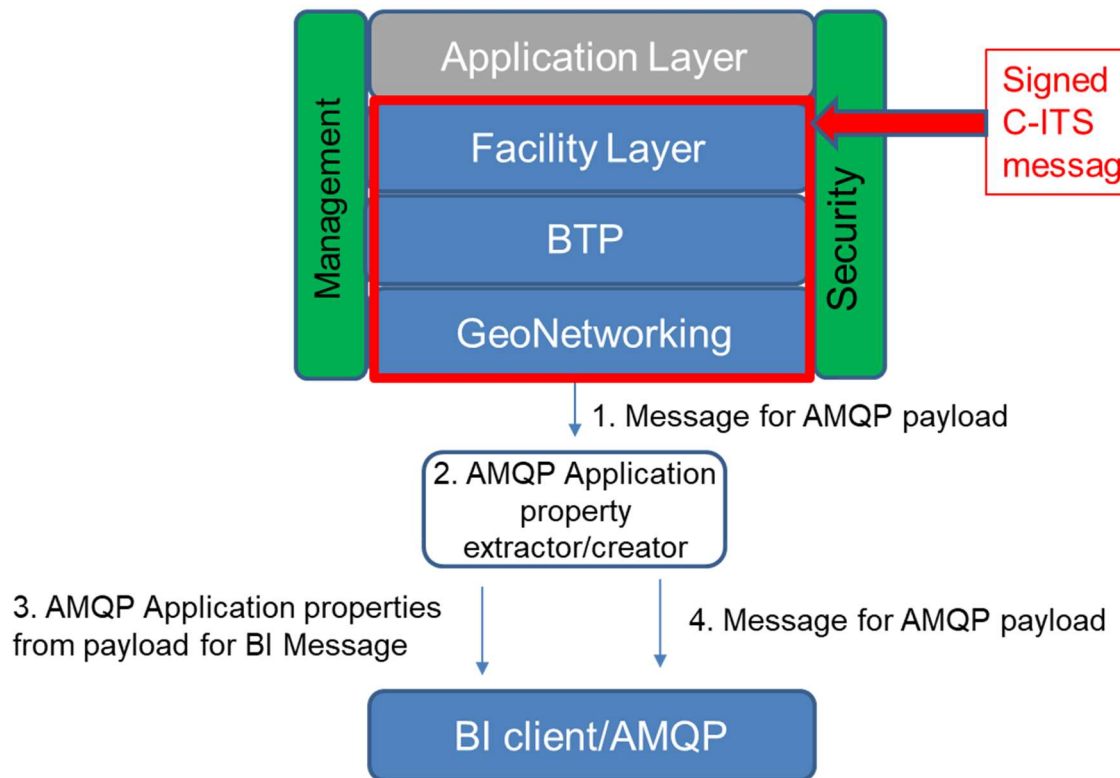


Figure 6 Central C-ITS station architecture for Basic Interface

If a C-ITS message is valid now or in the future, the content will be sent with a suitable repetition interval via the BI Interface as specified in requirement IP\_114.

1. The output from a Central C-ITS station is the payload part of an AMQP message.
2. Out of the payload message, the information required to populate the AMQP application properties needs to be created/extracted, see section 3.3.1 for AMQP application properties

Additional information: The AMQP application properties might be easier extracted from the message on the facility layer or even higher protocol layers.

3. The extracted or newly created AMQP properties are passed to the BI client to be used in the generation of the AMQP message.
4. The C-ITS message is passed to the BI client for inclusion as payload within the AMQP message.

## 3.2 Functional requirements

### *Requirement IP\_001/1*

- BI shall be used by all C-ITS actors for cross border C-ITS message exchange.

### *Requirement IP\_002/1*

- BI should be used by all C-ITS actors on national level.

### *Requirement IP\_003/1*

- BI shall be able to exchange C-ITS messages in a secured connection.

Additional information: See chapter 5 Session level security for more information

### **Functional needs of C-ITS actors:**

### *Requirement IP\_004/8*

- BI shall allow C-ITS actors to send and receive C-ITS messages.

### *Requirement IP\_005/1*

- BI shall allow to filter C-ITS messages according to chapter 3.3.

### *Requirement IP\_006/1*

- BI shall allow to route C-ITS messages according to chapter 3.3.

### *Requirement IP\_007/1*

- Time synchronization  
All C-ITS actors shall be time synchronized with an accuracy equivalent to a stratum 1 level.

### *Requirement IP\_008/1*

- Filtering by AMQP brokers shall be done without reading the AMQP payload (Reference to AMQP ISO/IEC 19464:2014 [1]).

### **Monitoring of message exchange and logging**

For operational monitoring of quality of service some set of parameters should be available to the broker operator.

This information should at least include

- Number of parallel message queues
- Number of messages in a queue (routable/unroutable - if available)
- Messages per second (message throughput)
- Application vitals (CPU load, memory, disk space, . .)

- Number of connections

This information can be used in dashboards and alarms.

To enable in-depth debugging, validation and testing, additional logging can be enabled as needed internally or based upon a request from other C-ITS actors.

Logging should be possible at four levels and the respective processing of logging files is defined as follows

- Debug (you should be able to activate storage)
- Info (you should be able to activate storage)
- Warning (you should activate storage for all warnings)
- Error (you shall activate storage for all errors and monitor them)

#### *Requirement IP\_009/12*

- Servers (both brokers and clients) shall be able to turn on logging of the following
  - Source filters
  - Client connect and disconnects
  - System and connection errors

#### *Requirement IP\_010/12*

- Servers (both brokers and clients) shall be able to turn on logging of the following for message types DENM, IVIM, SREM, SSEM, MAPEM:
  - AMQP Message timestamps precision of at least 1ms (Both arrival and departure)
  - AMQP Message application properties field except application data

#### *Requirement IP\_011/12*

- Servers (both brokers and clients) shall be able to turn on logging of the following for message types SPATEM, CAM:
  - AMQP Message timestamps precision of at least 1ms (Both arrival and departure)
  - AMQP Message application properties field except application data

#### *Requirement IP\_119/7*

- Servers (both brokers and clients) shall be able to turn on logging of AMQP message properties for sent and received messages.

#### *Requirement IP\_120/7*

- Servers (both brokers and clients) shall be able to turn on inclusion of application data (payload) in the log in Requirement 119/7.

#### *Requirement IP\_121/7*

- Logging format shall be JSON format.

Additional information for Requirements IP\_009, IP\_010, IP\_011, IP\_119, IP\_120 and IP\_121: This is to facilitate troubleshooting and testing, logging does not need to be turned on all the time. Turning on additional logging can be initiated by an internal need or an external need (e.g. other C-ITS actors or other interchange operators).

Logging format exemplified in appendix F.

## Latency requirements for AMQP brokers

### *Requirement IP\_012/8*

- A broker shall be able to route a single message with a payload size <500KB in <30ms, defined as the time interval from message arrival (on broker target) to message availability (on broker source).

### *Requirement IP\_013/8*

- A broker shall be able to route 5000 messages with a payload size <500KB in <1000ms, defined as the time interval from message arrival (on broker target) to message availability (on broker source).

Additional information:

Note that for high intensity information, e.g. SPAT, the minimum required throughput can be substantially higher. In that case the broker may handle the corresponding additional load by using a free choice of scaling mechanisms, e.g. vertical scaling (increasing e.g. the CPU and memory resources of the broker), horizontal scaling (dividing the load over multiple broker instances, can be automated with assistance of the II interface), etc.

## Integrity requirements for AMQP brokers

### *Requirement IP\_014/1*

- A broker shall never remove, alter or add anything to a message payload.

### *Requirement IP\_015/2*

- A broker shall never remove or alter any of the AMQP application properties field.

### *Requirement IP\_016/2*

- A broker should drop malformed AMQP messages that do not adhere to this specification or any extension of it and shall log the event.

## In-order delivery

### *Requirement IP\_128/11*

- If an Interchange opts to support in-order delivery of AMQP messages, that Interchange can realize this by not delivering messages with the same shardId out-of-order. In such

case, if no shardId is added to the message, that should be interpreted as if all messages belonging to the same capability have the same shardId (shardId = 1 and shardCount = 1).

Additional information on sharding can be found in appendix G “Sharding”

#### *Requirement IP\_129/11*

- Interchange entities that want to support in-order delivery of AMQP messages can only horizontally scale capabilities if they have a shardCount > 1 defined in their capability descriptor.

Additional information:

In-order delivery means that when a producer publishes messages in a certain time sequence on an Interchange (based on the time at which the message was published on the Interchange), that a consumer of these messages receives them in the same time sequence from the same or another Interchange.

### 3.3 BI protocol specification

**BI (Basic Interface)** is the interface between C-ITS actors and/or interchange entities. On this interface the protocols and profiles, specified below, shall be used for C-ITS services. This section provides information how AMQP shall be used, also external resources need to be consulted, e.g. Advanced Message Queuing Protocol (AMQP) specification.

BI can allow exchanging non C-ITS messages, outside the C-ITS domain.

Basic Interface sequence diagram covered in this sub-chapter, is shown in figure 7. Detailed technical requirements are covered by the referenced sections.

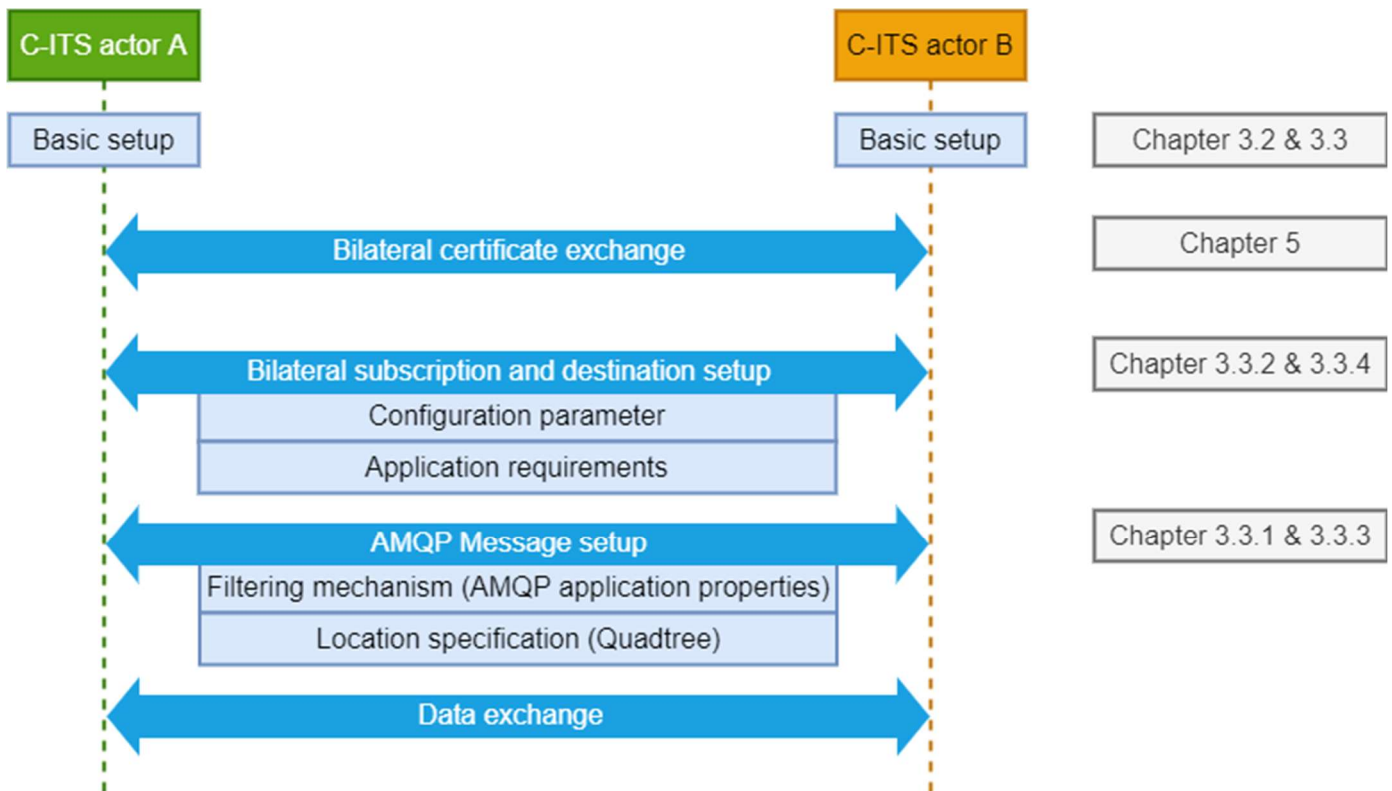


Figure 7 Basic Interface sequence diagram

#### Requirement IP\_018/1

- BI shall use Internet Protocol (IPv4) and Transmission Control Protocol (TCP).

#### Requirement IP\_019/1

- BI shall implement Transport Layer Security (TLS 1.3) according to RFC 8446 [5]. Profiling for TLS is described in chapter 5.

#### Requirement IP\_020/1

- BI shall use AMQP version 1.0 (ISO IEC 19464 [1]).

### 3.3.1 Payload requirements

#### Requirement IP\_118/8

The payload of an AMQP Message shall be encoded in binary format and put in a single AMQP Data binary data section.

Additional information: Different parts of message are encoded using different rules and standards, see relevant ETSI standards for C-ITS messages.

### 3.3.2 Filtering mechanism

#### *Requirement IP\_066/2*

- All AMQP Clients and Brokers shall be compatible with Apache Selector filters as the filtering mechanism to ensure interoperability

Additional information:

For more information on Selector filters AMQP Apache-filters-chapter 2: Java Message Service Support [4]

<https://svn.apache.org/repos/asf/qpid/trunk/qpid/specs/apache-filters.xml#type-selector-filter>

Filters used will be case sensitive

Examples for filtering:

For filtering C-ITS messages based on quadtree tiles:

"quadTree LIKE '%,031333110%' OR quadTree LIKE '%,031333111%' OR quadTree LIKE '%,031333112%'"

For filtering C-ITS messages based on messageType and originatingCountry:

Filtering all DENM messages from France:

"messageType = 'DENM' AND originatingCountry = 'FR'"

#### *Requirement IP\_067/8*

- All AMQP Clients and Brokers shall support filtering on application properties as defined in Tables 1, 2, 3, 4, 5 and 6.

Additional information: Message filtering is only relevant when receiving from a source, not when sending to a target.

#### *Requirement IP\_131/12*

- If any additional application properties beyond the properties defined in this specification are used, they shall be name spaced according to the following pattern: custom-  
<unique\_namespace\_id>-<property\_name>  
To ensure the uniqueness of the namespace id, a project name and/or country name should be included in the id.

Additional information: The use of name spacing in specification extensions ensure compatibility with future revisions of this specification, and reduces the possibility of confusion when messages with extended properties are received by others

#### *Requirement IP\_022/2*

- All mandatory fields defined in Table 1 shall be inside the AMQP application properties field for all C-ITS messages.

#### *Requirement IP\_023/2*

- All optional fields defined in Table 1 should be inside the AMQP application properties field for all C-ITS messages.



### Requirement IP\_024/1

- Filtering shall be requested by consumer based on selected fields defined in Table 1, Table 2, Table 3, Table 4, Table 5 or Table 6.

*Table 1 : Data field and settings for filtering for all C-ITS messages*

Name	Value and type	Description	Mandatory/Optional
publisherId	string A two-letter country code (based on ISO 3166-1 alpha-2 [8]) and a numerical identifier (value between 0 and 16383 including leading zeroes) based on ISO 14816:2005 [9] (same as used for providerIdentifier in IVIM), e.g. "AT00001", "DE15608"	Unique ID of the publisher. It is Linked to the country where the provider wants to register. It could be in one country or several.	M
publicationId	String Concatenation of publisherId and a unique identifier for the dataset/publication with a ":" between, e.g. "DE15608:IVIM_BERLIN_067" or "NO73944:679ABX92"	publisherId defined in table 1. Each dataset/publication identifier needs to be unique for the given publisher. When using the II, the publicationId shall uniquely identify a single capability entry.	O (Mandatory when using II, see chapter 4)
originatingCountry	string Country code (based on ISO 3166-1 alpha-2 [8])	Country code where the C-ITS message is created	M
protocolVersion	string E.g. "DENM:1.3.1" or "IVIM:1.2.1"	Represent the version of standard used to create the message, i.e. for DENM the version of ETSI EN 302 637-3 [12], for IVIM, SPATEM the version of ETSI TS 103 301 [13]	M
serviceType	string Comma separated list starting and ending with a comma E.g. ",HLN-RLX," or ",SI-GLOSA,SI-SPTI," .....	Acronym of C-ITS use case(s) defined in latest version of Common C-ITS Service and Use Case Definitions [16]	O
baselineVersion	String E.g. "1.8.0"	The baseline version indicates which release of the C-Roads specifications were	O

		used to create the C-ITS message	
messageType	string DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, CAM	For this version of the specification the string shall be one of the following: DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, and CAM. The list may be subject to changes in future versions of the specification	M
longitude	float Decimal degrees According to WGS84/EPSSG:4326	Longitude of the event published; for DENM (eventPosition) and for IVI and SPATEM/MAPEM/SSEM/SREM (referencePosition)	O
latitude	float Decimal degrees According to WGS84/EPSSG:4326	Latitude of the event published; for DENM (eventPosition) and for IVI and SPATEM/MAPEM/SSEM/SREM (referencePosition)	O
quadTree	string Comma separated list of quadtree tiles starting and ending with a comma, e.g. "202320120232120101," (single value) or "202320120232120101,202320120232120102,202320120232120103," (multiple values chained)	Relevant spatial index location of the C-ITS message	M
shardId	integer	The shard number of the current message if sharding is enabled for the capability for the message. <u>The id starts at 1 and the highest id is equal to the shardCount.</u> See appendix G "Sharding" for more details	O (but mandatory if sharding is enabled by message producer)
shardCount	integer	Defines the amount of shards for the capability. See appendix G "Sharding" for more details.	O (but mandatory if sharding is enabled by

			message producer)
--	--	--	-------------------

#### Requirement IP\_026/2

- All mandatory fields defined in Table 2 shall be inside AMQP application properties field for DENM messages.

Table 2 : Data field and settings for DENM filtering process

Name	Value and type	Description	Mandatory/Optional
causeCode	integer	CauseCode from ETSI_EN_302_637-3 [12]	M
subCauseCode	integer	subCauseCode from ETSI_EN_302_637-3 [12]	M

#### Requirement IP\_029/2

- All optional fields in Table 3 should be inside AMQP application properties field for IVIM messages.

Table 3 : Data field and settings for IVI filtering process

Name	Value and type	Description	Mandatory/Optional
iviType	string Comma separated list starting and ending with a comma, e.g. “,1,” (single value) or “,1,0,2,” (multiple values chained) as an IVIM may contain more than one iviType	iviType	O
pictogramCategoryCode	string Comma separated list starting and ending with a comma, e.g. “,557,” (single value) or “,557,559,612,” (multiple values chained) as an IVIM may contain more than one pictogramCategoryCode	The ISO 14823:2017 [10] pictogramCategoryCode is a combined numeral value (nature and serialNumber) referring to a specific sign of the ISO 14823:2017 [10] sign catalogue, e.g. 557 = Maximum speed limit	O

iviContainer	string All valid IviContainer abbreviations in the ISO 19321 standard starting and ending with a comma, e.g. ",giv," or ",rcc," or ",tc," or ",avc," (single values) or comma separated combinations of that, e.g. ",giv,tc,avc," (multiple values chained)	All valid IviContainer types out of the ISO 19321:2015 [11] standard that should be present in the target IVIM after applying filtering	O
--------------	--	---	---

#### Requirement IP\_100/3

- All optional fields defined in Table 4 should be inside the AMQP application properties field for SPATEM and MAPEM messages.

Table 4 : Data field and settings for SPATEM and MAPEM filtering process

Name	Value and type	Description	Mandatory/Optional
id	string Comma separated list starting and ending with a comma, e.g. ",5-57," (single region-id) or ",5-57,5-59,6-12," (multiple region-id chained) . Could be a list as an SPATEM/MAPEM may contain more than one id.	(IntersectionReferenceID) The combination of region and id (i.e region-id) must be unique within a country. Reference: C-Roads C-ITS Message Profiles [2]	O
name	String Comma separated list starting and ending with a comma, e.g. ",name1," (single value) or ",name1,name2,name3," (multiple values chained). Could be a list as an SPATEM/MAPEM may contain more than one name.	Typically human readable and recognizable by road authority.	O

#### Requirement IP\_103/3

- All optional fields defined in Table 5 should be inside the AMQP application properties field for SREM and SSEM messages.

*Table 5 : Data field and settings for SREM and SSEM filtering process*

Name	Value and type	Description	Mandatory/ Optional
id	string Comma separated list starting and ending with a comma, e.g. “,5-57,” (single region-id) or “,5-57,5-59,6-12,” (multiple region-id chained) . Could be a list as an SPATEM/MAPEM may contain more than one id.	(IntersectionReferenceID) The combination of region and id (i.e region-id) must be unique within a country. Reference: C-Roads C-ITS Message Profiles [2]	O

*Requirement IP\_122/9*

- All mandatory fields defined in Table 6 shall be inside the AMQP application properties field for CAM messages

*Requirement IP\_123/9*

- All optional fields defined in Table 6 should be inside the AMQP application properties field for CAM messages

*Table 6 : Data field and settings for CAM filtering process*

Name	Value and type	Description	Mandatory/ Optional
stationType	integer Values between 0 -15	As defined in ETSI_TS_102_894-2	M
vehicleRole	integer Values between 0 -12	As defined in ETSI_TS_102_894-2	O

*Requirement IP\_124/9*

- The frequency of CAM message distribution over BI shall be between 1 per second and 1 per 120 seconds

Additional information: The parameters of CAM message distribution (e.g. frequency, amount of messages) over BI would be based upon supported use-cases, numbers of relevant stations and area of message distribution for each implementation in order to control overall message load.

#### *Requirement IP\_031/1*

- C-ITS actors who want to publish information on BI shall register for EN ISO 14816:2005 [9] Road transport and traffic telematics - Automatic vehicle and equipment identification - Numbering and data structures, in order to obtain the mandatory publisherId as described in Table 1. More information about registration is available in the following references:

<https://www.tc278.eu/index.php/14816-register>

<https://www.tc278.eu/index.php/14816-registers>

Additional information:

Unless otherwise assigned during testing, a default value of [country code] + maximum value possible should be used for the publisherId.

### **3.3.3 Configuration parameters**

#### *Requirement IP\_032/1*

- A broker shall provide a buffer with a size of minimum 200 messages.

#### *Requirement IP\_033/12*

- An AMQP Message TTL (in seconds) shall be set to the BI repetition interval of the message (in seconds) multiplied by 1.2 with a minimum value of 1 second. A broker can directly enforce TTL policies, i.e. if TTL is not set, or dependent on message types.

#### *Requirement IP\_034/8*

- Brokers may set policies for destinations and shall make them available in the documentation.

#### *Requirement IP\_035/1*

- Systems that provide data shall be able to support multiple simultaneous receivers of the same data type.

#### *Requirement IP\_036/1*

- Consumers of data shall be able to receive data from different providers simultaneously.

### 3.3.4 Location specification

#### *Requirement IP\_037/1*

- Geolocation method shall be based on quadtree, where each quadtree zoomlevel shall be represented by a single character in the string. For complete description please see Appendix A.

#### *Requirement IP\_038/1*

- C-ITS actors shall publish AMQP messages with a minimum quadtree zoom level of 18 for the geographic reference location of the C-ITS message (e.g. referencePosition in IVIM and CAM, eventPosition in DENM, or refPoint in MAPEM).

Additional information: Zoom level refers to the length of the quadtree string, i.e. the individual quadtree strings used shall have a minimum number of characters of 18.

#### *Requirement IP\_112/5*

- Additional to IP\_038, C-ITS actors shall publish AMQP messages with a set of tiles with a minimum quadtree zoom level 13 covering detectionZone, relevanceZone for IVIM and traces, eventHistory for DENM as well as the GeoNetworking destinationArea for both IVIM and DENM.

Additional information: A destinationArea of up to 5 km radius is covered by a maximum set of 36 tiles at zoom level 13. Zoom level refers to the length of the quadtree string, i.e. the individual quadtree strings used shall have a maximum number of characters of 13.

For examples on how to filter based on quadtree tiles, see additional information for IP\_066

#### *Requirement IP\_113/5*

- Additional to IP\_038, C-ITS actors shall publish AMQP messages with a set of tiles with a minimum quadtree zoom level of 14 covering the GeoNetworking destinationArea of SPATEM, MAPEM, SSEM and SREM.

Additional information: A destinationArea of up to 1 km radius is covered by a maximum set of 9 tiles at zoom level 14. Zoom level refers to the length of the quadtree string, i.e. the individual quadtree strings used shall have a maximum number of characters of 14.

For examples on how to filter based on quadtree tiles, see additional information for IP\_066

#### *Requirement IP\_039/1*

- C-ITS actors shall filter with a maximum zoom level of 18 for referencePosition.

Additional information: Zoom level refers to the length of the quadtree string, i.e. the individual quadtree strings used shall have a maximum number of characters of 18.

For examples on how to filter based on quadtree tiles, see additional information for IP\_066

### 3.3.5 Application requirements

#### *Requirement IP\_044/1*

- The originating C-ITS station shall provide GeoNetworking layer parameters consistent with the reference location of the message.

#### *Requirement IP\_045/1*

- PacketLifetime in GeoNetworking layer parameters should be compliant with latency due to the channel and the meaning of the message.

#### *Requirement IP\_048/1*

- Each time a DENM or an IVIM is created and signed by C-ITS actors to be sent on BI , the message shall be repeated at least every 9 min if still valid.

Additional information:

Repetition is needed, since in vehicles, the allowed time window set in the security header is normally 10 minutes and is compared to message reception time, and if message received outside allowed time window, message is discarded.

#### *Requirement IP\_049/1*

- When a C-ITS actor receives an already signed DENM or IVIM (and their repetitions), it shall store the information for 9 min so it can repeat them through BI.

Additional information:

Within the 9 min interval, repeated messages can be ignored.

#### *Requirement IP\_104/3*

- C-ITS actors shall publish SPATEM only after corresponding MAPEM has been published

#### *Requirement IP\_111/4*

- C-ITS actors shall publish messages in a timely manner to enable other C-ITS actors to react to it in time.

#### *Requirement IP\_114/6*

- For any valid DENM or IVIM, the content shall be sent according to the requirements IP\_048 and IP\_049 via the BI Interface. For AMQP message distribution, GeoNetworking repetition interval shall not be taken into account.

#### *Requirement IP\_130/11*

- When publishing messages on a capability with shardCount > 1, the producing C-ITS actor publishing the message at an Interchange shall make sure that a shardId <= shardCount is provided to messages for which the producer opted that they should be delivered in-order.



Additional information on sharding can be found in appendix G “Sharding”.

## 4 Improved Interface - IP based interface for backend communication

### 4.1 Introduction

To facilitate a scalable solution, an Interface/protocol to automate service discovery and federate information between countries/regions is introduced, this interface/protocol is named **II (Improved Interface)** and provides a control plane for BI. This is needed to avoid manual configurations when data sources are added and to overcome the need for an ‘all to all’ full mesh of interconnections between the actors. The network scenario is exemplified below.

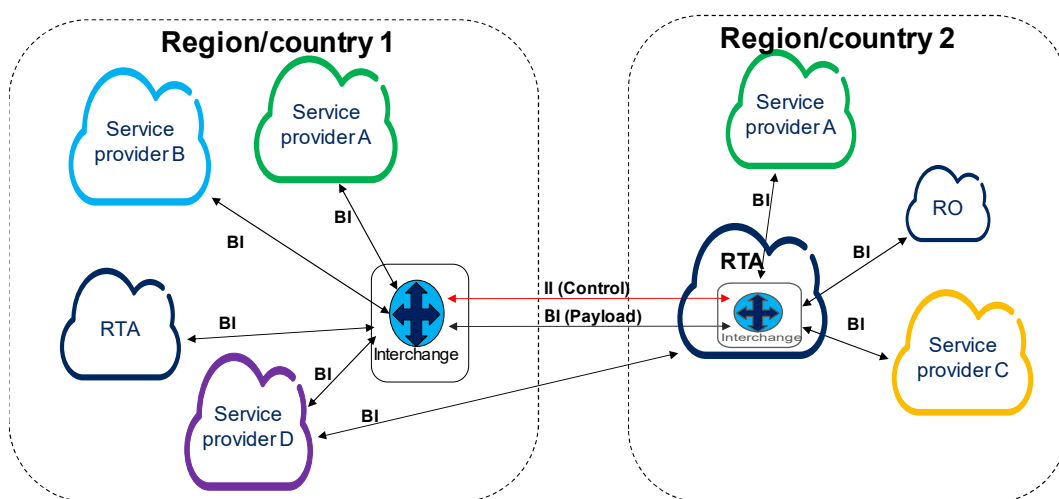


Figure 8 Evolved architecture for country/region information sharing

Figure 8 illustrates the flow of the Improved Interface implementation, further details on the procedures can be found in this chapter and appendix C and D. Further details on deployment models can be found in appendix B.

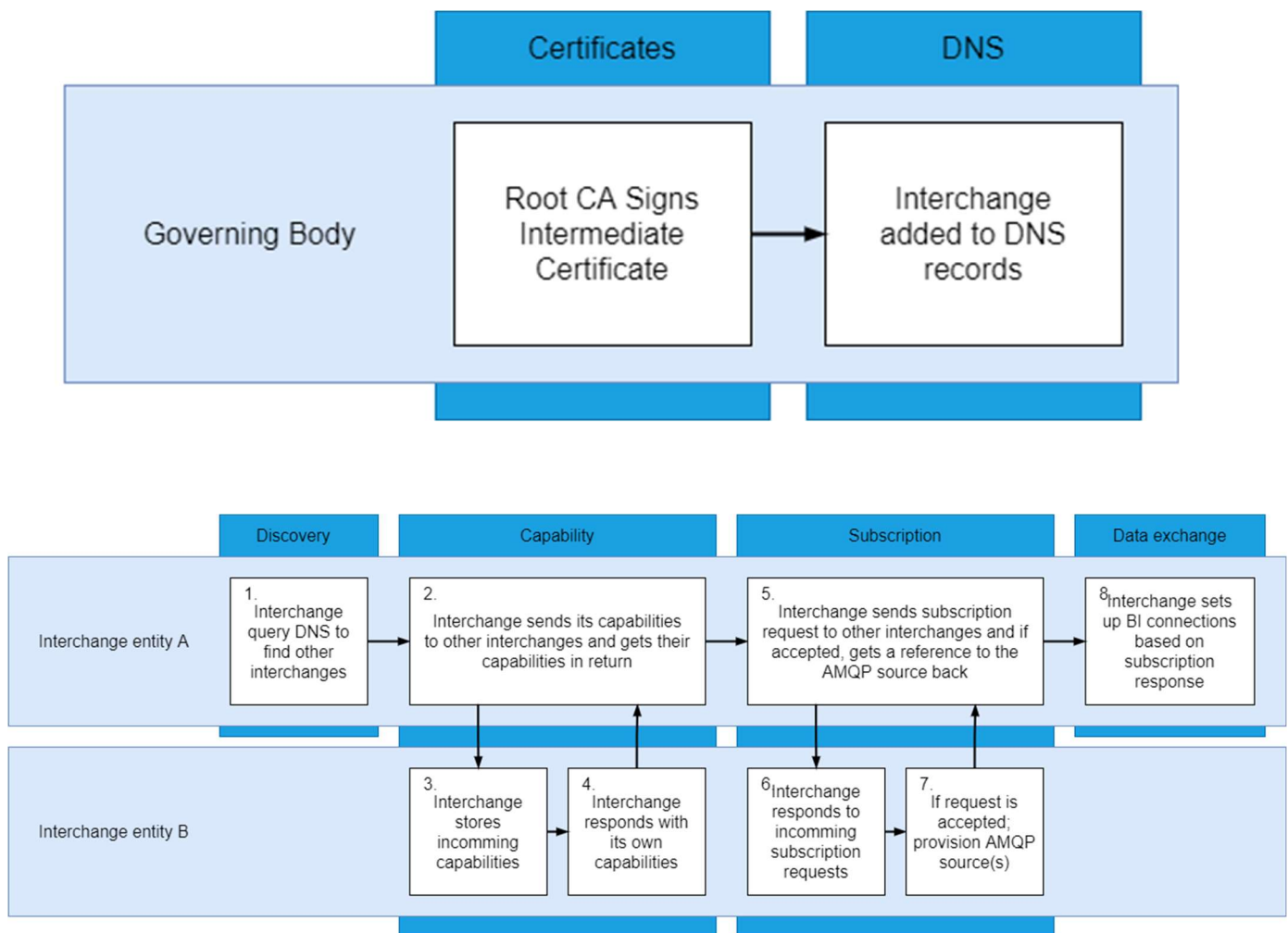


Figure 9 Sequence overview

## 4.2 Functional requirements

### General

#### Requirement IP\_068/3

- Improved Interface is an optional interface. If implemented it shall be used as control plane between interchange entities and the requirements in chapter 4 shall apply.

Additional information: Between an interchange entity and its clients, selected parts of Improved Interface may be implemented based upon a bilateral agreement, e.g. capability and subscription exchange

## **Certificates**

### *Requirement IP\_069/3*

- Security for Improved Interface shall be as described in chapter 5 Session level security.

## **DNS configuration**

### *Requirement IP\_072/3*

- The relevant governing body shall approve, handle registration and maintenance of interchange entities in the DNS.

### *Requirement IP\_071/3*

- Interchange entities shall be discoverable if registered as subdomain of a trusted domain name.

### *Requirement IP\_070/3*

- Interchange entities shall be registered in DNS as subdomain of a master trusted domain name (e.g. c-its-interchange.eu) or any other trusted domain name with the same trust/security level as the master domain name.

## **Interchange discovery**

### *Requirement IP\_073/3*

- Interchange entities shall automatically discover other interchange entities in the network based on a list of trusted domain names provided by the relevant governing body.

## **Control channel establishment**

### *Requirement IP\_074/3*

- An interchange entity shall establish a control channel to all other active interchange entities in the network to be able to share valid subscriptions and capabilities.

## **Capabilities exchange**

### *Requirement IP\_075/3*

- Interchange entities shall send updated capabilities to all other interchange entities.

### *Requirement IP\_076/3*

- Interchange entities shall receive and maintain capabilities from all other interchange entities.

#### *Requirement IP\_077/3*

- Interchange entities shall maintain updated capabilities of all their connected C-ITS actors (clients).

### **Subscription exchange**

#### *Requirement IP\_078/3*

- Interchange entities shall receive subscription requests from all other interchange entities.

#### *Requirement IP\_079/3*

- Interchange entities shall send subscription requests on behalf of their own C-ITS actors (clients) to other interchange entities.

#### *Requirement IP\_080/3*

- An interchange entity shall be able to redirect their C-ITS actors to other interchange entities where requested data is available, both for new subscriptions and for active data transfers between interchange entities.

#### *Requirement IP\_081/3*

- An interchange entity should be able to provide data available from other interchange entities to their C-ITS actors.

#### **Additional information:**

The interchange entity either fetch information available on other interchanges on behalf of its connected C-ITS actors or maintains information on where information is available and redirects its connected C-ITS actors to the data source.

#### *Requirement IP\_082/3*

- Interchange entities shall respond to subscription requests either by providing data or a rejection if the data is not available.

### **Data exchange**

#### *Requirement IP\_083/3*

- Interchange entities shall use Basic Interface for data exchange.

## **4.3 Improved Interface protocol specification**

Improved Interface sequence diagram covered in this sub-chapter, is shown in figure 10. Detailed technical requirements are covered by the referenced sections.

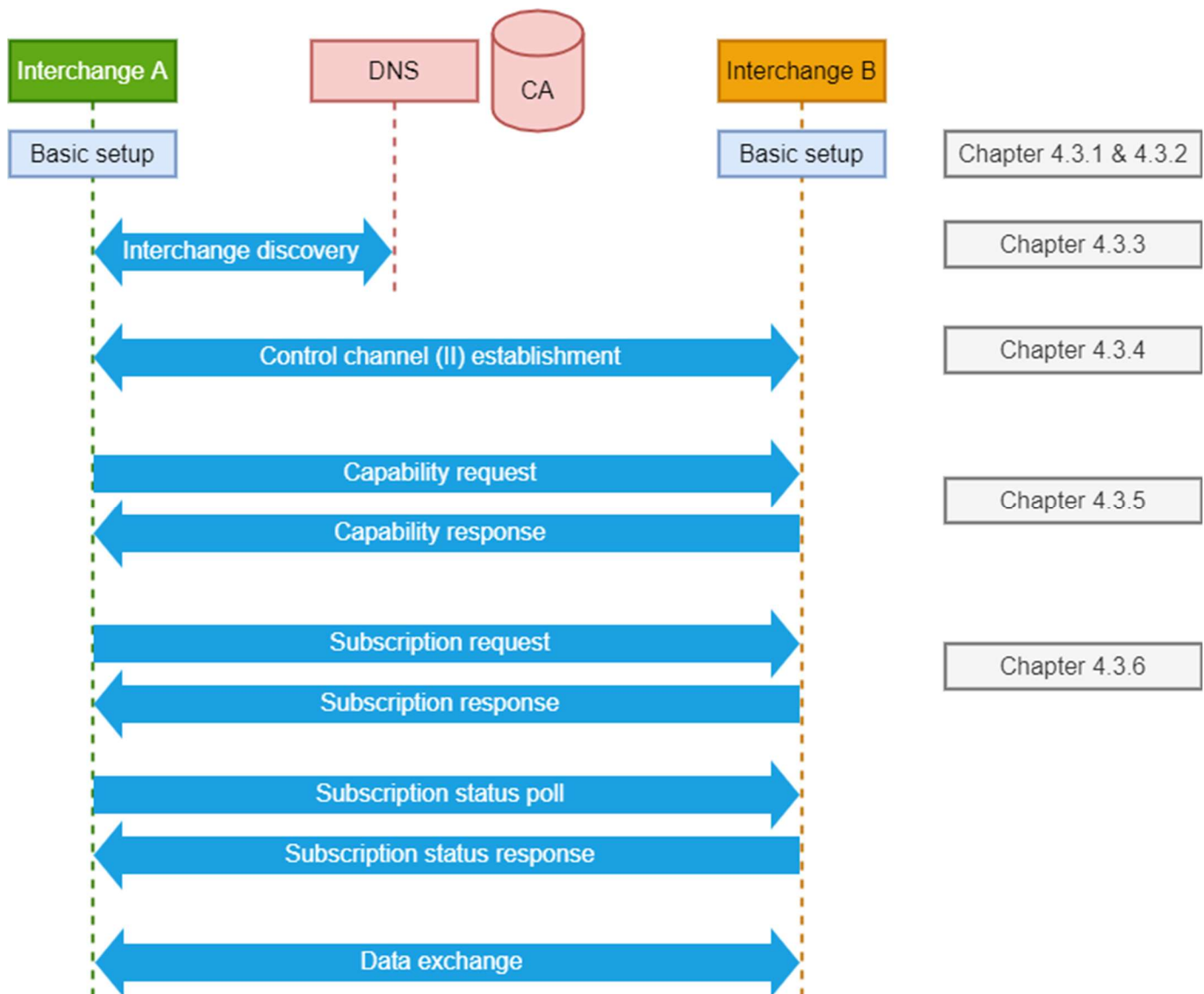


Figure 10 Improved Interface procedure overview

### 4.3.1 Certificates

#### Requirement IP\_084/3

- The relevant governing body shall handle the issuing of certificates and approval of trusted certificate authorities.

### 4.3.2 DNS configuration

#### Requirement IP\_085/3

- For any given Interchange entity an DNS A record shall be created in one of the trusted domain names.

#### *Requirement IP\_086/3*

- Each interchange entity shall have one DNS SRV record entry in one of the trusted domain names to identify the control channel. The symbolic name used shall be “IXC” for II.

#### *Requirement IP\_087/3*

- The target host name pointing to the Interchange entity in the SRV records shall be identical to the Interchange entities DNS A record.

#### *Requirement IP\_125/9*

- The common name of the certificates used by interchange entities shall match the target used in the DNS SRV record.

#### *Requirement IP\_088/3*

- The relevant governing body shall publish a list of trusted domain names.

### **4.3.3 Interchange discovery**

#### *Requirement IP\_089/3*

- An Interchange entity shall periodically, at least every 12 hours check for new and updated DNS SRV records with the symbolic name “IXC” on all trusted domain names to maintain an updated list of addresses and ports of other available interchange entities.

### **4.3.4 Control channel establishment**

#### *Requirement IP\_090/3*

- The control channel shall use HTTPS [15] with mutual authentication based on the allocated Interchange entity certificates, using the address and port obtained from the interchange discovery procedure.

#### *Requirement IP\_126/9*

- Interchange entities shall refuse any requests on the II for certificates with a Common Name not matching a target in the DNS SRV records.

### 4.3.5 Capabilities exchange

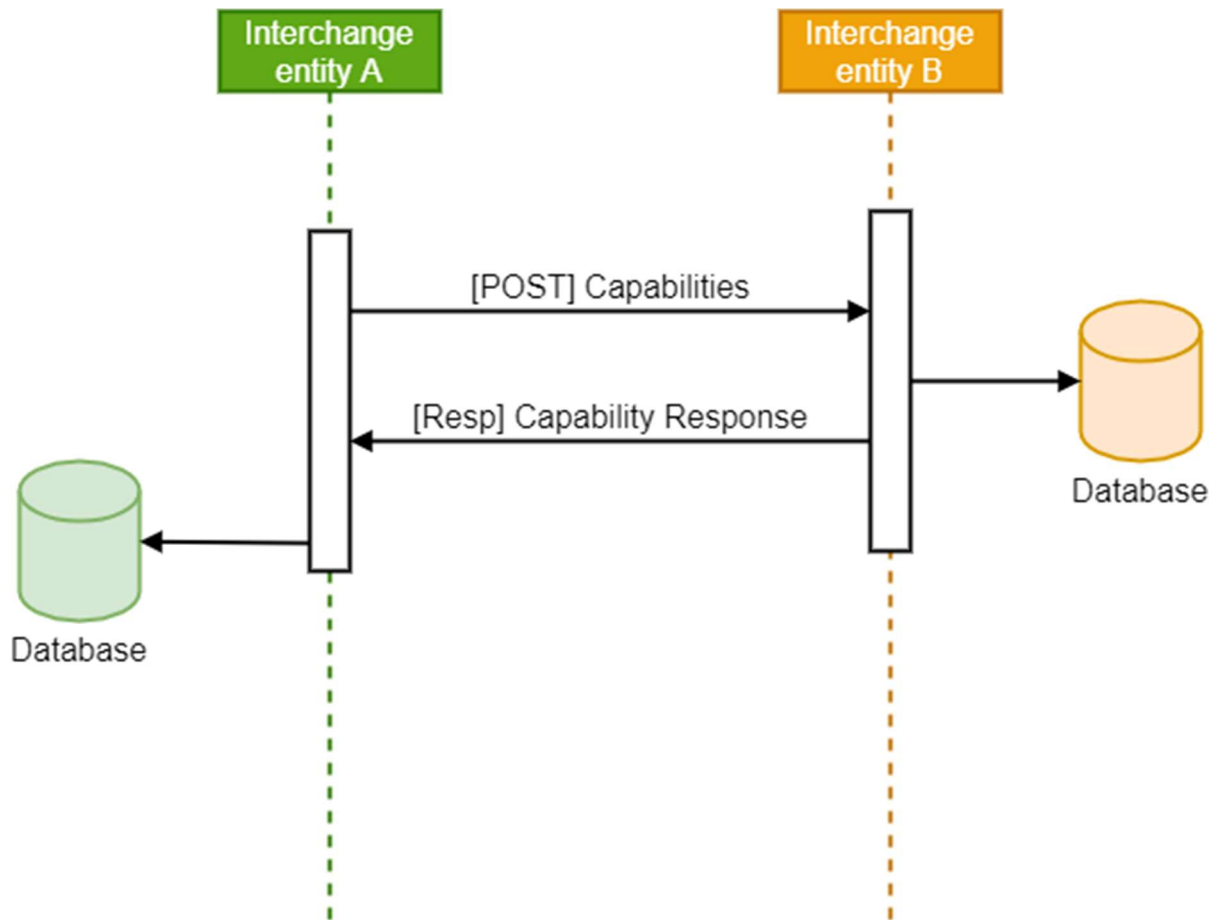


Figure 11 Capabilities exchange sequence

#### Requirement IP\_105/3

- For posting capabilities to other interchange entities, HTTP POST request shall be used to the endpoint formatted in the following way:  
<receiving interchange II base URL>/capabilities

#### Requirement IP\_091/3

- An interchange entity shall send their capabilities to all other interchange entities when capabilities change and at regular intervals of maximum 24 hours.

#### Requirement IP\_092/3

- The capabilities exchange shall use the JSON format defined in appendix C and properties as defined in Table 7.

If the capability exchange contains JSON properties not defined in this document, then these JSON properties can be ignored but the capability exchange shall be processed using the defined properties.

Additional information: This requirement is to ensure compatibility with future releases.

#### *Requirement IP\_093/3*

- The interchange entity shall send the capabilities exchange using HTTPS POST [15] with its capabilities as JSON payload defined in appendix C and using properties as defined in Table 7.

Additional information: The complete set of capabilities should be sent during the capability exchange.

#### *Requirement IP\_094/3*

- An interchange entity receiving a capability request from another interchange entity shall respond to the HTTPS POST [15] with their own capability in the same JSON format defined in appendix C and using properties as defined in Table 7.

Additional information: The complete set of capabilities should be sent during the capability exchange. Received capabilities replaces any previously received capabilities.

#### *Requirement IP\_132/12*

- If any additional capability properties beyond the properties defined in this specification are used, they shall be name spaced according to the following pattern: custom-  
<unique\_namespace\_id>-<property\_name>  
To ensure the uniqueness of the namespace id, a project name and/or country name should be included in the id.

Additional information: The use of name spacing in specification extensions ensure compatibility with future revisions of this specification, and reduces the possibility of confusion when messages with extended properties are received by others.

*Table 7 : Interchange capabilities exchange properties (format defined in appendix C)*

Property name	Type	Mandatory/Optional	Description
version	string	mandatory	Improved Interface JSON format version Starting with release 2.0.7 this value shall be version 2.0
name	string	mandatory	name of the interchange
capabilities	array of JSON objects	mandatory	Array of JSON objects each containing the properties defined in table 7a. The array



			can be empty if no datasets are available
--	--	--	---

*Table 7a Interchange Capabilities*

Property name	Type	Mandatory/Optional	Description
application	JSON Object	mandatory	JSON object containing the properties defined in table 7b
metadata	JSON Object	mandatory	JSON object containing the properties defined in table 7c

*Table 7b: Interchange Applications*

Property name	Type	Mandatory/Optional	Description
messageType	string DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, CAM	mandatory	For this version of the specification the string shall be one of the following: DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, and CAM. The list may be subject to changes in future versions of the specification
publisherId	string	mandatory	publisherId of dataset (see chapter 3.3.1 Table 1)
publicationId	String Concatenation of publisherId and a unique identifier for the dataset/publication with a ":" between, e.g. "DE15608:IVIM_BERLIN_6" or "NO73944:679ABX92"	mandatory	Concatenation of publisherId defined in table 1, and a unique identifier for the dataset/publication. Each dataset/publication identifier needs to be unique for the given publisher. When using the II, the publicationId shall uniquely identify a single capability entry.
originatingCountry	string	mandatory	originatingCountry of dataset (see chapter 3.3.1 Table 1)
protocolVersion	string	mandatory	protocolVersion of dataset (see chapter 3.3.1 Table 1)

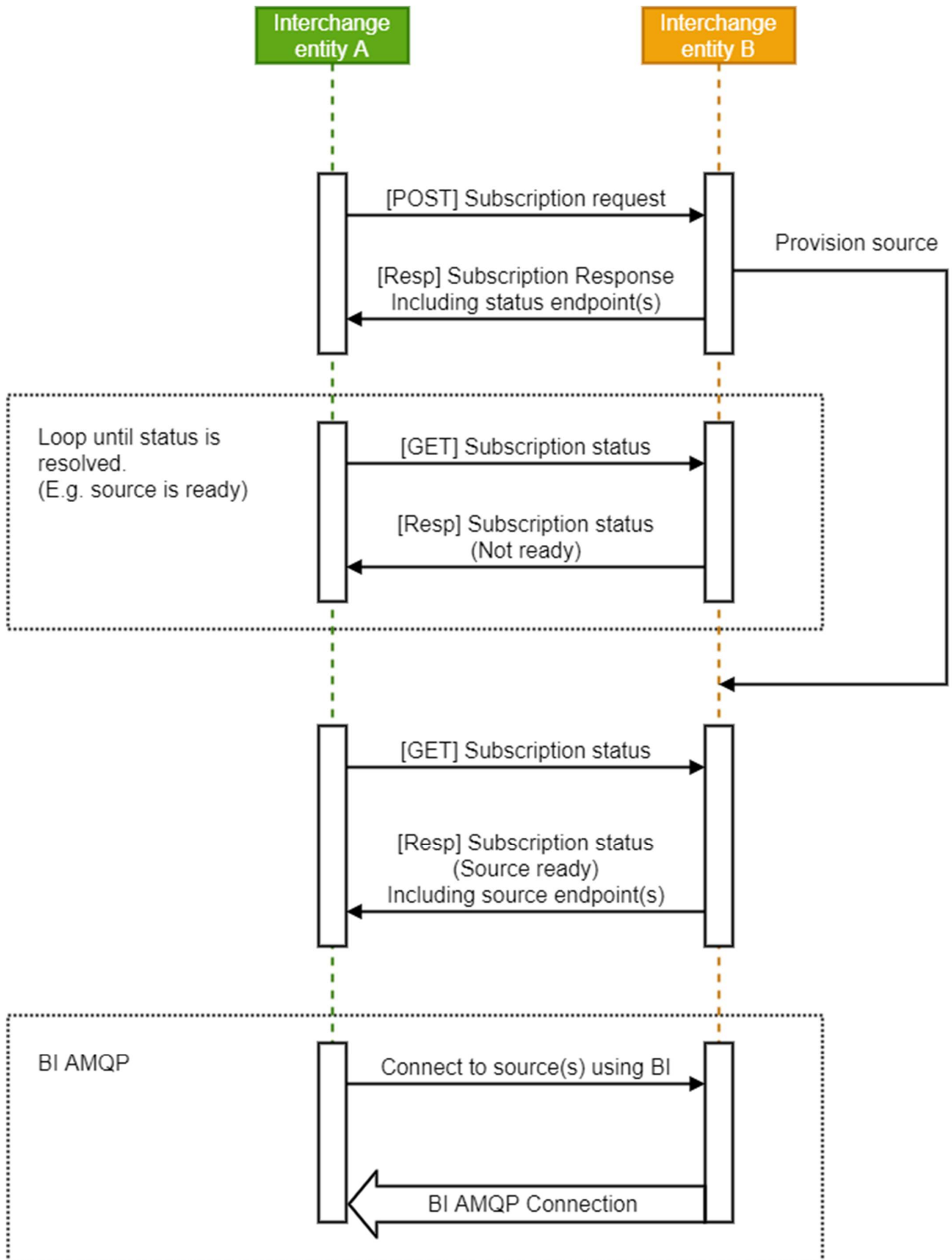
quadTree	array of strings	mandatory	quadTree tiles for coverage of the entire dataset
causeCode	array of integer	mandatory if messageType is "DENM"	causeCodes available in the dataset and default value "null" if unknown

*Table 7c: Interchange Metadata*

Property name	Type	Mandatory/Optional	Description
infoURL	string	optional	URL for a webpage created by the producer of the data that can be visited for more information about this dataset
shardCount	integer	optional	Defines the number of shards for the capability. See appendix G "Sharding" for more details.
redirectPolicy	String enum	optional	Indicates the redirect policy for the dataset. If this property is omitted, it shall be interpreted as OPTIONAL. Possible values are: [OPTIONAL, MANDATORY, NOT_AVAILABLE] OPTIONAL: A subscriber can choose to use redirects or not. (Default) MANDATORY: All subscribers shall use redirects when subscribing to this dataset. NOT_AVAILABLE: Subscriptions to this dataset shall not use redirects.
maxBandwidth	integer	optional	The maximum bandwidth (in bytes per second) this dataset will produce, measured over a duration of 5 seconds. If the dataset is sharded, this property indicates the bandwidth per shard.
maxMessageRate	integer	optional	The maximum message rate (in message per second) this

			dataset will produce over a duration of 5 seconds. If the dataset is sharded, this property indicates the message rate per shard.
repetitionInterval	integer	optional	Maximum interval between repetitions of messages in milliseconds

#### 4.3.6 Subscription exchange



*Figure 12 Subscription exchange sequence*

#### *Requirement IP\_095/3*

- The subscription exchange shall use the JSON format defined in appendix D. If the subscription exchange contains JSON properties not defined in this document, then these JSON properties can be ignored but the subscription exchange shall be processed using the defined properties.

Additional information: This requirement is to ensure compatibility with future releases.

#### *Requirement IP\_106/3*

- For the request of new subscriptions to other interchange entities, HTTP POST request shall be used to the endpoint formatted in the following way: <receiving interchange II base URL>/subscriptions.

Additional information: Subscription request should only contain new subscriptions. The new subscriptions will be appended to any existing subscriptions.

#### *Requirement IP\_096/3*

- The interchange entity shall send the subscription request using HTTP POST [14] with its subscriptions as JSON payload using properties as defined in Table 8.

#### *Requirement IP\_097/3*

- An interchange entity receiving a subscription request from another interchange entity shall respond to the request with HTTP 202 [14] containing a JSON payload defined in appendix D and using properties as defined in Table 9. The JSON payload shall contain endpoint(s) which the requesting interchange entity can use to poll the status of the subscription request by using an HTTP GET request to those endpoint(s).

Additional information: Received subscription requests shall be appended to any existing subscriptions.

#### *Requirement IP\_110/3*

- The endpoint defined by the "path" property in the subscription response (defined in Table 9) should be used by the interchange entity that made the initial subscription request to poll for the status of individual subscriptions by sending a HTTP GET request to that endpoint.

#### *Requirement IP\_127/9*

- An interchange entity with an active subscription shall poll for the subscription's status at least every 5 minutes

#### *Requirement IP\_107/3*

- An interchange entity receiving a HTTP GET request from another interchange entity to the endpoint with the following format.  
<receiving interchange II base URL>/<requesting interchange name>/subscriptions shall respond to the request with HTTP 200 [14] containing the requesting interchange entities existing subscriptions in the JSON payload defined in appendix D and using properties as defined in Table 9. The JSON payload shall contain endpoint(s) (path property) which the requesting interchange entity can use to terminate the subscription by using an HTTP DELETE request to those endpoint(s).

#### *Requirement IP\_108/3*

- An interchange entity receiving a subscription status request from another interchange entity shall respond to the request with HTTP 200 [14] containing a JSON payload defined in appendix D and using properties as defined in Table 10.

#### *Requirement IP\_109/3*

- Unless mechanisms are in place to prevent looping of messages, an interchange entity shall not re-distribute AMQP messages coming from another interchange entity to any other interchange entity.

Additional information:

This requirement is to prevent looping of messages in the network.

#### *Requirement IP\_133/12*

- When an interchange (subsequently referred to as sub-interchange) sends a subscription request to another interchange (subsequently referred to as pub-interchange), the sub-interchange shall not send a subscription request that is not compliant with the redirect policy of any of the matching capabilities of the pub-interchange.

Additional information: "Matching capabilities" here refers to the set of capabilities that match with the selector of a subscription request

#### *Requirement IP\_134/12*

- If an interchange (subsequently referred to as pub-interchange) receives a subscription request that is not compliant with the redirect policy of one or more of the matching capabilities, the pub-interchange shall respond according to the following rules:
  - If the subscription request is not compliant with the redirect policy of any of the matching capabilities, the pub-interchange shall respond with a NO\_OVERLAP subscription status.
  - If the subscription request is only compliant with some of the redirect policies of the matching capabilities, the pub-interchange shall respond with a subscription

containing only the subset of the matching capabilities that comply with the redirect policy.

Additional information: “Matching capabilities” here refers to the set of capabilities that match with the selector of a subscription request.

## Request

*Table 8 : Interchange Subscription Request (format defined in appendix D)*

Property name	Type	Mandatory/Optional	Description
version	string	mandatory	Improved Interface JSON format version Starting with release 2.0.2 this value shall be version 1.2
name	string	mandatory	name of the interchange
subscriptions	array of objects	mandatory	Subscriptions as defined by the properties below
selector	string	mandatory	JMS-selector filter. Needs to be checked against the capabilities of the interchange that the request is being sent to.
consumerCommonName	string	optional	This is the username (certificate Common Name) that should have access to the source. This property can be used to request a redirect on behalf of a c-its actor by setting this property value to the certificate Common Name of the local c-its actor that is requesting the subscription. Either omitting this property or setting it to the certificate Common Name of the requesting interchange shall result in the subscription not being redirected. The redirectPolicy (See table 7, requirements IP_133/12 and IP_134/12) defines whether a specific dataset is able to be redirected or not.  (Defaults to the username(certificate Common Name) of the requesting interchange if not present)

--	--	--	--

## Response

*Table 9: Interchange Subscription Response (format defined in appendix D)*

Property name	Type	Mandatory/Optional	Description
version	string	mandatory	Improved Interface JSON format version Starting with release 2.0.2 this value shall be version 1.2
name	string	mandatory	name of the interchange
subscriptions	array of objects	mandatory	Subscriptions as defined by the properties below
id	string	mandatory	Identifier of the subscription. (generated by the interchange that receives the subscription request)
selector	string	mandatory	JMS-selector filter. Needs to be checked against the capabilities of the interchange that the request is being sent to.
consumerCommonName	string	optional	This is the username (certificate Common Name) that should have access to the source. This property can be used to request a redirect on behalf of a c-its actor by setting this property value to the certificate Common Name of the local c-its actor that is requesting the subscription. Either omitting this property or setting it to the certificate Common Name of the requesting interchange shall result in the subscription not being redirected. The redirectPolicy (See table 7, requirements IP_133/12 and IP_134/12) defines whether a specific dataset is able to be redirected or not.



			(Defaults to the username(certificate Common Name) of the requesting interchange if not present)
path	string	mandatory	URL path the requesting interchange entity can poll to check the status of the request (GET) The URL path can also be used to terminate the subscription (DELETE)
status	String (enum)	mandatory	Status of the request.  Possibilities:  "REQUESTED" The request is being processed.  "CREATED" The data is ready for consumption.  "ILLEGAL" The request is rejected (eg. request too large)  "NOT_VALID" The request selector is not a valid selector.  "NO_OVERLAP" The request does not match any available dataset.  "RESUBSCRIBE" A new capability (i.e. dataset) relevant for the current subscription has become available. To include the new capability to the current subscription, the subscriber needs to delete the current subscription and resubmit the subscription request.  "ERROR" An error has occurred during processing of the subscription request. E.g. one of the

			endpoints has responded with ILLEGAL and another with CREATED. If this flag is set, an errorMessage property can be added to this response.
errorMessage	string	optional	If the status property flag is set to "ERROR", this property can be used to give a human readable error message describing the problem.

### Status poll response

Table 10: Interchange Subscription Status poll response (format defined in appendix D)

Property name	Type	Mandatory/Optional	Description
id	string	mandatory	Identifier of the subscription. (generated by the interchange that receives the subscription request)
selector	string	mandatory	JMS-selector filter. Needs to be checked against the capabilities of the interchange that the request is being sent to.
consumerCommon Name	string	optional	<p>This is the username (certificate Common Name) that should have access to the source. This property can be used to request a redirect on behalf of a c-its actor by setting this property value to the certificate Common Name of the local c-its actor that is requesting the subscription. Either omitting this property or setting it to the certificate Common Name of the requesting interchange shall result in the subscription not being redirected. The redirectPolicy (See table 7, requirements IP_133/12 and IP_134/12) defines whether a specific dataset is able to be redirected or not.</p> <p>(Defaults to the username(certificate Common</p>

			Name) of the requesting interchange if not present)
path	string	mandatory	<p>URL path the requesting interchange entity can poll to check the status of the request (GET)</p> <p>The URL path can also be used to terminate the subscription (DELETE)</p>
status	String (enum)	mandatory	<p>Status of the request.</p> <p>Possibilities:</p> <p>“REQUESTED” The request is being processed.</p> <p>“CREATED” The data is ready for consumption.</p> <p>“ILLEGAL” The request is rejected (eg. request too large)</p> <p>“NOT_VALID” The request selector is not a valid selector.</p> <p>“NO_OVERLAP” The request does not match any available dataset.</p> <p>“RESUBSCRIBE” A new capability (i.e. dataset) relevant for the current subscription has become available. To include the new capability to the current subscription, the subscriber needs to delete the current subscription and resubmit the subscription request.</p> <p>“ERROR” An error has occurred during processing of the subscription request. E.g. one of the endpoints has responded with ILLEGAL and another with CREATED. If this flag is set, an errorMessage</p>

			property can be added to this response.
endpoints	array of objects	mandatory	list of endpoints defined by the properties below. A client should connect to all endpoints in order to receive all available information.
host	string	mandatory only if status is "CREATED"	in order to support for instance load-balancing the message broker can provide a different amqp endpoint host than the interchange entity itself.
port	Integer	mandatory only if status is "CREATED"	in order to support for instance load-balancing the message broker can provide a different amqp endpoint port than the interchange entity itself.
source	string	mandatory only if status is "CREATED"	The name of the source where the data is available. (generated by the interchange that receives the subscription request)
errorMessage	string	optional	If the status property flag is set to "ERROR", this property can be used to give a human readable error message describing the problem.
lastUpdatedTimestamp	long	mandatory	Timestamp in UNIX time in milliseconds, of when the status poll response was last changed. Can be used by the subscriber to check if the subscription has changed since the last time it was checked.

## 5 Session level security

### 5.1 Introduction

The scope of session level security is to protect the transport layer connection between two end points that implement BI/II for C-ITS message exchange. The end points can be:

- two interchange entities

- an interchange entity and a C-ITS actor
- two C-ITS actors that communicate C-ITS messages with each other over BI.

The role of the Interchange entities for security is to establish secure connections but NOT to verify security properties from the C-ITS trust domain.

Further information on governance and session level security can be found in Appendix E.

## 5.2 Common TLS profile

### *Requirement IP\_050/6*

- For the transport layer protection TLS with mutual authentication using standard X.509 certificates according to Appendix E shall be used.

### *Requirement IP\_051/6*

- Certificates renewal periods for client and server certificates shall be maximum one year.

### *Requirement IP\_053/1*

- TLS 1.3 as specified in RFC 8446 [5] shall be supported.

### *Requirement IP\_054/1*

- Earlier versions of TLS shall not be supported.

### *Requirement IP\_055/1*

- The rules on cipher suites and extensions given in TLS 1.3 RFC 8446 [5]) shall be followed.

### *Requirement IP\_057/7*

- The whole certificate chain shall be sent in the TLS handshake.

### *Requirement IP\_063/1*

- TLS version 3 certificates specified in RFC 5280 [7] shall be used.

## 5.3 BI – BI TLS profile

This chapter covers a direct connection using BI only, between two C-ITS actors.

Trust and the exchange of certificates is based on bilateral agreements, for more information see chapter 3.1.

## 5.4 BI / II TLS profile

This chapter defines requirements for connections from a C-ITS actor to an interchange entity and between two interchange entities.

### *Requirement IP\_115/6*

- All interchange entities shall have the common TLS root certificate in their trust list.

Additional information:

Description of session level trust domain can be found in Appendix E.

### *Requirement IP\_116/6*

- All C-ITS actors shall have the common TLS root certificate in their trust list.

Additional information:

Description of session level trust domain can be found in Appendix E

### *Requirement IP\_117/6*

- All client and server certificates used for mutual authentication shall be issued and signed by a trusted subordinate CA (intermediate CA), derived from the common TLS root certificate

Additional information:

Description of session level trust domain can be found in Appendix E

## 6 Appendix A – Quadtree

Quadtree is a method to build a data structure for distributing data streams w.r.t. geographic areas (single points, lines or links, areas ), and used often in GIS (Geographic Information Systems) and backend servers.

Quadtree is a tree data structure in which each node has exactly four children. Quadtree is used by eg. Microsoft and Google to divide an area into manageable parts.

The quadtree tile is denoted as a string of the characters 0,1,2 and 3. The length of the string is equal to the zoom level.

Level 0 is being the world, and then at each level you slice each tile in 4 tiles, as following:

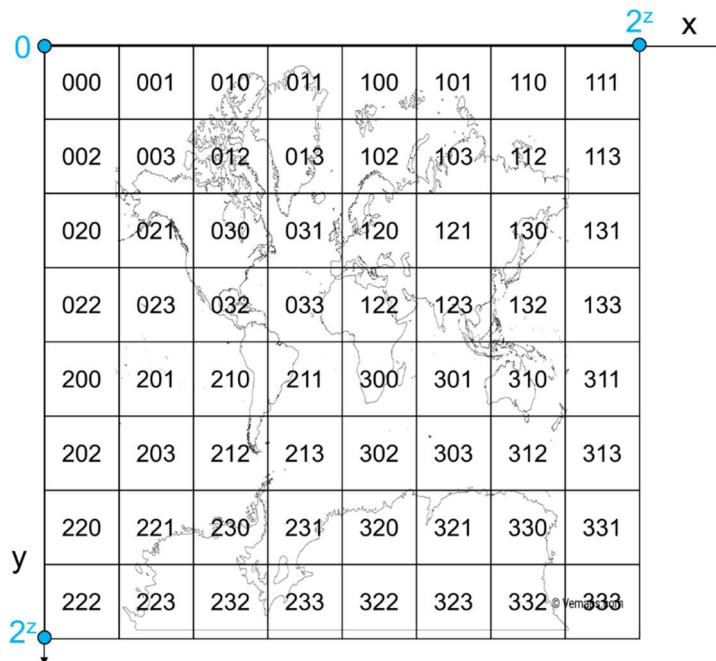
- 0 being the top left tile (NW)
- 1 the top right tile (NE)
- 2 the bottom left tile (SW)
- 3 the bottom right tile (SE)

The quadtree uses a Mercator projection of the world, and the latitudes are scaled so that the tiles (at higher zoom levels) are squares (i.e. northbound length equal to eastbound length). For the zoom level  $z$ , the projection contains " $2^z$ " tiles in horizontal direction and in vertical direction.

The position of the quadtree tile is calculated for a location, identified by latitude and longitude in WGS84 coordinate system. The location in the Mercator projection is calculated using the equations:

$$x = 2^z * (0.5 + lon/360)$$

$$y = 2^z * \left( 0.5 - \ln \left( \frac{1 + \sin(lat * \pi/180)}{1 - \sin(lat * \pi/180)} \right) / 4\pi \right)$$



Latitudes over 85.05 degrees are not addressed, as there is no human habitation at this latitude.

Both  $x$  and  $y$  values are rounded to integers and converted to bit string  $Xs$  and  $Ys$  of length  $z$ . The quadtree tile string  $Qs$  is obtained from the characters of the bit strings:

$Qs(i) = Xs(i) + 2*Ys(i)$ , i.e.:

- $Qs(i)=0$ : top left (NW)

- $Qs(i)=1$ : top right (NE)
- $Qs(i)=2$ : bottom left (SW)
- $Qs(i)=3$ : bottom right (SE)

#### Examples

location	latitude	longitude	quadtree tile	size of tile (east-west)
Kilpisjärvi (NO-FI)	69.111746	20.749621	102231321102200323	54 m
Valenca-Tui (ES-PT)	42,033415	-8,65392	031332213323322232	127 m
Hazeldonk (E19, BE-NL)	51.485992	4.735311	120202130121133020	95 m

A reference implementation of quadtree is available at: <https://github.com/passchieri/Hybrid-IF2>  
(Remark: in this implementation the characters in the quadtree path are separated by "/")

Here follow example Java and Python code:

#### JAVA:

```
public String latLonToQtree(double lat, double lon, int zoom)
{
    double sinlat = Math.sin(lat*Math.PI/180.);

    double x = 0.5+lon/360.;
    double y = 0.5-Math.log((1.+sinlat)/(1.-sinlat))/(4*Math.PI);

    int ix = (int)(Math.pow(2,zoom)*x);
    int iy = (int)(Math.pow(2,zoom)*y);

    String qtree = "";
    for (int i=0;i<zoom;i++)
    {
        qtree = (ix&1 | 2*(iy&1))+qtree;
        ix = ix>>1;
        iy = iy>>1;
    }
    return qtree;
}
```

#### PYTHON:

```
def latLonToQtree(lat,lon,zoom=18):

    sinlat = math.sin(lat*math.pi/180.)

    x = 0.5+lon/360.
    y = 0.5-math.log((1.+sinlat)/(1.-sinlat))/(4*math.pi)
```



```
x = math.floor(math.pow(2, zoom)*x)
y = math.floor(math.pow(2, zoom)*y)

qtree = ""
for bn in range(zoom):

    qtree = str(x&1 | 2*(y&1))+qtree
    x = x>>1
    y = y>>1

return qtree
```

## 7 Appendix B – Deployment Models

The image below provides a simplified view of C-Roads deployment model which consist of two different approaches; centralized approach (model B) and decentralized approach (model A) to allow flexibility of the deployments and ensure the interoperability between all Member States. It is depicted how C-ITS actors or a group of C-ITS actors within one/different Member states can establish the informationsharing network to share C-ITS messages with each other through backend communication.

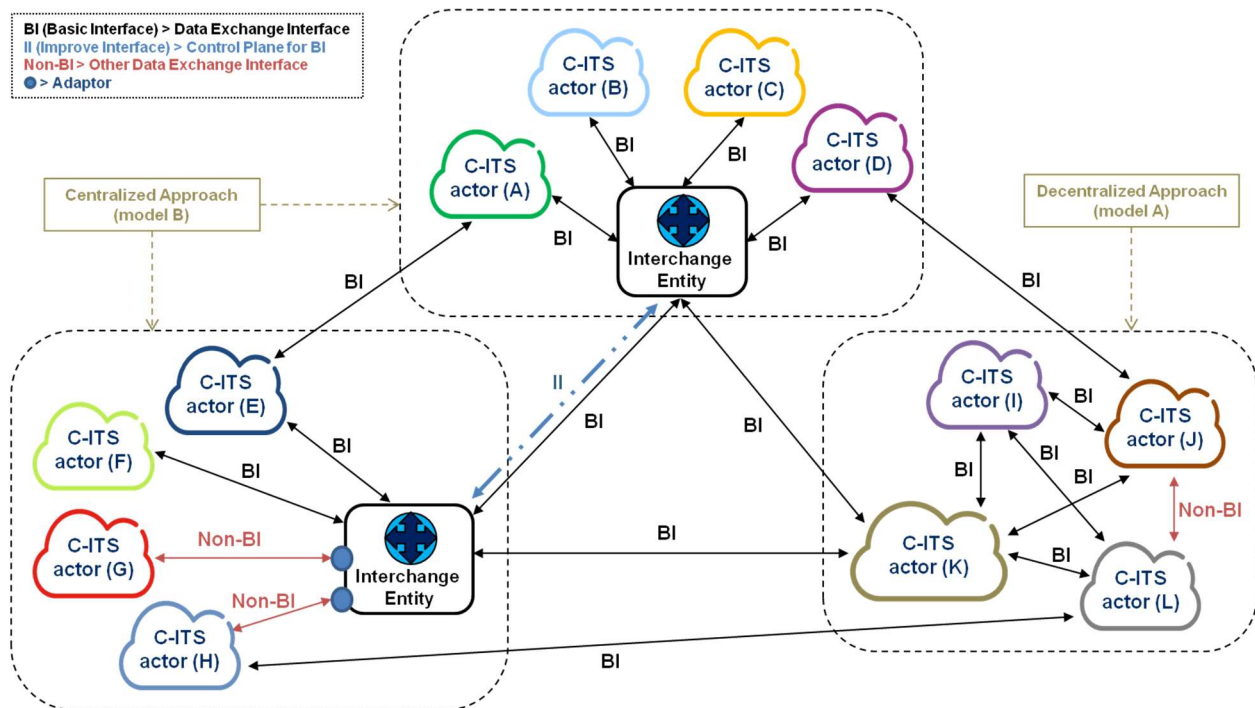


Figure 13 Deployment models

Based on the centralized approach (model B); each group of C-ITS actors can establish an Interchange Entity to interconnect with each other. Each Interchange Entity can connect to every other Interchange Entity and route data from all other interconnected Interchange Entities to be able to serve it to their own interconnected C-ITS actors.

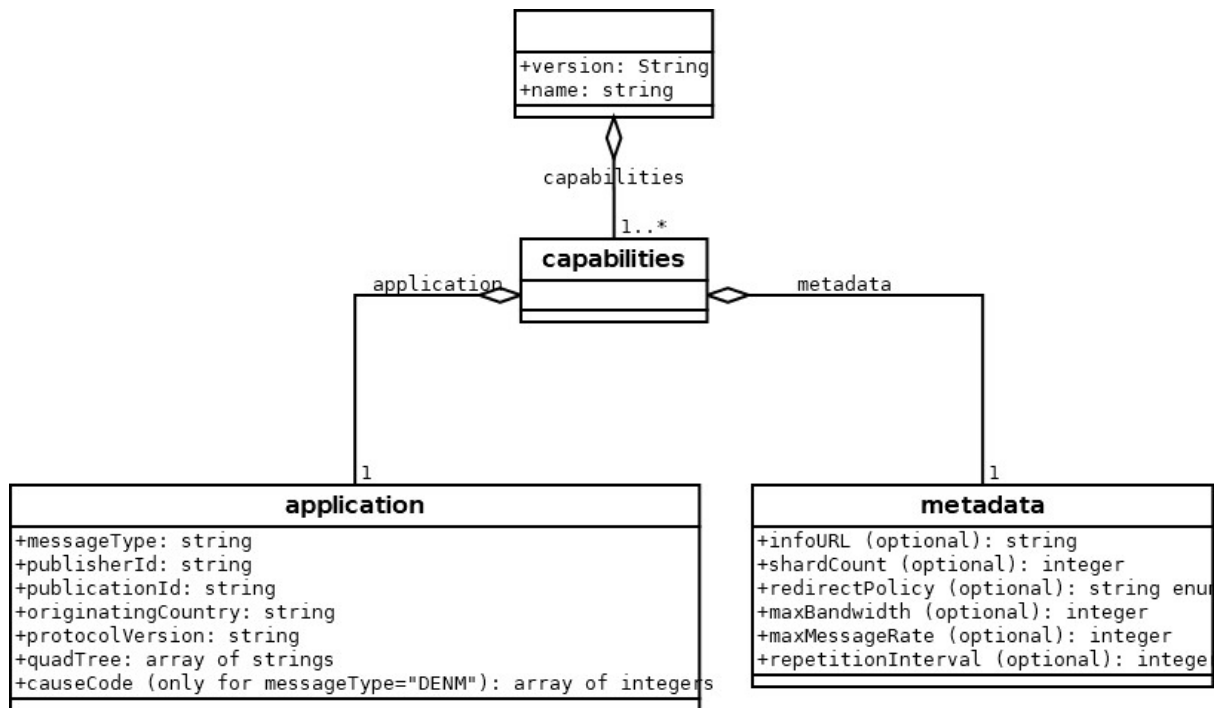
Alternatively;

Based on the decentralized approach (model A); each C-ITS actors can interconnect via multiple logical point-to-point connections with each other or with every other Interchange Entities to be able to share information.

Information about Basic Interface (BI) and Improved Interface (II) can be found in chapter 3 and 4 respectively

Additional information: On national level Basic Interface is not a mandatory requirement.

## 8 Appendix C – Capabilities exchange JSON format



```

{
  "version": "2.0",
  "name": "a.c-its-interchange.eu",
  "capabilities": [
    {
      "application": {
        "messageType": "DENM",
        "publisherId": "SE12345",
        "publicationId": "SE12345:DENMSTCKHLM345",
        "originatingCountry": "SE",
        "protocolVersion": "DENM:1.2.2",
        "quadTree": [
          "01220111",
          "01200132"
        ],
        "causeCode": [6,4,5]
      },
      "metadata": {
        "infoURL": "https://trafikverket.se/denm/",
        "shardCount": 2,
        "redirectPolicy": "OPTIONAL",
        "maxBandwidth": 350000,
        "maxMessageRate": 35,
        "repetitionInterval": 60000
      }
    },
    {
      "application": {

```

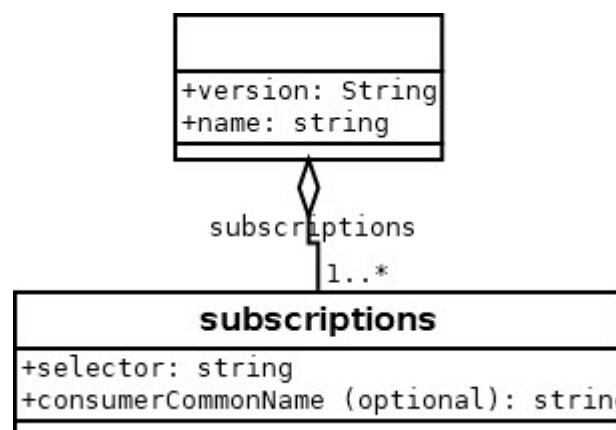
```

    "messageType": "DENM",
    "publisherId": "N012345",
    "publicationId": "N012345:DENMOSL0125",
    "originatingCountry": "NO",
    "protocolVersion": "DENM:1.2.2",
    "quadTree": [
        "01230122",
        "01230123"
    ],
    "causeCode": [3,4,5]
  },
  "metadata": {
    "infoURL": "https://vegvesen.no/denminf/",
    "redirectPolicy": "OPTIONAL",
    "maxBandwidth": 550000,
    "maxMessageRate": 55,
    "repetitionInterval": 45000
  }
}

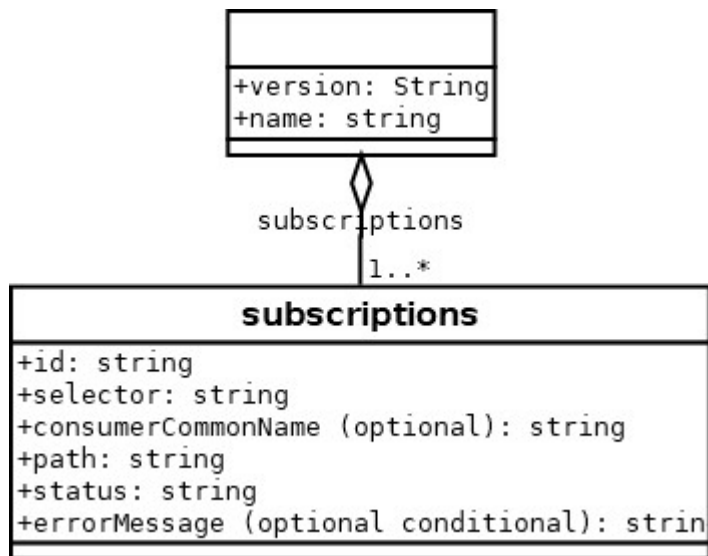
```

## 9 Appendix D – Subscription exchange JSON format

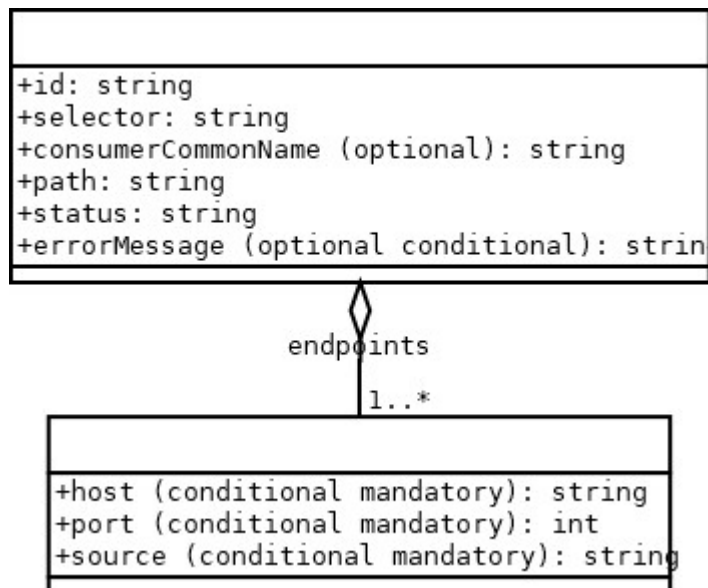
Request



Response



## Status response



## Subscription exchange examples

### Request

```
{
  "version": "1.2",
  "name": "a.c-its-interchange.eu",
```

```

"subscriptions": [
  {
    "selector": "messageType='DENM' AND
originatingCountry='SE'"
  },
  {
    "selector": "messageType='DENM' AND originatingCountry='NO'",
    "consumerCommonName": "c-its-company-client1"
  }
]
}

```

### Response

```

{
  "version": "1.2",
  "name": "a.c-its-interchange.eu",
  "subscriptions": [
    {
      "id": "{id1}",
      "selector": "messageType='DENM' AND originatingCountry='SE'",
      "path": "/subscription/{id1}",
      "consumerCommonName": "a.citsinterchange.eu",
      "status": "REQUESTED"
    },
    {
      "id": "{id2}",
      "selector": "messageType='DENM' AND originatingCountry='NO'",
      "path": "/subscription/{id2}",
      "consumerCommonName": "client1",
      "status": "REQUESTED"
    }
  ]
}

```

### Status response

```

{
  "id": "{id2}",
  "selector": "messageType='DENM' AND originatingCountry='NO'",
  "path": "/subscription/{id2}",
  "consumerCommonName": "client1",
  "endpoints": [
    {
      "source": "0QPjabpeFgQSIPFrHJ3BM567nQwCD",
      "host": "b.c-its-interchange.eu",
      "port": 5671
    }
  ]
}

```

```
    },  
    {  
      "source": "0QPjabpeFgQSIPFrHJ3dfghsfdgQwcD",  
      "host": "b2.c-its-interchange.eu",  
      "port": 5671  
    }  
  ],  
  "status": "CREATED"  
}
```

## 10 Appendix E – Session level security and governance

Session level governance and security is necessary when you have a high number of actors interconnected in a network containing interchange entities. This enables a scalable automated operation of interchange entities within the session level trust domain and needs a governing body to be responsible for the governance of the trust domain.

Responsibilities of the Governing body are

- Operation of TLS Root CA
- Approval of TLS intermediate CAs
- Operation of trusted domain name DNS records
- Approve Interchange entities for inclusion in DNS based upon recommendations from TLS Intermediate CAs
- Maintains a list of trusted domain names
- The publication of revoked certificates

The TLS Intermediate CAs are responsible for

- Approving C-ITS actors
- Recommending Interchange entities to be included in the trusted domain names DNS records by the Governing Body
- Issuing both Server and client certificates

This is exemplified in below figure

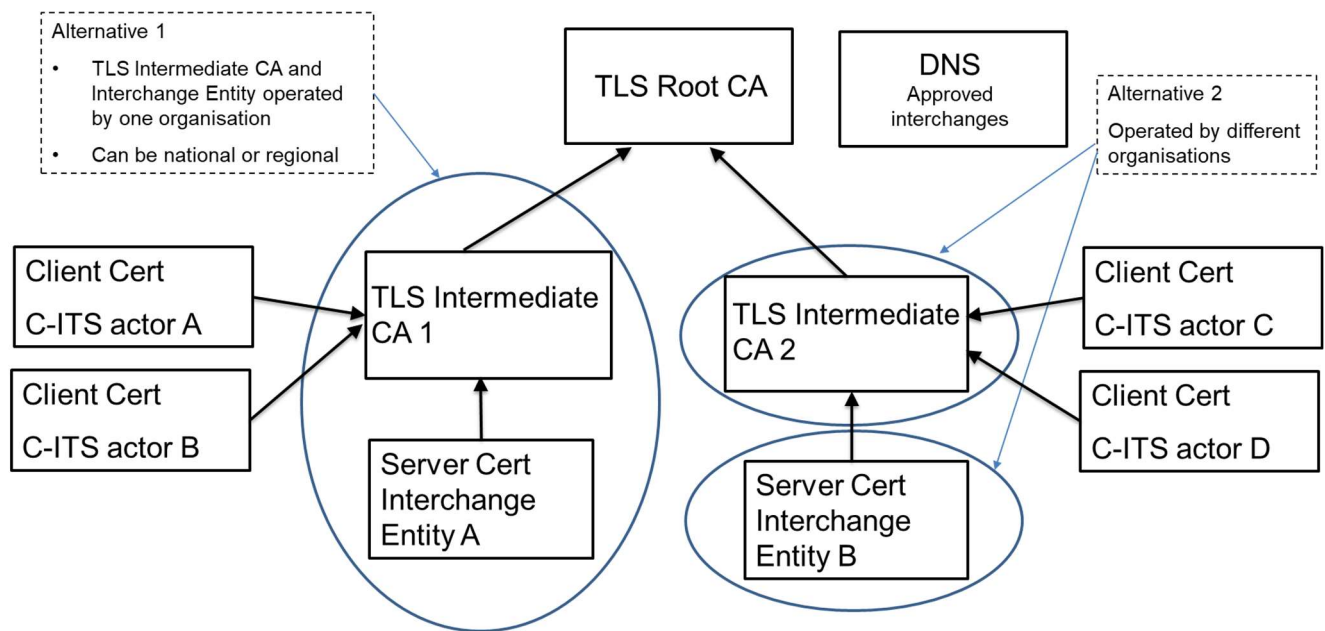


Figure 14 Session level PKI hierarchy

Examples of interactions between session level trust domain and other trust domains is found below figure.

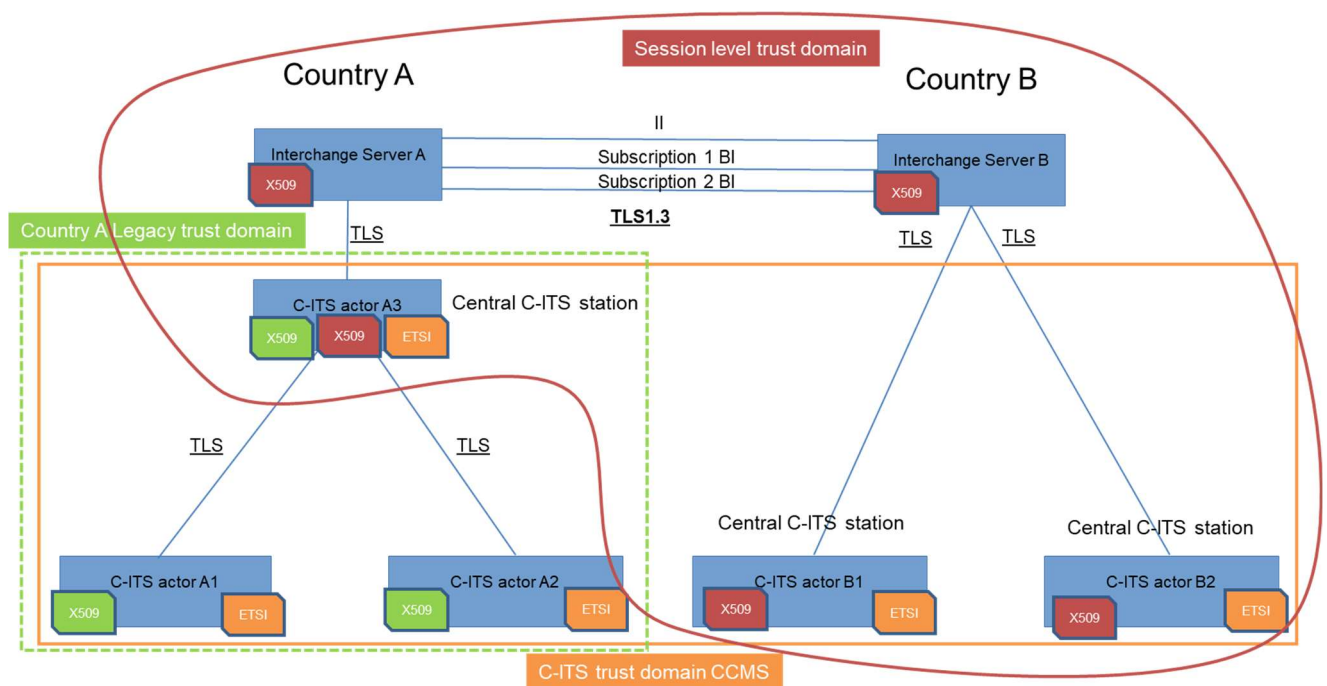


Figure 15 Examples of trust domain interactions



## 11 Appendix F – Pilot testing information

### 11.1 Basic Interface Registry

Template for BI Registry, for BI interoperability testing within C-Roads. For further information contact member state C-Roads partner.

Table for the BI registry:			v03
Nr.	Url.	responsible partner for BI	contact person name, contact person email
1	<a href="http://www.xyz.eu">www.xyz.eu</a>	Company A	<a href="mailto:john.doe@example.com">john.doe@example.com</a>

Message types available	test period in Calendar Week	last update	next update
DENM, IVI, <b>SPAT/MAP</b>	48/2020 to 10/2021	2020-10-11	2021-04-01

geographic indication for area served	remark1 (total number of available sets)	remark 2 – connection security used (recommended TLS 1.3)
set of tiles (covering all messages)	e.g. 54 intersections	e.g. TLS 1.2 used for encryption and authentication

### 11.2 BI Bilateral pilot testing

For BI-BI bilateral testing, agreements on security and configuration needs to be agreed between the involved parties, guidelines can be found in chapter 3.1.

### 11.3 Pilot Governance

One partner (Pilot Governing Body) responsible for operating

- central DNS
- Root CA (pilot security rules will be applied)
- Add interchanges to DNS on behalf of active partners for testing

Every participating member has to enroll interchange entities and active clients with the Pilot Governing Body for the full duration of the piloting or the Pilot Governing Body can delegate server/client certificates handling to national intermediate CAs.

### 11.4 Test logging format

The example below is a message logged in JSON format with two fields

- “applicationProperties” containing the custom header properties
- “bodyContentHex” containing the hex string of the binary data received in the payload.

```
2021-07-15T12:30:23.317Z [info] - received_message: {
  "applicationProperties": {
    "latitude": "50.2268645",
    "longitude": "14.4041937",
    "messageType": "DENM",
    "protocolVersion": "DENM:1.3.1",
```

```

    "causeCode": "1",
    "subCauseCode": "4",
    "serviceType": "HLN-TJA",
    "quadTree":
    ",120212302013111223,1202123020110,1202123020111,1202123021000,1202123021001
    ,1202123021010,1202123020112,1202123020113,1202123021002,1202123021003,12021
    23021012,1202123020130,1202123020131,1202123021020,1202123021021,12021230210
    30,1202123020132,1202123020133,1202123021022,1202123021023,1202123021032,120
    2123020310,1202123020311,1202123021200,1202123021201,1202123021210,",
    "originatingCountry": "CZ",
    "publisherId": "CZ00003"
  },
  "bodyContentHex":
  "204000000006b0a00001a00003ccbfacc7e8427fadb6a87621df002e50895e7d1000000001df
  002e50895e7d11770000000000000007d2000002012bb55606c395daab030000101b6d50ec240
  6db543b0d394ebe573dfb9d1ffffffe11186a0040259387878801042abefc083ffc0ffeb639c
  3b9a71f57639c3e5bb0c7ee39c3e5bd0c7ee39c3cdf1f9b0e39c3ece70a90639c3ece90a9063
  9c3aef92de6e39c"
}

```

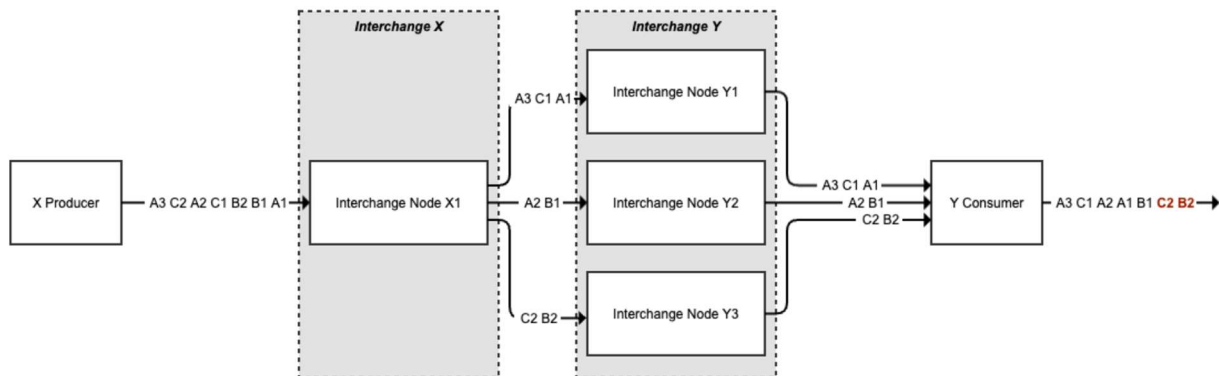
## 12 Appendix G – Sharding

This appendix elaborates on the concept of **sharding data streams** across a C-Roads Interchange network. Sharding data streams is required when horizontally scaled interchanges need to preserve the **in-order delivery of AMQP messages** belonging to a single capability.

Some data streams require in-order delivery of messages (e.g. traffic light preemption based on SRM+SSM+CAM+SPAT message flows). For high volume data streams, horizontal scaling might be needed on interchange level. Currently however, the data stream of a single capability cannot be horizontally scaled without losing guaranteed in-order delivery of messages. The image below depicts the problem having:

- two interchanges (X and Y)
- one local actor for interchange X producing data for a single capability
- one local actor for interchange Y consuming data of this single capability
  - interchange Y has horizontally scaled the provisioning of this capability over three nodes
- the producer sending messages belonging to three logical contexts that are required to be in-order (A, B and C) - e.g. SPAT messages from device A, B and C

Since the interchange network is unaware of the “in-order contexts” of the produced data stream, it might be split causing a possibility for out-of-order delivery to consumer Y.



To solve this issues, the **following data elements are added** to the capability descriptor and application properties:

- An optional “**shardCount**” property is added to the **capability descriptor**; this allows interchanges to inform others about the amount of shards for a capability via II or local actor API.
- A conditional mandatory “**shardId**” application property is added to the messages. Mandatory if the corresponding capability has a “shardCount” specified.

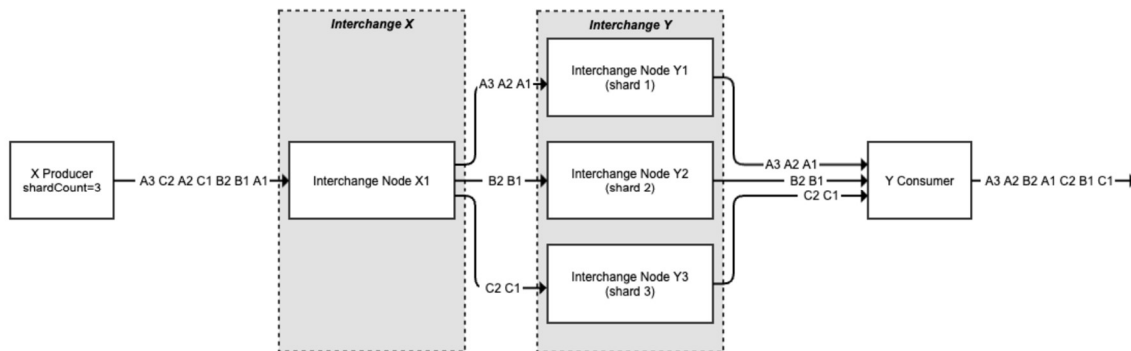
It is up to the Interchange to make sure **messages within the same shard are never delivered out-of-order**. Note: if no shardId is added (because e.g. the capability has no shardCount specified), that should be interpreted as if all messages belonging to that same capability have the same shardId.

**Interchanges can only horizontally scale capabilities if they have a shardCount > 1 defined in their capability descriptor. Producer MUST supply the “shardId” application property when producing messages for a capability with a shardCount defined.** The “shardId” application property must be ≤ “shardCount” defined in the corresponding capability descriptor.

The only entity in the interchange network that has knowledge of the logical in-order context of the data stream is the producer. By adding a “shard indicator” to the messages, producers can indicate which messages should be kept in-order and should not sent across separate data paths. To guarantee that the sharding enables interchanges to horizontally scale correctly, the producer should also try to define shard indicators in such a way that the **expected load in terms of message flows is spread out as evenly as possible** across the different shards.

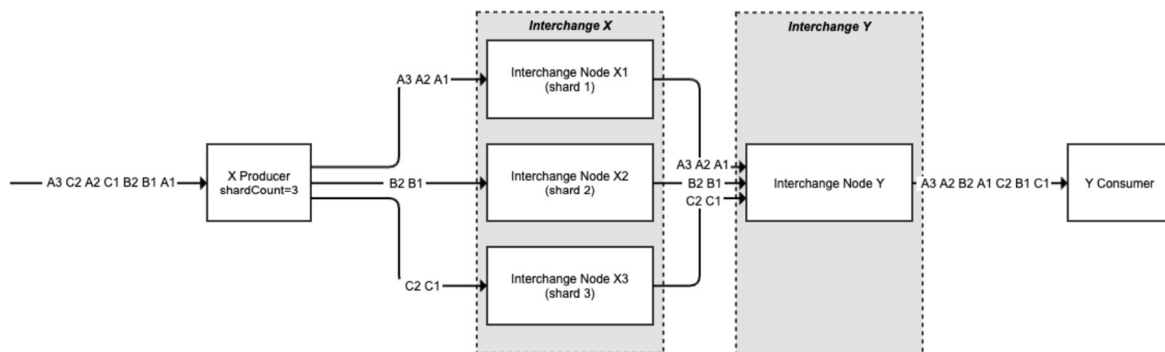
The image below depicts the solution in a **first example scenario** having:

- two interchanges (X and Y)
- one local actor for interchange X producing data for a single capability with shardCount = 3
- one local actor for interchange Y consuming data of this single capability
  - interchange Y has horizontally scaled the provisioning of this capability over three nodes, respecting the shardCount
- the producer sending messages belonging to three logical contexts that are required to be in-order (A, B and C) where - e.g. SPAT messages from device A, B and C
  - A messages are given application property shardId=1
  - B messages are given application property shardId=2
  - C messages are given application property shardId=3



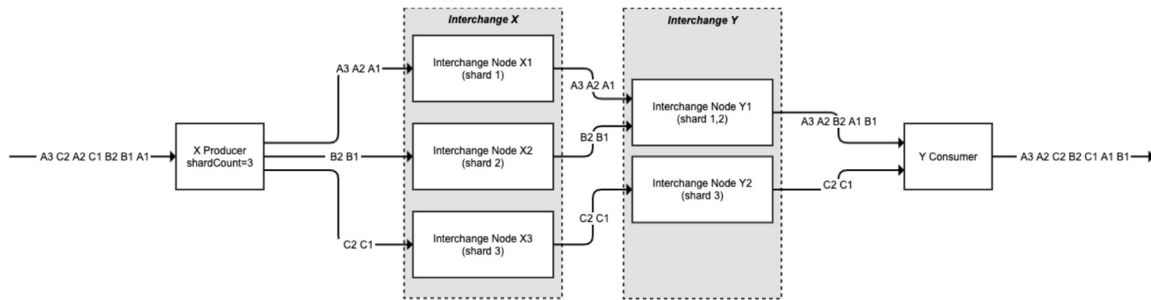
The image below depicts the solution in a **second example scenario** having:

- two interchanges (X and Y)
- one local actor for interchange X producing data for a single capability with shardCount = 3
  - interchange X has horizontally scaled the provisioning of this capability over three nodes, respecting the shardCount
- one local actor for interchange Y consuming data of this single capability
- the producer sending messages belonging to three logical contexts that are required to be in-order (A, B and C) where - e.g. SPAT messages from device A, B and C
  - A messages are given application property shardId=1
  - B messages are given application property shardId=2
  - C messages are given application property shardId=3



The image below depicts the solution in a **third example scenario** having:

- two interchanges (X and Y)
- one local actor for interchange X producing data for a single capability with shardCount = 3
  - interchange X has horizontally scaled the provisioning of this capability over three nodes, respecting the shardCount
- one local actor for interchange Y consuming data of this single capability
  - interchange Y has horizontally scaled the provisioning of this capability over two nodes, respecting the shardCount
- the producer sending messages belonging to three logical contexts that are required to be in-order (A, B and C) where - e.g. SPAT messages from device A, B and C
  - A messages are given application property shardId=1
  - B messages are given application property shardId=2
  - C messages are given application property shardId=3



The **expected impact** of introducing this sharding concept to the C-Roads C-ITS IP Based Interface Profile is as follows:

- When not using this optional field, and hence not defining a shardCount for the capability, the impact is zero. But: Interchanges will only be able to scale vertically, not horizontally (because they will need to provide in-order delivery of all messages, which are considered to all be part of the same implicit shard).
- When using this field (initiative would lie at the Interchange that cannot handle the received load, will inform Producer to start supporting sharding):
  - the corresponding producers need to contain the logic to identify which messages should be put on the same shard
  - the Interchanges that needs to forward these messages and perform horizontal scaling need to support sharding in their implementation. If they were not involved in taking the initiative to activate sharding, they are informed about this by the other Interchange before sharding is activated. This could be automated using II with new capabilities that are being announced, or as part of manual configuration exchanges when not using II. The corresponding timing requirements depend on the maturity level and known support of sharding by all involved actors. E.g. in a first trial phase such a manual warning needs to be given much more in advance than in a mature production deployment that relies on II for highly dynamic scaling in the full chain.

## 13 Appendix H – Deleted requirements

- Requirement IP\_017
- Requirement IP\_021
- Requirement IP\_025
- Requirement IP\_027
- Requirement IP\_028
- Requirement IP\_030
- Requirement IP\_040
- Requirement IP\_041
- Requirement IP\_042
- Requirement IP\_043
- Requirement IP\_046
- Requirement IP\_047
- Requirement IP\_052

- *Requirement IP\_056*
- *Requirement IP\_058*
- *Requirement IP\_059*
- *Requirement IP\_060*
- *Requirement IP\_061*
- *Requirement IP\_062*
- *Requirement IP\_063*
- *Requirement IP\_064*
- *Requirement IP\_065*
- *Requirement IP\_098*
- *Requirement IP\_099*
- *Requirement IP\_101*
- *Requirement IP\_102*