Specification for interoperability of backend hybrid C-ITS communication

Version 1.5

C-Roads Platform

Working Group 2 Technical Aspects

Taskforce 4 Hybrid Communication

Co-financed by the European Union
Connecting Europe Facility

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

Table of Contents

List of Figures

1 Introduction

This specification aims to provide C-ITS service interoperability between C-ITS actors using IP backend communication.

1.1 Purpose of this document

The purpose of this document is to provide specifications and profiles for an IP based C-ITS interface needed for interoperability and backend communication.

1.2 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

1.3 Definitions

C-ITS Actors – entities or organisations which operate C-ITS stations and/or provide C-ITS services based on high quality traffic information

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.

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

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 Roadside System Profile (RSP).

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

1.4 References

- AMQP ISO/IEC 19464:2014
- C-ITS Infrastructure Functions and Specifications
- Roadside ITS G5 System Profile
- ETSI TS 103 097 V 1.3.1 ITS Security header and certificate formats

2 Scope of specification

This document provides a description of the functionality and profiles which are needed to provide hybrid communication via interconnection of backend systems to allow sharing of C-ITS information.

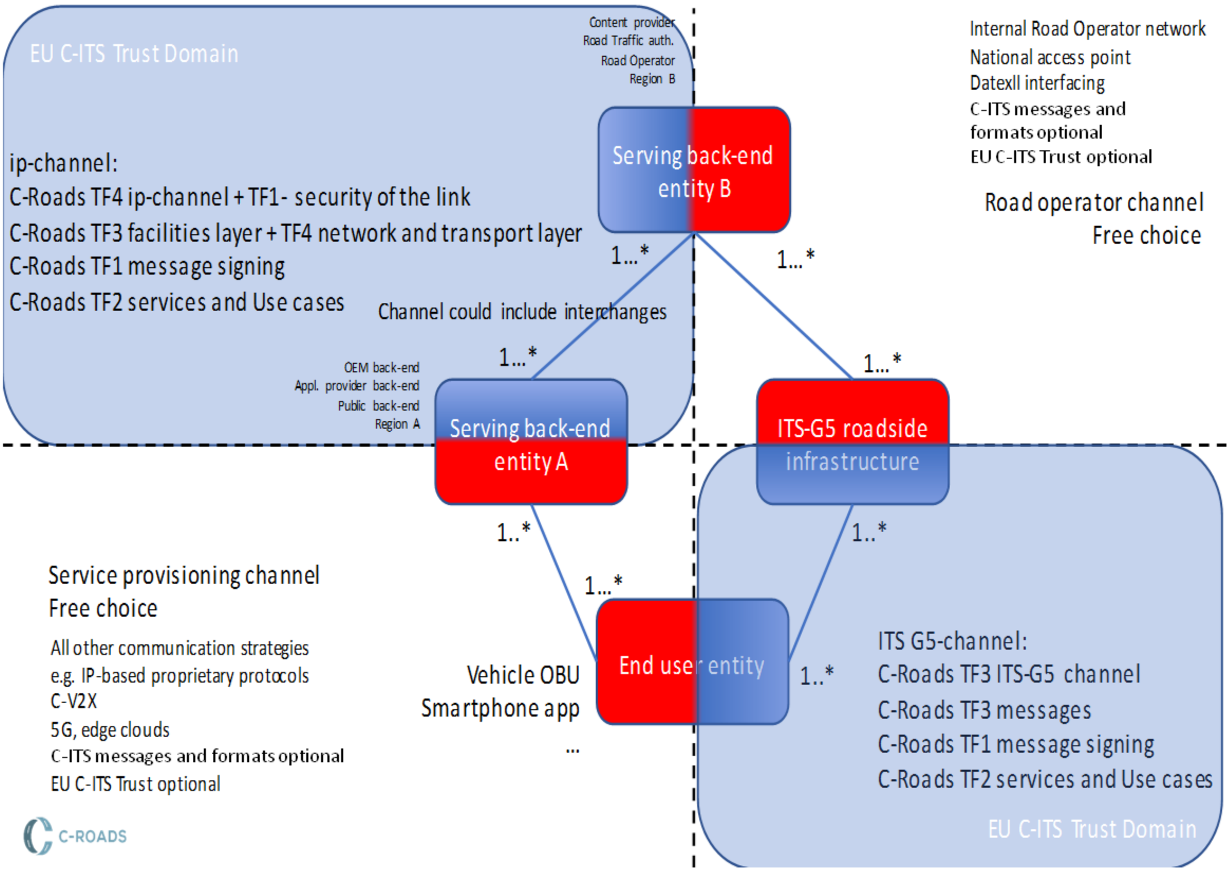

EU C-ITS Trust Domain
Content provider
Road Traffic auth.
Road Operator
Region B
Serving back-end entity B
Internal Road Operator network
National access point
Datexll interfacing
C-ITS messages and formats optional
EU C-ITS Trust optional
Road operator channel
Free choice
ip-channel:
C-Roads TF4 ip-channel + TF1- security of the link
C-Roads TF3 facilities layer + TF4 network and transport layer
C-Roads TF1 message signing
C-Roads TF2 services and Use cases
Channel could include interchanges
1...*
1...*
1...*
1...*
OEM back-end
Appl. provider back-end
Public back-end
Region A
Serving back-end entity A
ITS-G5 roadside infrastructure
1..*
1...*
1..*
Service provisioning channel
Free choice
All other communication strategies
e.g. IP-based proprietary protocols
C-V2X
5G, edge clouds
C-ITS messages and formats optional
EU C-ITS Trust optional
Vehicle OBU
Smartphone app
...
End user entity
1..*
ITS G5-channel:
C-Roads TF3 ITS-G5 channel
C-Roads TF3 messages
C-Roads TF1 message signing
C-Roads TF2 services and Use cases
EU C-ITS Trust Domain
C-ROADS

Figure 1 Overview of specification scope

Upper, left part shows the solution area related to hybrid communication via backend communication that is 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.

Lower, right shows the ITS-G5 communication.

3 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 2.
BI is independent of any deployment model that Member States or C-ITS actors choose to deploy.

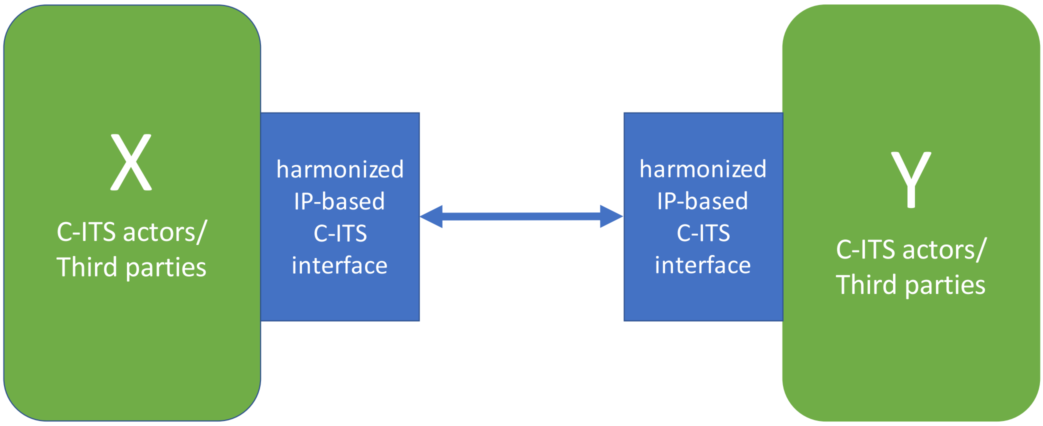


Figure 2: Basic IP interface for C-ITS message exchange

3.2 Functional requirements

Requirement HYB_001

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

Requirement HYB_002

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

Requirement HYB_003

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

Functional needs of C-ITS actors:

Requirement HYB_004

- BI shall allow C-ITS actors to publish and subscribe to C-ITS messages.

Requirement HYB_005

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

Requirement HYB_006

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

Requirement HYB_007

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

Requirement HYB_008

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

Logging

Requirement HYB_009

- Servers (both brokers and clients) should keep a log of the following for at least 3 months:
  - Queue filters
  - Client connect and disconnects
  - System and connection errors

Requirement HYB_010

- Servers (both brokers and clients) should keep a log of the following for at least 3 months for message types DENM, IVIM, SREM, SSEM, MAPEM:
  - AMQP Message timestamps precision of at least 1ms (Both arrival and departure)
  - AMQP Message headers

Requirement HYB_011

- Servers (both brokers and clients) can keep a log of the following for at least 1 month for message types SPATEM, CAM:
  - AMQP Message timestamps precision of at least 1ms (Both arrival and departure)
  - AMQP Message headers

Latency requirements for AMQP brokers

Requirement HYB_012

- A broker shall be able to route a single message with a payload size <500KB in <30ms. (from message arrival to available on client queue)

Requirement HYB_013

- A broker shall be able to route 5000 messages with a payload size <500KB in <1000ms. (from message arrival to available on client queues)

Integrity requirements for AMQP brokers

Requirement HYB_014

- A broker shall never remove, alter or add anything to a message payload as defined in chapter 3.4.

Requirement HYB_015

- A broker shall never remove or alter any of the message headers defined in 3.3.3.

Requirement HYB_016

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

Integrity responsibility of C-ITS actors

Requirement HYB_017

- C-ITS actors shall ensure the integrity of the information they exchange.

3.3 BI protocol specification

BI (Basic Interface) is the interface between C-ITS actors. On this interface the following 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.

Requirement HYB_018

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

Requirement HYB_019

- BI shall implement Transport Layer Security (TLS 1.3) according to RFC 8446. Profiling for TLS is described in chapter 3.4.3.

Requirement HYB_020

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

3.3.1 Filtering mechanism

The first release of this document focuses more on DENM and IVIM. Other messages filtering process will be detailed in next releases.

Requirement HYB_021

- All mandatory fields in Table 1 shall be present for publishing for all C-ITS messages.

Table 1 : Data field 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) and a numerical identifier (value between 0 and 16383 including leading zeroes) based on ISO 14816 (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
originatingCountry	Country code (based on ISO 3166-1 alpha-2	Country code where the C-ITS message is created	M
protocolVersion	string E.g. “DENM:1.2.2”	Represent the version of standard used to create the message	M
serviceType	String HLN-RLX ……	Acronym defined in C-Roads_Common C-ITS Service Definitions	O
messageType	String DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, CAM	This is the type of the published message	M
longitude	Float Decimal degrees	Longitude of the event published; for DENM (eventPosition) and for IVI (referencePosition)	O
latitude	Float Decimal degrees	Latitude of the event published; for DENM (eventPosition) and for IVI (referencePosition)	O
quadTree	String	Relevant spatial index location of the C-ITS message	M

Requirement HYB_022

- All mandatory fields defined in Table 1 shall be inside the AMQP header.

Requirement HYB_023

- All optional fields defined in Table 1 should be inside the AMQP header.

Requirement HYB_024

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

Requirement HYB_025

- All AMQP messages with a DENM as payload exchanged in BI shall contain information described in Table 2.

Requirement HYB_026

- All mandatory fields in Table 2 shall be present for publishing DENM.

Requirement HYB_027

- All optional fields in Table 2 should be present for publishing DENM.

Table 2 : *Data field for DENM filtering process*

Name	Value and type	Description	Mandatory/ Optional
CauseCode	String	CauseCode from ETSI_EN_302_637-3	M
subCauseCode	String	subCauseCode from TSI_EN_302_637-3; (in the case of absence of information, it is equivalent to unavailable)	O

Requirement HYB_028

- All AMQP messages with an IVIM as payload exchanged in BI shall contain information described in Table 3.

Requirement HYB_029

- All optional fields in Table 3 may be present for publishing IVIM.

Requirement HYB_030

- Wildcards can be used to obtain a subset of information. Without wildcards, the complete set of information is retrieved. An example for the use of wildcards would be: subset of protocolVersion = 1.* to exclude versions >1.

Table 3 : Data field for IVI filtering process

Name	Value and type	Description	Mandatory/ Optional
iviType	NUMERICAL	iviType	O
pictogramCategoryCode	NUMERICAL or a list of NUMERICALS. Either a single numerical value (e.g. 557) or a comma separated list (e.g. 557,559,612) of numerical values as an IVIM may contain more than one pictogramCategoryCode	The ISO 14823 pictogramCategoryCode is a combined numeral value (nature and serialNumber) referring to a specific sign of the ISO 14823 sign catalogue, e.g. 557 = Maximum speed limit	O
IviContainer	String All valid IviContainer abbreviations in the ISO 19321 standard, e.g. ”gic”, ”rcc”, ”tc”, ”avc” or comma separated combinations of that, e.g. ”gic,tc,avc”	All valid IviContainer types out of the ISO 19321 standard that should be present in the target IVIM after applying filtering	O

Note: Adding filtering element will be included in next release for CAM, SPATEM, MAPEM, SSEM, SREM.

Requirement HYB_031

- C-ITS actors who want to publish information on BI shall register for EN ISO 14816 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

3.3.2 Configuration parameters

Requirement HYB_032

- A broker shall provide a minimum queue length of 200 messages.

Requirement HYB_033

- An AMQP Message TTL shall be set based on the validity time of the payload. If this is not applicable the AMQP Message should have a minimum time to live of 60 seconds and a maximum of 10 minutes. A broker can directly enforce TTL policies, i.e. if TTL is not set, or dependent on message types.

Requirement HYB_034

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

Requirement HYB_035

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

Requirement HYB_036

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

3.3.3 Location specification

Requirement HYB_037

- Geolocation method shall be based on quadtree, for complete description please see Appendix A.

Requirement HYB_038

- C-ITS actors shall publish with a minimum zoom level of 18.

Requirement HYB_039

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

3.4 BI security specification

3.4.1 Security requirements

Requirement HYB_040

- According to the European C-ITS Certificate Policy (CP), individual messages shall be signed according to ETSI TS 103 097.

Requirement HYB_041

- The originating ITS station shall be responsible for the signature and the timestamping of the message content.

Requirement HYB_042

- No signature change during message transport from the original sender to the final receiver shall be allowed.

3.4.2 C-ITS message signing

Requirement HYB_043

- According to the European C-ITS Certificate Policy (CP), a CA part of the EU-PKI is used to issue certificates according to ETSI TS 103 097 V1.3.1 (i.e. 1609.2 certificates) to C-ITS actors for message signing according to ETSI ITS specifications i.e. for message signing by a Central C-ITS station.

Requirement HYB_044

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

Requirement HYB_045

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

Requirement HYB_046

- The security mechanisms related to this data interface shall respect all the provisions of the latest and valid version of the EU Certificate Policy – CP for C-ITS.

Requirement HYB_047

- When transmitting C-ITS messages via different channels (technologies/ networks) all specific ETSI certificates and ID´s created with them shall be preserved to guarantee message authenticity.

Requirement HYB_048

- In vehicles, the C2C-CC Basic System shall check the timestamp in the security envelope compared to the reception time and accept only CAMs in the last time of pSecCamToleranceTime and other messages within the last time of pSecMessageToleranceTime.
  with :
  - pSecCamToleranceTime = 2 s
  - pSecMessageToleranceTime = 10 mn

Each time a DENM or an IVIM is created and signed by C-ITS actors to be sent on BI , it shall be repeated each 9 min.

Requirement HYB_49

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

Additional information:
C-ITS actors need to keep every 9 min messages even if there are considered as duplicate messages.

3.4.3 Transport layer security

Requirement HYB_050

- For the transport layer protection TLS with mutual authentication shall be used, a Commercial, well establish CA shall be used for issuing standard X.509 certificates for long lived security associations between backend entities.

Requirement HYB_051

- Certificates renewal periods should follow security best practices.

Requirement HYB_052

- Security gateways/firewalls should be configured to further enhance security according to latest industry standards.

Requirement HYB_053

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

Requirement HYB_054

- Earlier versions of TLS shall not be supported.

Requirement HYB_055

- The rules on allowed and mandatory cipher and suites allowed and mandatory extensions given in TLS 1.3 (RFC 8446) shall be followed.

Requirement HYB_056

- Mutual authentication shall be done with X.509 certificates.

Requirement HYB_057

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

Requirement HYB_058

- Certificate Status Requests (OCSP stapling) as specified in [RFC6066] and Section 4.4.2.1 of [RFC8446] shall be supported and used.

Requirement HYB_059

- Later releases and verified revisions of TLS shall be supported.

3.4.4 TLS Certificates

The certificates used for authentication are standard X.509 TLS certificates [RFC 5280] and are supported by almost all CAs.

The TLS certificates are issued and signed by a trusted subordinate CA (sub CA) for interchange network certificates.

Requirement HYB_060

- The sub CA may belong to any of the trusted root CAs.

Requirement HYB_061

- The sub CA may be a national CA or a commercial CA.

Requirement HYB_062

- The TLS certificates used shall be Organization Validated (OV) certificates where both the domain and the organisation are validated.

Requirement HYB_063

- TLS certificates shall be version 3 certificate according to [RFC 5280].

Requirement HYB_064

- The public key algorithm shall be id-ecPublicKey with secp256r1 or secp384r1.

Requirement HYB_065

The security level of the signature algorithm shall be at least as strong as the public keys in the certificate, minimum 128 bit key length.

4 Future work items

Continued work for this specification is to define an **Improved Interface (II)** and different interfaces.

This Improved interface is a control plane interface that can be used between C-ITS actors to maintain and evolve the information exchange network over time. It will handle meta data about services that the C-ITS actors can deliver and how to get access to the relevant BI interface of the C-ITS actors. It will be specified as a second step with target delivery by the end of 2019.

Coming releases will also address

- Filtering process for additional message types (e.g. SPATEM, MAPEM, CAM, SSM, SRM)
- System scalability
- Deployment models analysis, discussion and decision on future implementations
- At the time of publication the specification only allows to sign messages on Geonetworking layer but ongoing work in ETSI (ETSI Work Item DTR/ITS-00551) will allow signing on facilities layer.

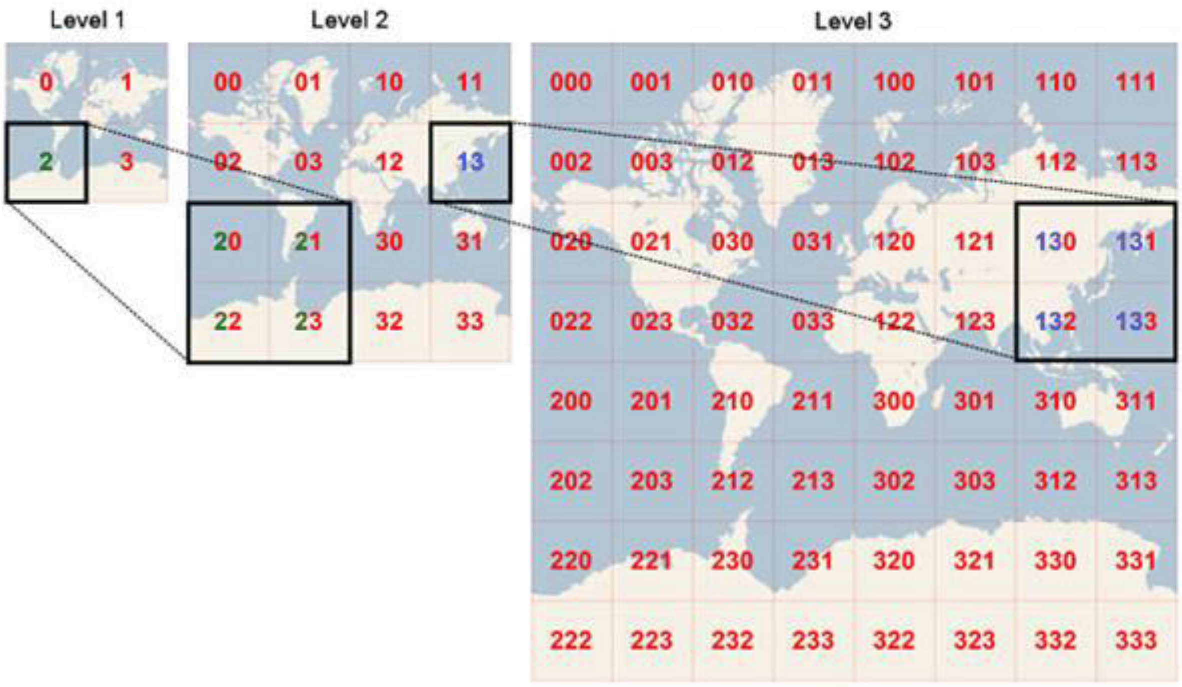
5 Appendix A Quadtree

Quadtree is a method to buid a data structure for distributing data streams w.r.t. geographic ar eas (single points, lines or links, areas), and used often inGIS (Geographic Information Systems) and backend servers.
Algorithm are explained in:
http://www.cs.tau.ac.il/~haimk/seminar12b/Quadtrees.pdftp://www.cs.tau.ac.il/~haimk/seminar12b/Quadtrees.pdf
More detailed with C-ITS relations of single points e.g. send as events and DENM messages and the request for a specific region / area: https://jimkang.com/quadtreevis/
Quadtreepath designates the consecutive tiles you have to go throw to obtain the desired tile. The number of characters for a quadtreepath is equal to the zoom level of this tile. For example: “1122” has 4 characters and designates a tile of level 4 and is somewhere in Siberia. Level 0 being the world.
At each level you slice each tile in 4 which means that you need 4 symbols to identify each of them.
It could be anything like “a, b, c and d” OR “hl, hr, bl, br”. We chose to do it with “0, 1, 2 and 3”.

0 being the top left tile.
1 the top right tile.
2 the bottom left tile.
3 the bottom right tile.

There is no limit for the number of level but we chose to stop at level 18, in Europe it represents a size of ~175m.

You can find the exact method to obtain the size of a tile by following these links: https://wiki.openstreetmap.org/wiki/Zoom_levels
https://docs.microsoft.com/en-us/bingmaps/articles/bing-maps-tile-system


Level 1
0 1
2 3
Level 2
00 01 10 11
02 03 12 13
20 21 30 31
22 23 32 33
Level 3
000 001 010 011 100 101 110 111
002 003 012 013 102 103 112 113
020 021 030 031 120 121 130 131
022 023 032 033 122 123 132 133
200 201 210 211 300 301 310 311
202 203 212 213 302 303 312 313
220 221 230 231 320 321 330 331
222 223 232 233 322 323 332 333