Work in progress !!!


# Hybrid solution description

# Version 0.0.3

**C-Roads Platform**
**Working Group 2 Technical Aspects**
**Taskforce 4 Hybrid**
**15/02/2019**

# Revision information and document handling

| Version | Date | Description | Status |
|---|---|---|---|
| 0.0.1 | 5.10.2018 | Draft for discussion in C-ROADS TF4. | Draft |
| 0.0.2 | 23.10.2018 | Updated following TF4 review comments and discussions. | Draft |
| 0.0.3 | 5.11.2018 | Updated following TF4 review comments and discussions.<br>Excel file comments addressed according to 'status' in exel file.<br>To address general document principles raised and comments received directly written in V002 version, modifications done according to the proposed (and agreed) actions discussed in the TF4 conf call 31.11.2018<br>(I.e. Some comments addressed without specific notation in excel file)<br>Scope first chapter<br>Clarification in privacy chapter<br>Clarification in logging chapter<br>Clarifications in solution overview<br>TLS and Certificate profile added (appendix C) | Draft |
| 0.0.3 | 25.01.2019 | Various clarifications and modifications<br>Basic interface made to focus, future improved interface made to background to be out of first review. | |
| 0.0.3 | 18.2.2019 | Updated according to:<br>-Excel review comments<br>-Agreement made at conf call 7/2<br>-Discussions with TF1 | |

# Index

Co-financed by the European Union

# 1 Scope and abbreviations

## 1.1 Abbreviations

| | |
|---|---|
| 3GPP | The standardization organization for cellular systems |
| AMQP | Advanced Message Queueing Protocol |
| C-ITS | Cooperative Intelligent Transport System |
| MNO | Mobile Network Operator |
| OBU | On Board Unit |
| RO | Road Operator |
| RSU | Road Side Unit |
| RTA | Road Traffic Authority |
| TLS | Transport Layer Security |

Editors note: To do

## 1.2 Scope for this document

This document provides a description of the functionality and profiles needed to interconnect backend systems to facilitate sharing of C-ITS information and more, e.g. future applications. Please note that this document also contains informative text to provide an understanding of the end-to-end system solution.
Figure 1 below provides a graphical overview of the different solution areas that form a cooperative intelligent transport system.

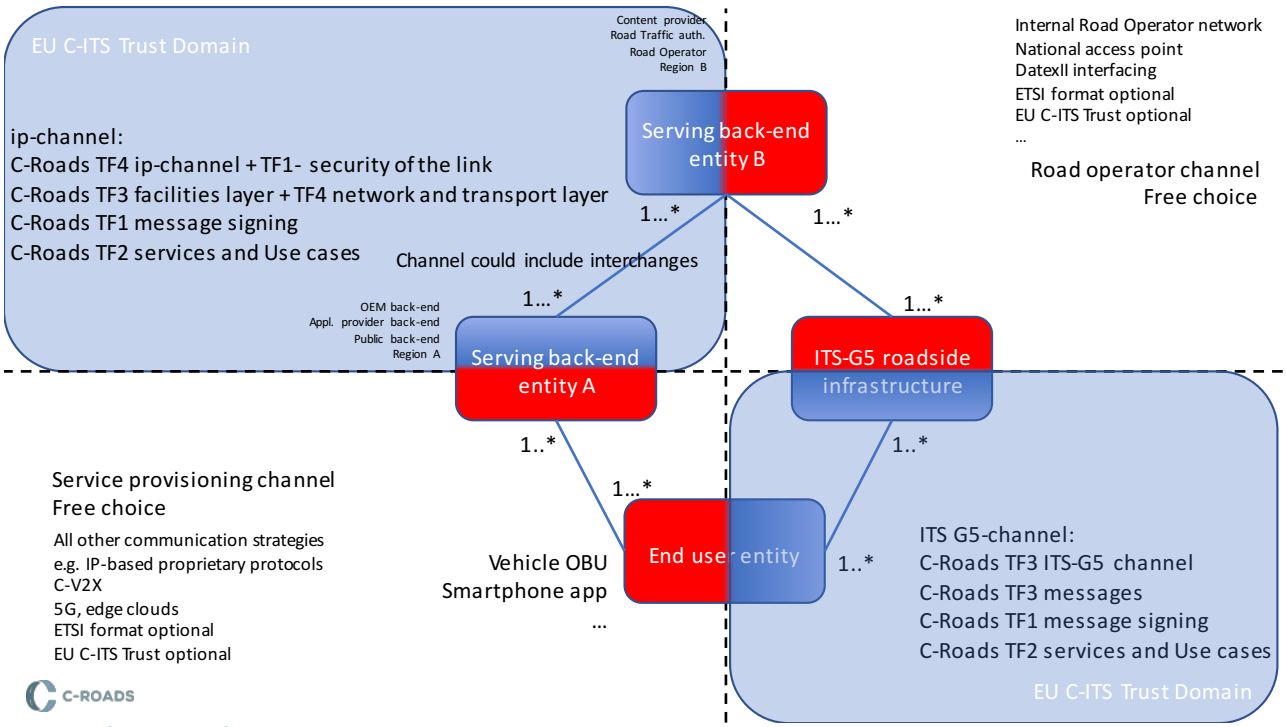


*Figure 1 Overview of TF4 scope*


Co-financed by the European Union

Upper, left part shows the solution area related to backend communication that is addressed by this document,
Lower, left part shows the solution area related communication between a backend entity and the end-user application, and it is up to each application on how this communication is performed or realized.
Upper, right shows the solution area related to communication internal to an implementation model, i.e. it is up to the implementation model how this is realized.
Lower, right show the ITS-G5 communication.

Important considerations and high-level solution requirements to consider are:

- A hybrid communication architecture should allow for different implementation models and different hybrid architectures
- A hybrid communication architecture should allow for road traffic authorities/road operators to communicate directly or indirectly (via OEMs or application providers) to vehicles
- Central C-ITS Stations can be implemented in backend systems
- Backend systems from different countries need to be interconnected (directly or indirectly) to provide an interoperable service across Europe
- A hybrid communication architecture should allow for communication using only Short range technology (e.g. ITS-G5) or long range cellular networks or both
- A hybrid communication architecture should allow for various personal devices (e.g. smartphones) as receivers of safety related traffic information
- Both cellular and ITS-G5 may be present at the same geographical location, however the hybrid solution would provide C-ITS services also with only one system present.
- The communication architecture needs to cater for a scalable and cost efficient system with 10.000.000+ vehicles from many different OEMs roaming all over Europe.

The first version of this description covers

- Architecture and related system functions
- Trust domain
- Security
- Transport level support needed for applications/services.
    - Services addressed in first release[1] are 'Road Works Warning (RWW)' and 'Hazardous Location Notification (HLN)'
- Summary and high level descriptions of 'Service descriptions and Use cases', full descriptions are available in TF2 documentation. Editors note: add reference to proper document number.
- Relation to short range technology
- Relation to cellular networks
- Profiles needed for interoperability

Figure 1 (the quadrant) view provides the top-level view of the architecture. Following this figure all types of backend entities are connected by communication links. Every backend entity can also be connected to non-backend entities.

Figure 2 is intended to show the internal structure of the backend with the Basic Interface (BI) and Improved Interface (II) communication links. These two interfaces are described in later chapters of this document.

[1] Additional Use cases and services such as traffic light information, In-vehicle signage etc, will be addressed in later revisions

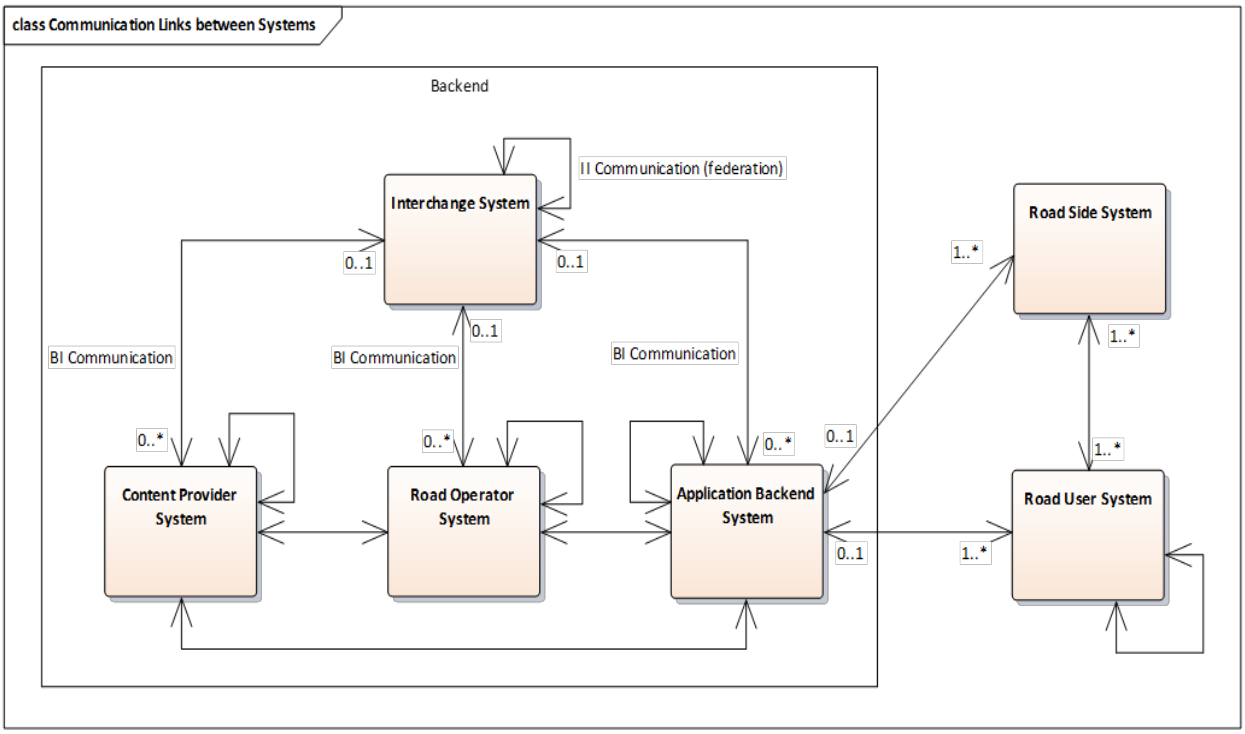


*Figure 2 Communication Links between Systems according to Services and Use case description*

Figure 2 includes all backend communication links. Communication links between non-backend entities and backend entities other than application backend entities are not shown. Figure 2 does not include all possible communication links of the Figure 1 quadrant view, nor does all communication links need to be used. The work in TF4 focuses on the following two types of communication links of the backend, BI communication between backend systems and II communication between interchange systems.
It should be noted that "direct" communication between content provider systems and road operator systems on one hand and non-backend systems is covered by considering application backend systems as submodules of the two backend systems
For a full description please refer to TF2 documentation regarding Services and Use cases.
Editors note: add reference, 'TF2 documentation' correct term ?

# 2 Definitions

The below definitions are used in this document and are described here to ease the understanding of this document.

Service providers are a generic term for the actors, service provider is used when no need to distinguish between the actors.

**Road Operator (RO) backend/system** is where applications related to a road operator (I.e. the entity that is responsible for certain roads) are hosted.

**Road Traffic Authority (RTA) backend/system** is where applications related to an RTA reside, the RTA could have interconnections to road side equipment/system, (e.g. RSUs), or operate without any specific roadside equipment.

**Application (provider) backend/system** hosts applications, such as a navigator or smartphone applications. An application backend system may also interact with Road side systems (e.g. RSUs) or interact with Road user systems (e.g. clients connected using cellular networks).
Application provider, content provider is used interchangeable in this document.

One example of an application provider or content provider used in this document is OEM backend which is the term used for an OEMs functionality to realize services related to the vehicles supplied by the OEM via a cellular connection. An OEM can be a seen as a special kind of service provider and are in some instances referred to using that term.

**Backend systems/servers** are referred to when no need to distinguish between the actors.

**Interchange system** is the functionality that facilitates information exchange between backend servers and can be used to enable scalability. A term used for that in this documentation is **Interchange entity (entities)**.

**'Trusted actor'** means a well-known, established and trustworthy actor on the market, known to be compliant to laws, rules and regulations. A trusted actor shall be governed as prescribed in section A of the C-ITS Security Policy which outlines the roles, responsibilities and requirements set on an actor to enrol in the EU-PKI, i.e. verified by an accredited PKI auditor (as for other Root CAs).

**BI (Basic Interface)** is the interface between backend actors or between backend actors and interchange entities.

**II (Improved – Interface)** is the interface between Interchange entities.

# 3 Introduction to implementation models [Informative]

Different implementation models are discussed to realize C-ITS services as well as other services such as traffic related safety, traffic optimization services to increase traffic flow on roads etc. Some different implementation models are exemplified in Figure 3 below.
Note: not all variants of implementation models are shown, these examples are provided and explained to provide an understanding of an end to end solution.

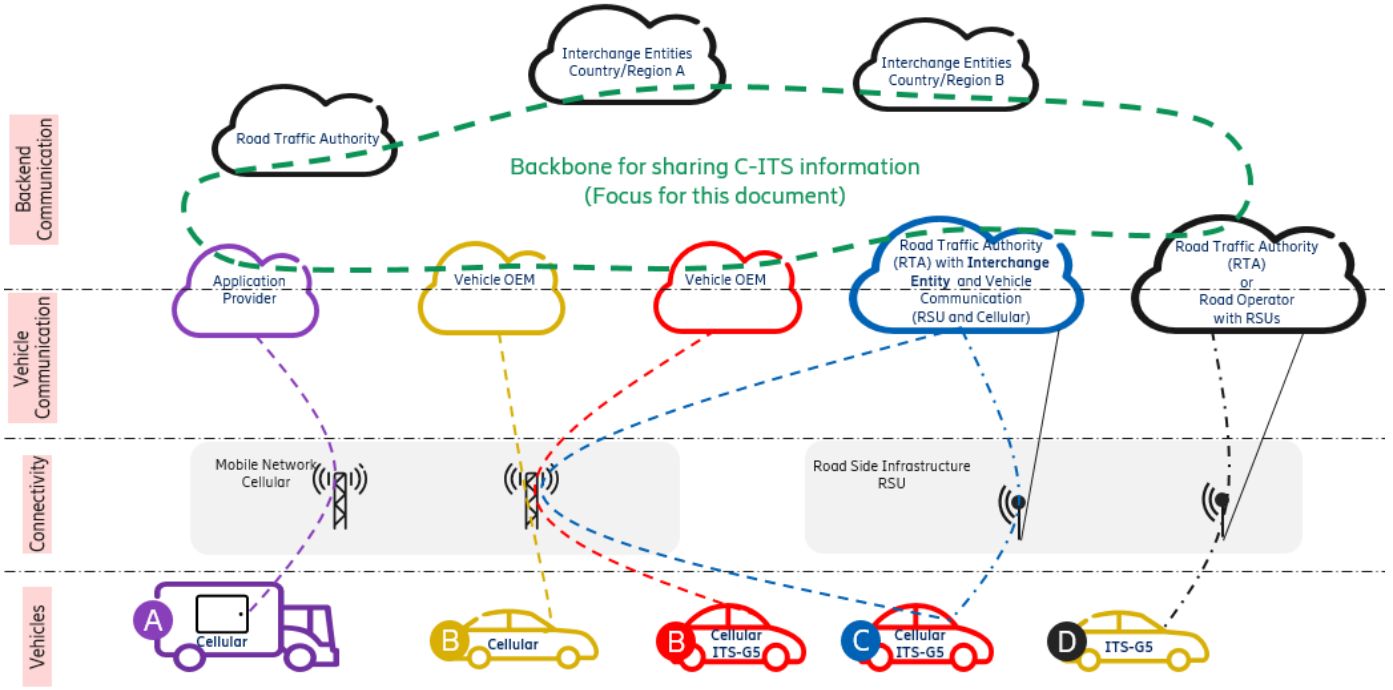


*Figure 3 Overview of implementation models*

The 'Backbone' for sharing of C-ITS information consists of interconnected trusted actors, e.g. C-ITS actors. (In this version, C-ITS information refers to UCs RWW and HLN)
Short introduction of above Figure 3 from left to right (referring to the circles with a letter).

- **Implementation model A** is to include additional communication devices in the C-ITS ecosystem, e.g. smartphones,navigators. In this scenario, the devices communicate with their application. This communication path to the devices may be used by Road Traffic Authorities/road operators in agreement with application providers. In this scenario, it is the application providers and the road traffic authority/road operator that are the trusted actors. (note: this type of devices may be used outside vehicles as well, e.g. for Vulnerable road users).
- **Implementation model B** is to use the OEM and its existing connection to its vehicles for C-ITS. This communication path to vehicles may be used by Road Traffic Authorities/road operators in agreement with OEMs. In this scenario, the OEM and the road traffic Authority/road operator are the trusted actors.
- **Implementation model C** is to have a dedicated connection from vehicles to Road traffic Authorities for C-ITS, either using cellular and/or short-range communication via Road Side Units (RSUs). In this scenario, the Road traffic Authority is the trusted actor.
- **Implementation model D** is that road traffic authorities or Road operators use RSUs to communicate with vehicles. In this scenario, the Road traffic Authority and/or the Road operator are the trusted actors.

Not shown in Figure 3, is the combination of using model B and model D, i.e. a vehicle using its cellular long range communication to connect to its OEM and have short range capabilities to communicate with RSUs.

Worth noting, and clarifying is that the interpretation of the term 'Hybrid' differs, the term 'Hybrid' can mean that the identical message that is sent on short range technology also can be sent on cellular, Another, wider meaning is just that cellular is used to convey C-ITS information, without specifying any message format, i.e. that could be the case for

implementation model B where an OEM is responsible for conveying the information between its backend system and its vehicles.
Depending on different implementation model, different important functionality will be distributed among the different actors as illustrated in Figure 4 below.

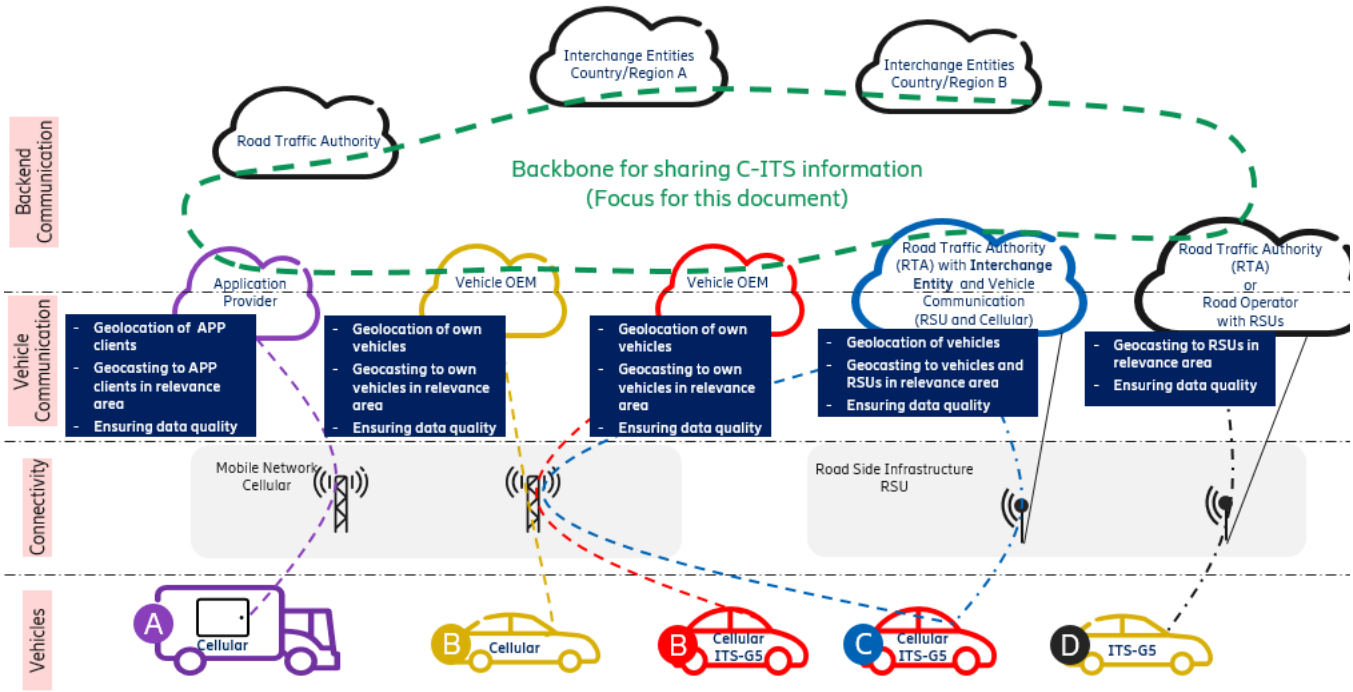


*Figure 4 Functional distribution*

Three important functions are, geolocation, geo-casting and quality of data.

- Geolocation means the functionality to know the location[2] of the vehicles/clients, enabling to inform only vehicles/clients in a specific relevance area. To keep track of vehicle/client location, a user consent would be needed due to privacy. To exemplify, a service provider (E.g. an OEM or application provider) would likely have a user consent in place due to existing services provided, thus can maintain information about its users' locations.

- Geo-casting means the functionality to distribute information to vehicles and devices in relevant areas.

- Ensuring quality of data means that before sharing data with other actors/vehicles/clients, confidence in the data is built to maintain confidence of information. Confidence in data can for example be achieved by analysing input from many sources, e.g. to avoid that a faulty sensor on one vehicle leads to that information about a slippery road is distributed. An entity having user consent in place and aggregating information can store information received from clients and perform analytics to identify misbehaving/faulty clients. Also, in a vehicle quality of data can be improved by applying sensor fusion, e.g. if snow is detected at the same time as wheel traction detects slippery road. How to achieve quality of data is being studied and discussed in the industry. It is not further elaborated in this document.

[2] The resolution of the location information can be very large, e.g. tiles of several kilometres, to assure privacy.


Co-financed by the European Union

Another way of doing geolocation/geo-casting being discussed is the concept of “interest areas”. In this concept, a user declares the area of interest to an application. The application then always delivers information from that area to the user whether the user is present in that area or not. Such a concept could increase the privacy aspect, since the application is not aware if the users are in the actual area of interest or not, however this is with the cost of additional data traffic to the user, i.e. information sent to user even if user is not in area of interest. If the area of interest is small and if area of interest is changed frequently then the application would still be able to know the users’ approximate locations, e.g. if user updates area of interest as the user is moving, then it will be an indication that user moves to new area.

Depending on implementation models and evolution of the ecosystem, additional actors could be present in the future. For example, it is likely that public safety organisations could join to provide information about emergency vehicles such as fire trucks and ambulances, and parking companies could join to announce parking possibilities etc.
Furthermore, the EU Commission have in Delegated Regulation 2015/962 specified that DATEX II[3] should be used e.g. for Real Time Traffic Information (RTTI) and Safety Related Traffic Information (SRTI).
Therefore, it is important to have an architecture that allows different implementation models, evolution, scalability and easy ways to join the ecosystem. This objective can be fulfilled by ensuring interoperability in backend systems by using industry standards to interconnect backend systems.
Thus, the interoperability and scalability using communication between backend systems is the focus of this document.

# 4 Architecture

All the actors could be considered to be service providers. However, to ease understanding of the following descriptions/examples, a distinction has been done between service providers (e.g. OEM, application provider) and providers of road infrastructure (e.g. Road Traffic Authority (RTA) and Road operators (ROs)

Editors note: Potentially Basic interface and Improved Interface details can be lifted out to separate specifications to allow them to evolve independently (currently interface/protocol details in appendix). To be concluded.

## 4.1 Basic network architecture for information sharing with Service providers

The service providers typically operate in one country/region and share information to/from its clients located in that country/region. The service provider connects to entities in the relevant country to consume or provide information e.g. from/to a RTA/RO. The service provider may operate in additional countries/regions and connect directly to the relevant actors in those countries/regions for information sharing. To facilitate this information sharing, an Interface/protocol named **BI (Basic Interface)** is introduced**.** Two network scenarios are exemplified below.

[3] The delegated act also includes the following statement: "or any machine-readable format fully compatible and interoperable with DATEX II"

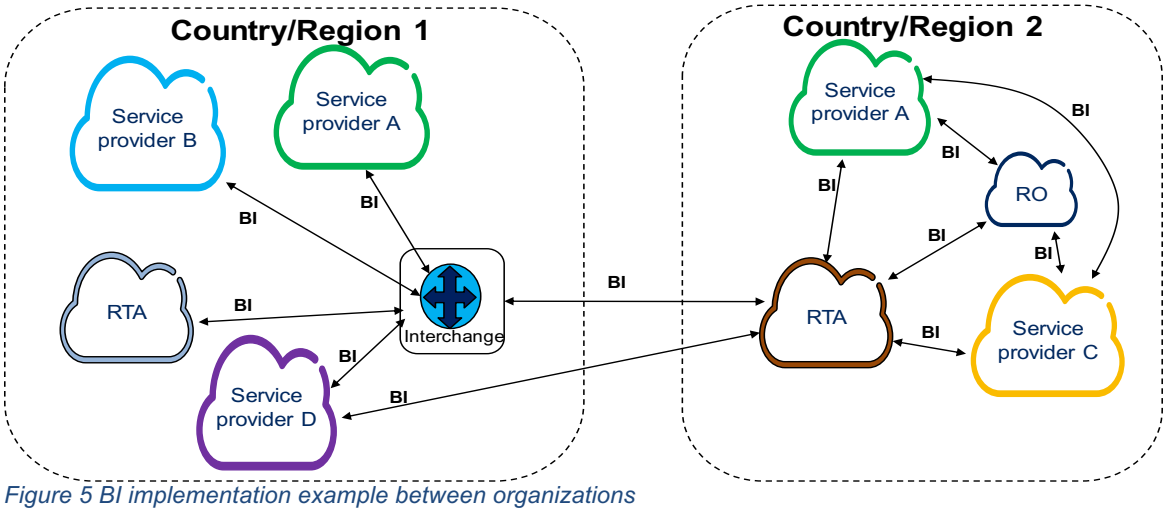


*Figure 5 BI implementation example between organizations*

In Figure 5, a simplified illustration of the basic network architecture scenario is illustrated with the BI between backend system. In this example two different approaches are exemplified.

- Country/region 1 is using an interchange entity that interconnect actors. (Note. Interchange entity is functionality than can be supported by backend servers)
  The interchange entity provides publish/subscribe mechanisms to facilitate information sharing between the actors, e.g. information received from the RTA is distributed to all service providers that have subscribed to the information, the replication is handled by the Interchange entity without the RTA needing to replicate it to all interested actors.

- In country/region 2, Actors interconnect with direct (logical) connections and provides publish/subscribe mechanisms to share information between them, I.e. service providers connect directly to RTA and RO for information sharing. Also, RTA and RO are interconnected to share information. In this scenario, an RTA would have to replicate and send information to all subscribing actors individually on the direct connections.

Figure 5 further exemplifies that there potentially are different strategies among Service providers, e.g. OEMs and application providers for their backend systems which need to be considered for a solution. Figure explanation:

- 'Service provider A' has instances of it's backend system in several regions/countries. Each backend instance is then connected to relevant actors. This is for example a common approach for many OEMs, then vehicles connect to the 'best' OEM backend instance depending on vehicle location.
- 'Service provider B' is active in one country/region and its backend is interconnected with the Interchange entity in that country/region.
- 'Service provider C' has a backend instance in region/country 2 and is directly connected to RTA and RO in that country/region. To share information with service provider A about events in country/region 2, an additional direct connection is established between the service providers A and C.
- 'Service provider D' has a backend instance in one region/country 1 and is connected to interchange entity in country/region 1 and, also directly to RTA in country/region 2 in order to provide services for its clients located in country/region 2. The service provider can thus support information sharing for its clients in both these countries/regions. In this scenario the interchange entity in country/region 1 and RTA in country/region 2 needs to provide a common BI to avoid that the 'Service provider D' needs to implement multiple protocols. To obtain and share information with RO and service providers in country/region 2, Service provider D would need an additional direct connection to RO(s) and service providers in country/region 2.

- There is also a BI established between RTA in in country/region 2 and Interchange entity in country/region 1 for information exchange.

### 4.1.1 BI protocol/profiles

- **BI (Basic Interface)**: Is the interface between backend actors or between backend actors and interchange entities, on this interface the following protocols and profiles shall be used for C-ITS services to facilitate a uniform implementation across Europe for service providers, i.e. avoid that a service provider with operations in several countries need to implement several different protocols.

    - Internet Protocol (IPv4/IPv6) and Transmission Control Protocol (TCP)
        - Supported by basically all operating systems
    - Transport Layer Security (TLS 1.3) according to RFC 8446 shall be used for the operational phase, for pilot phase deployments, TLS 1.2 can be used.
        - Profiling for TLS described in Appendix B
    - Advanced Message Queuing Protocol (AMQP) according to OASIS specification for version 1.0
      Profiling and details for AMQP on BI is described in Appendix A.
    - Payload
        - AMQP is payload agnostic, i.e. different payload formats can be carried.

### 4.1.2 BI procedures overview

The Service providers (e.g. OEMs, application providers), RTAs connect to the relevant actor, e.g. Interchange entity, RTA, RO using the BI and subscribe using AMQP to the information they are interested in, e.g. based on type of payload (e.g. ETSI DENM format, DATEX II format), country, type of event. To exemplify using Figure 5:

- The ‘Service provider A’ would thus connect and subscribe from its backend instances in respective region/country directly from relevant producers of information, i.e. in country/region 1 from the Interchange entity, in country/region 2 direct from the RTA and RO.
- The ‘Service provider B’ would connect and subscribe from its backend instance to the Interchange entity in the region/country 1.
- The ‘Service provider C’ would connect and subscribe to the RTA and RO in country/region 2.
- The ‘Service provider D’ would thus connect and subscribe from its backend instance directly from the Interchange entity in country/region 1, and to RTA in country/region 2 (to interact with RO in country/region 2 an additional direct connection would be needed).
- The RTAs/ROs would subscribe to information related to their country/road to get informed about accidents, road conditions etc. detected by service provider clients, e.g. a slippery road detected by vehicles sensors.

### 4.1.3 BI message flows: Establishment of secure sessions and application initialization

Below in Figure 6 it is exemplified, how secure TLS sessions and application communication are established in country/region1 using an interchange entity.
The below example shows BI establishment from an OEM backend to an Interchange entity, and BI establishment from an RTA to an Interchange entity, however same BI procedures would

be present for other types of service provider backends. (Also, an example of the backend to client procedure is shown for completeness).

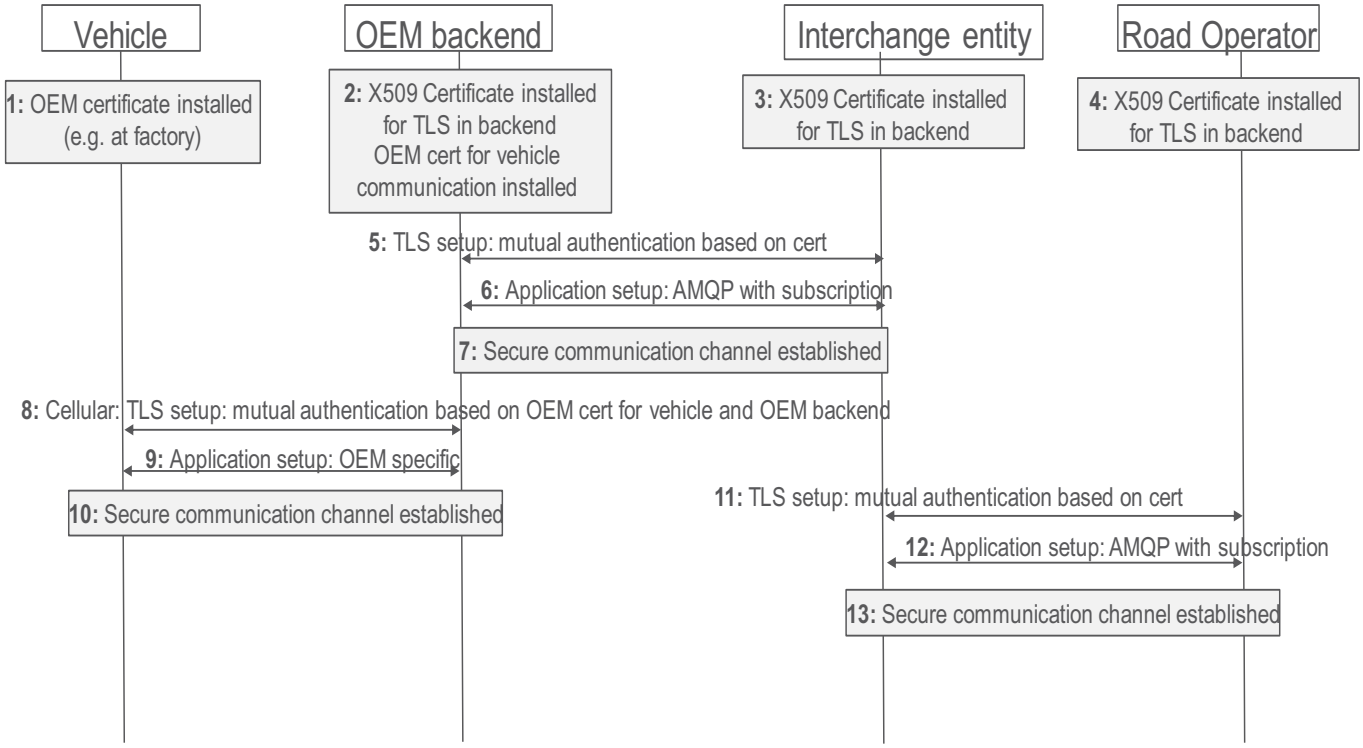


*Figure 6 Example of secure TLS session and application communication establishment*

For backend transport security, TLS and industry standard X509 certificates are used. Transport layer security using TLS and Application layer security according to ETSI TS 103 097 are further elaborated in chapter 5.

1. OEM have certificate installed in vehicle at factory, using a Certificate Authority (CA) of OEM choice.
2. OEM have downloaded and installed a certificate from a Certificate Authority (CA), e.g. from a commercial CA.
3. Interchange entity have downloaded and installed a certificate from a Certificate Authority (CA), e.g. from a commercial CA.
4. Road operator have downloaded and installed a certificate a Certificate Authority (CA), e.g. from a commercial CA.
5. A TLS session using the certificates for mutual authentication is established between OEM backend and interchange entity. Both the OEM and the vehicle execute a certification chain validation based on the cert received during the handshake.
6. OEM requests subscription from interchange entity using AMQP
7. A secure communication channel is established between OEM and interchange entity
8. 9, 10. The OEM establish communication with its vehicles. (this step likely performed earlier, i.e. since needed for things like telematics),
11. A TLS session using the certificates for mutual authentication is established between Road Operator and interchange entity. Both the Road Operator and the vehicle execute a certification chain validation based on the cert received during the handshake.

12. Road operator requests subscription on information related to the area related to the managed roads from interchange entity using AMQP
13. A secure communication channel is established between Road Operator and interchange entity

Now information can be securely exchanged between actors, to exemplify, Road operator can send information about a road work to the interchange entity indicating location in AMQP application properties, interchange entity forwards the information to OEM (assuming OEM has subscribed to this type of information or information related to this location). Finally, the OEM distributes the information to vehicles that may be in the location or may be affected due to their current position.

In the scenario with country/region 2, the Interchange entity (refer to Figure 5 above) would not be present so procedures are executed direct between service providers (e.g. OEM backends and RO/RTA), and between all actors that should share information.

## 4.2 Evolved network architecture for sharing information between countries/regions

To facilitate scaling and automatic service discovery between countries/regions an additional interface with a more advanced protocol is foreseen.
This protocol would allow that an actor using one Interchange entity can be served with information related to another country/region without needing to establish direct (logical) connections there, i.e. relieve a service provider the cumbersome task to obtain addresses to data sources in other part of Europe and maintain connections.
To obtain and maintain addresses and connections to data sources would be manageable in an initial phase with a low number of actors, but when many data sources are to be used, e.g. Traffic Light Controllers (TLCs) which could be many in a country, e.g. several TLCs in a city the concept of direct (logical) connections would have problems to sustain.
Also, information from a TLC is more latency critical (e.g. compared to a road works warning), the foreseen protocol would facilitate that data can be fetched directly by service providers from the data sources in an automatic way, thus optimize the data path used and keep down latency.
This 'federation' of information and advanced protocol is worked on in other EU project for C-ITS and will be addressed at a later stage.

For information the current understanding of this advanced protocol is described in Annex
Editors note: Annex not part of review

### 4.2.1 II protocol/profiles

To be completed.

### 4.2.2 II procedures overview

To be completed.

### 4.2.3 Evolved architecture overview

To be completed.

# 5 Security

## 5.1 Backend trust domain

Figure 7 below show the boundaries for the C-ITS backend trust domain.

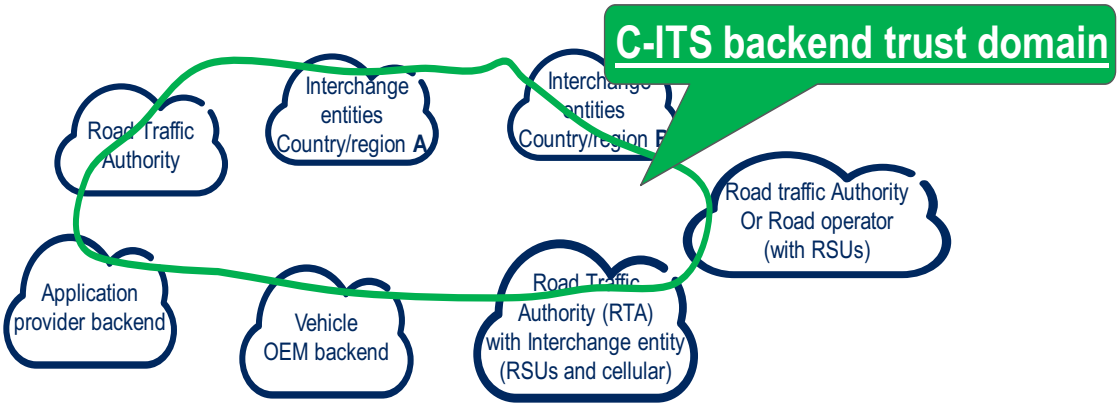


*Figure 7 C-ITS backend trust domain*

In the C-ITS backend trust domain, communication is between a relatively low number of trusted actors that are mutually authenticated at session establishment based on the certificates exchanged.
Depending on what is supported by the used Certificate Authority (CA), Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs) can be used to check the validity of a received certificate
The backend entities are provisioned with certificates on 'Organizational' level, e.g. indicating an OEM, a road authority in a country etc. to provide 'privacy', i.e. certificates do not contain any individual user information.
Transport level security between actors are based on TLS which is a mass market industry standard, thus security in C-ITS backend trust domain can leverage on future evolution and mitigation of security issues.

- TLS provides:
  - Mutual authentication
  - Confidentiality protection
  - Integrity protection
  - Replay protection

Security gateways/firewalls can be configured to further enhance security, e.g. by IP address white lists only allowing trusted actors. Also, the AMQP protocol level provides security by username/password.
For transport level security with TLS in the C-ITS backend trust domain, all payload is protected on transport level between actors.
For ETSI level security, individual message shall be signed according to ETSI TS 103 097 to provide non-repudiation if required/needed.

## 5.2 Public Key Infrastructure (PKI)

Below in Figure 8 shows an example outline of the PKI setup.

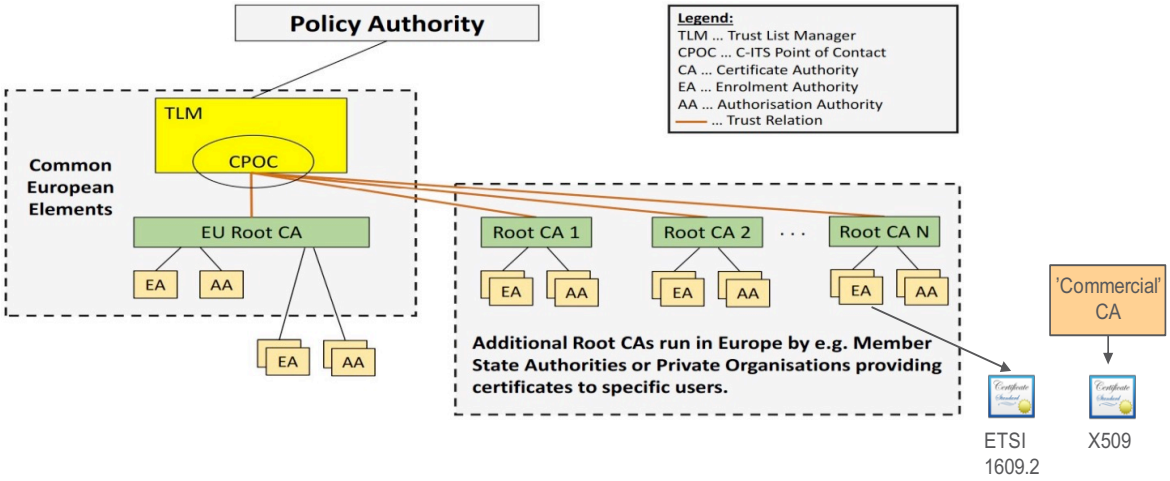


*Figure 8 PKI with sub CA for C-ITS backend trust domain*

A CA part of the EU-PKI is used to issue certificates according to ETSI TS 103 097 (i.e. 1609.2 certificates) to backend entities in the interchange network for message signing according to ETSI ITS specifications, i.e. for message signing by a Central C-ITS station if required/needed.

For TLS, a Commercial, well establish CA can be used for issuing standard X509 certificates for long lived security associations between backend entities. i.e. certificates renewal periods can follow industry practices. Using an established, commercial CA for X509 certificates simplifies verification of certificates between actors.
Hierarchies with Sub-CAs could be created for example to separate certificates issued to authorities and private companies.

## 5.3 Certificates

The CAs used for the ETSI TS 103 097 certificate issuing should be part of the European Certificate Trust List (ECTL) to achieve a common trust for the C-ITS backbone trust domain.

The ETSI TS 103 097 certificates used in the C-ITS backend trust domain could be on 'organizational' level, e.g. indicating a car manufacturer, a road authority in a country etc. to ensure privacy. I.e. there is no need to use anonymous certificates since no individual/personal information is exchanged on this interface since anonymization is handled by applications before information is shared in the C-ITS backend trust domain. (e.g. anonymized by the OEM backend, application provider backend, etc).

The ETSI TS 103 097 certificates used in the C-ITS backend trust domain can have a longer validity time than those used in vehicles on the road, since no complex revocation and/or pseudonymization is required between known and trusted backend systems. Based on current policy requirements, 3 months validity time is assumed for Central C-ITS stations in the C-ITS backend trust domain.
Editors note :Regulations unclear, Discussions ongoing in TF1 how to handle.

The ETSI TS 103 097 certificates are used for signing individual messages according to ETSI security principles.
The X509 certificates are used to establish the secure transport connection, i.e. actors exchange certificates and establish a secure TLS connection where all future communication is exchanged having all payload between actors protected.

# 6 Privacy

A service provider handling user data must comply to GDPR. In order to fulfill GDPR, backend systems that handle personal data could remove certain personal data and should anonymize as much as possible before sharing information with other actors, e.g. sharing information with traffic authorities or other OEMs.
This task can be performed by backend systems that have a user consent in place. (e.g. vehicle or personal device owner most likely already has a consent in place with its Service provider for existing services offered by the service provider.)
Note: the transport layer does not include any information that can identify an individual, only necessary location information is conveyed.

# 7 Logging

For misbehavior and fault detection, backend actors shall log sent/received events with timestamps. For backend actors with a user consent in place, identification of individual can be logged for misbehavior/fault analysis. Logs should be kept for at least 6 months to comply with the EU data retention directive
Actors should use NTP (Network Time Protocol) to sync on time of day to allow correlation of logged information, e.g. by using NTP servers from europe.pool.ntp.org
Editors note: suggestion from MS (UK) to add more details about logging, to be discussed.

# 8 Liability for information distribution [Informative]

The current understanding is that there are no liability concerns for day 1 & 1.5 use cases. There are several reasons for this approach, e.g. even though cellular networks employ mechanisms to secure communication, radio communication is by nature difficult to guarantee therefore radio communication should be considered as ‘an additional sensor input’ that needs to be fused with other sensors, such as cameras to make an educated decision. Furthermore, physical infrastructure, e.g. traffic lights, road signs etc. will for a foreseeable future overrule information received on radio, especially when using todays exiting application protocols that do not include acknowledgements that information received, when it was received etc. making liability based on radio communication infeasible. This leads to that information provided to actors is of ‘informal nature’.

Informational note: There are work ongoing in the industry for more advanced application protocols to allow acknowledgements, negotiations etc.

# 9 Positioning and geographical distribution

Editors note: move this chapter (or parts of it), e.g. to BI part

The backend actors provide geographical position (latitude/longitude) on the BI interface when sharing information about an event, i.e. geographical position in AMQP headers. Backend actors can also include relevance area if possible, to determine or received from reporting vehicle/client. An example of relevance area could be a road segment/road stretch, or a square area indicated by 4 geographical positions, if backend can obtain this information is dependent on information available.

The Interchange entity use the received geographical position in AMQP headers to disseminate the information to actors that has subscribed to information related to this geographical position (AMQP and the Interchange provides additional filtering mechanisms for more specific subscriptions).

The service provider backend in most cases have knowledge about the actual position of its clients at some granularity and decides to which relevant vehicles the information is distributed to, also considering indicated relevance area (if available), i.e. the service provider backend handles the 'Geo casting' functionality.
Same for other consumers of the information, e.g. for smartphone applications it is the related application provider that distributes the information to relevant devices.

# 10 Short range technology considerations

This chapter describes interaction and relations between short range technology and long range technology (cellular).

## 10.1 Interaction with short range technology

If short range technology exists, it is the responsibility of the road traffic authority/operator/ Road side infrastructure operator to handle distribution of information received from other sources to relevant road side units. E.g. the operator of road side units can connect to the C-ITS backend trust domain, subscribe to events shared on the C-ITS backend trust domain and distribute relevant information to relevant road side units. The operator of road side units can also provide information to the C-ITS backend trust domain to be shared among backend actors.

## 10.2 Cooperative Awareness messages (CAM)

Handling of CAM messages are not part of this revision.

## 10.3 Event identification

If an event message is sent on both long range cellular and short range technology, the event identifier shall be the same.

Editors note: Propose to use the action identifier for this purpose, i.e. Action ID in a DENM message will remain the same across both short & long range communication.

However, events will be generated from multiple sources, e.g. at an accident several vehicles will generate messages related to the same event, it will eventually be up to the OEM/application/road traffic authority implementation to filter out and decide what to present dependent on the event and location of the event.

# 11 Cellular networks [Informative]

The long range (cellular leg) works without any special handling in cellular networks nor is any special interaction with the cellular networks needed for basic communication, i.e. vehicles and smartphones can just use the cellular connection as a normal 'Internet' connection with the ordinary subscription to any Mobile Network Operator (MNO). However, there are

standardized features in mobile networks that potentially can be used to optimize for C-ITS as described below. These features would however incur a cost for the MNOs.

## 11.1 Quality of service (Priority for ITS information)

Mobile networks can be configured to identify certain traffic flows based on the IP five tuple (IP addresses, port numbers, protocol), this can be used to provide quality of service and priority for ITS information over normal Internet traffic in case of high load in the mobile network.

This requires that the MNO is informed about one of the identifiers from the IP five tuple and configure the network accordingly. For C-ITS actors this means that they need to use a certain IP address and/or port for their communication with their clients (e.g. vehicles/smartphone applications) and that the MNO is informed about the used identifier so that the mobile network can be configured accordingly.
A port number (port number on receiver side) can be agreed/standardized as identifier to simplify MNO configuration.

## 11.2 Charging (Different tariff for ITS information)

The identification of flows (as described for 'Quality of service and priority for ITS information') can also be used to configure different tariffs for ITS information. This can be used to separate the costs for ITS information transfer on the cellular networks, e.g. to fulfil requirements on different charging for traffic related information that should be provided free of charge to end users as outlined in various regulations.

## 11.3 Cross border (Mobile network change)

When changing serving MNO an interruption in connectivity usually occurs due to reselection of frequency and attachment to new serving MNO. This interruption can be substantially reduced or eliminated by features available in cellular networks, however these features are seldom activated between MNOs.
The interruption time is relative to the configuring effort needed, how to reduce or even eliminate the interruption time is described in (editors note: add references)

## 11.4 Latency and Distributed computing

Cellular networks of today provide low latency, a common performance is around 20-40 millisecond to reach a server on Internet, so C-ITS day 1 and 1.5 use cases can be supported. For C-ITS information exchange, ´car to backend to car' latency has been shown to be in the range of 50-150 ms when using (early version of) LTE in PoCs[4]. However, the latency is strongly dependent on the implementation and the design of the geocast function and protocol translation, which may add 1-2 seconds to the latency. For future use cases, e.g. related to autonomous vehicles a lower latency may be needed, this can be achieved by placing equipment to provide hosting of needed applications (e.g. compute and storage) in the MNO and by that reduce the latency added by transport and Internet. In a cellular radio network, User Equipment (UEs) are put into 'inactivity' state on the radio interface when no traffic for certain time (configurable by MNO), this to optimize battery consumption and to maximize the number of UEs that can be served, this result in some additional latency when UEs are brought back to connected state again. However, this additional latency can be eliminated since a vehicle in operation do not suffer from battery constraints it can be in connected mode, thus remove the radio connection establishment latency, i.e. no radio sleep modes necessary.

[4] https://www.etsi.org/deliver/etsi_tr/102900_102999/102962/01.01.01_60/tr_102962v010101p.pdf

## 11.5 Network slicing (virtual private network)

A virtual private (cellular) network can be established by an MNO so that dedicated resources are used for ITS services. (Editors note: Add more description)

# 12 References

(Editors note: to do)

# 13 Appendix A: AMQP, headers and example flow

Editors note: *This chapter presents a basic working solution for BI. However the discussion about all technical specification on BI such as header, the filtering, the software version, the application properties, the geographical information and so on continues within TF4.*
*It is also investigated if several methods can co-exist or if a certain method needs to be selected.*

To be updated with final list of headers/application properties for first version.
Alignment with other Proof of concepts using AMQP needed and ongoing, e.g. with Intercor.

This appendix provides information how to use AMQP, also additional information needs to be consulted, e.g. Advanced Message Queuing Protocol (AMQP) specification available at:
OASIS specification for version 1.0

The text description in this section use the term Interchange and interchange entity to denote the AMQP broker and related functionality for a scenario where a central entity handles AMQP functionality. If actors are directly inter-connected both sides would have to handle the AMQP broker and related functionality, in such case the Interchange entity should be read as the endpoint for the communication.

**AMQP and Interchange overview**

**Header** – this includes username and time to live (of the AMQP message).

**Application-specific properties** – Header fields set by the client and used by the interchange to route the message to the correct consumer queues.

**Body** – Contains payload, an interchange entity is payload agnostic as can be seen in Figure 9, examples are given below how to set the application properties for different payloads.

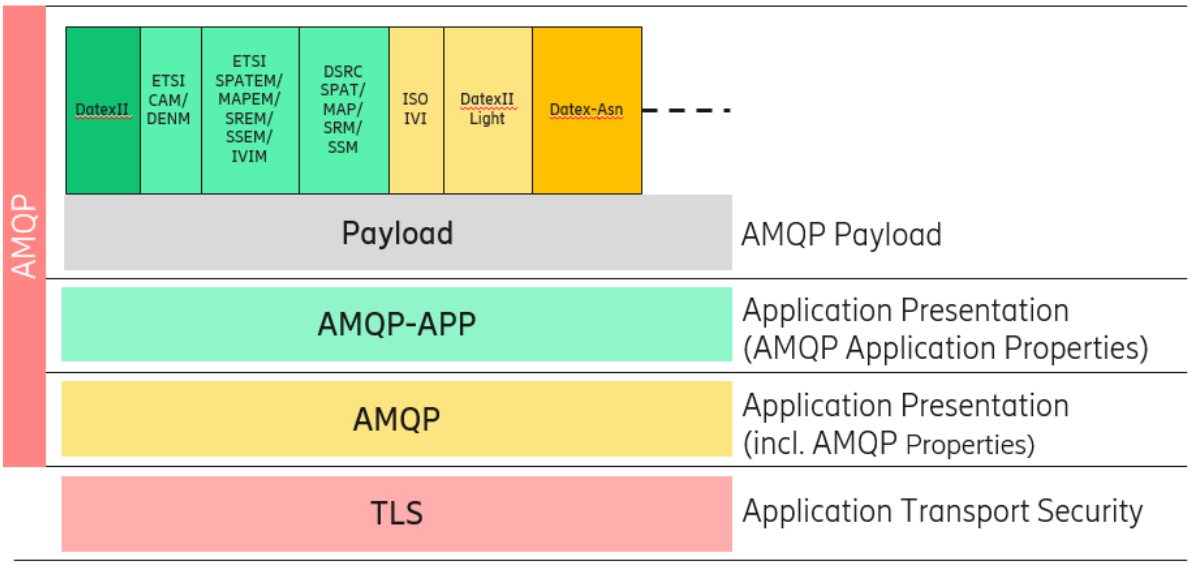


*Figure 9: Simplified protocol stack view, lower layers, e.g. TCP and IP excluded (examples of payloads that could be exchanged)*

## AMQP Basic Interface details

### Username and password

Username and password are required for connecting to the Interchange entity.

### Queues

Queues for receiving messages from the interchange

A default queue is setup for receiving messages for consumers. (Default is 'all' that is published, this mode has been selected to provide all information and let the consumer decide what should be used, i.e. avoid potential issues caused by that information was not delivered, this can be restricted by using filters as outlined below)

Any queue that is associated with a user can have a custom filter on it. These filters can use any combination of the application properties fields defined in this document, set up as a boolean expression. E.g. based on standard AMQP Filter Expressions Version 1.0

An example filter expression could be: "where1"="no" AND NOT who="Norwegian Public Roads Administration". This filter will filter out all messages that happened in Norway (no) except the ones that were sent by Vegvesen (Norwegian Public Roads Administration). So Vegvesen will receive all messages related to Norway except the one they sent to the Interchange them self.

### Queue for sending messages to the interchange

The default queue for sending messages to the interchange is called "onramp".
(Indicated as routing key when publishing information)

| | |
|---|---|
| **Default queue for sending messages to the interchange:** | **Onramp** |



Co-financed by the European Union

### Sending messages to the Interchange

### Message format

The AMQP messages can be split in to three parts:

The header. This includes time to live (of the AMQP message).

Application-specific properties. These are the header fields set by the client and used by the interchange to route the message to the correct consumer queues. Fields are mandatory when sending to the interchange unless specified to be optional.

Body. The message payload, e.g. ETSI DENM, DATEX II, etc.

### Header

The only field in the AMQP message header that is required to be set by the client is the userId field. This field must be identical to the username that the client is using to connect to the Interchange.

| | |
|---|---|
| **userId** | Must be identical to the username that the client is using to connect to the Interchange. All messages for which it does not match will be rejected. |
| **ttl** | Set to default 24 hours in case it is not set in AMQP header for use cases supported by this version of the specification. |

### Application-specific properties

This is a list of the specified application-specific properties defined for the Interchange:

| Property name | Description | Type |
|---|---|---|
| **who** | This is the identifier for the message distributer.<br>Should be 'Username' of authorized user | String |
| **uuid** | A universally unique identifier to identify message, to be kept and logged to ease analysis | Editors note: specify how to obtain, e.g. use mac address as part of uuid ? |

| | | |
|---|---|---|
| **what** | This identifies the information at a high-level what the payload is carrying.<br>For a C-ITS station using ETSI DENM messages this property should contain:<br>The CauseCode in EventType in SituationContainer should be used for New DENM and Update DENM<br>The Termination in ManagementContainer should be used for Cancellation DENM and Negation DENM<br><br>During migration and for other data sources using DATEX II message, this property should at a minimum contain a list of the types of the DATEX II PayloadPublications of the AMQP payload. message. The elements are separated by a comma. (“,”). The available PayloadPublication types will depend on the version of the DATEX II. In this version of the specification only SituationPublication payloads are supported. | String<br><br>Enumerated names are used.<br><br>Strings used for ETSI DENM CauseCode should be according to ETSI EN 302 637-3 ‘CauseCodeType’ in table 9<br><br>Values for Termination should be according to ETSI EN 302 637-3 Annex A (ASN.1), that is:<br>isCancellation<br>isNegation |
| **how** | The type of data contained in the body of this message.<br>This property is defined as <payload>;<version> | String |
| **lat** | The latitude of the ‘event’. This field is used by the Interchange/receiver for doing filtering based on the geographical location of the incident. This value should be as precise as possible, but it is not required to exactly match the actual location, since incidents can be relevant for a larger area.<br>For a C-ITS station using ETSI DENM messages, the value can be obtained from Reference Position.<br>During migration and for other data sources using DATEX II payloads, the value can be obtained from the PointCoordinates element defining the coordinatesForDisplay for elements of the DATEX II PayloadPublication. For SituationPublications this information is available at the SituationRecord level. | Float<br>Decimal degrees<br>According to ETRS89 (WGS 84 can also be used since these standards are similar with a little difference in accuracy which is not crucial) |
| **lon** | The latitude of the ‘event’. This field is used by the Interchange/receiver for | Float<br>Decimal degrees |

| | | |
|---|---|---|
| | doing filtering based on the geographical location of the incident. This value should be as precise as possible, but it is not required to exactly match the actual location, since incidents can be relevant for a larger area.<br>For a C-ITS station using ETSI DENM messages, the value can be obtained from Reference Position.<br>During migration and for other data sources using DATEX II payloads, the value can be obtained from the PointCoordinates element defining the coordinatesForDisplay for elements of the DATEX II PayloadPublication. For SituationPublications this information is available at the SituationRecord level. | According to ETRS89 (WGS 84 can also be used since these standards are similar with a little difference in accuracy which is not crucial) |
| **when** | Timestamp of the message. | According to ISO 8601 |
| **where** | The code for the country that the incident occurred in. | EN ISO 3166-1 two-character country code |
| **Content-type** | Identifying mime-type.<br><br>application/xml is used for xml payload<br><br>application/octet-stream is used for binary [ASN.1] payload<br><br>application/base64 is used for base64 encoded payload [could be ASN.1 data encoded as base64]<br><br>any | String |

**Body**

The body of the message contains the actual message, the interchange function is transparent to any payload. (e.g. ETSI-DENM format, DATEX II format or any future developments e.g. for day 2 and day 3 applications).

When sending ETSI-DENM message in ASN.1, the body of the message should either be binary or base64 encoded payload.
Editors note: need to agree on coding for ETSI ?

It is the responsibility of the application to distribute new messages if situation change. This should be done according to rules of standards, e.g. for ETSI, DATEX etc.

**AMQP example**

Figure 10 shows the principles for information sharing. If no Interchange entity present to perform the message distribution to multiple consumers, a directly connected endpoint (i.e. data receiver/consumer) would be performing the tasks (or parts of tasks) listed in step 2


*Figure 10 Information publishing principles*

1. A authorized data producer writes a message to the “onramp” queue. Interchange entity (data receiver) reads from the “onramp” queue.

2. Interchange entity (data receiver) applies validation of the message

a. Checks the presence of the header properties, application properties and payload. If any of them are absent, the message is dropped.

b. Checks the “userId” property and the related “who” application property. “userId” is expected to be present and if the “who” doesn’t match, a warning is issued.

c. Deletes any messageAnnotations since certain AMQP clients cannot handle them (Messageannotations specifies non-standard header attributes of the AMQP message)

d. If “to” property received it is set to null.

e. If “ttl” is absent, it is set to 86400000 milliseconds (1 day) and if greater than 691200000 milliseconds (8 days), it is set to 691200000 milliseconds.

f. The “userId” is set to the interchange username. (if Interchange entity used for message distribution)

g. If “lat”, “lon” and “what” application properties are missing, the message is dropped.

h. If “what” does not have a value [implying there is no payload], the message is dropped.

Note: step i to j is implementation specific and relates to if AMQP functionality is used to redistribute information and that Geo-lookup is supported (E.g.Geo-lookup by a query to a Geographic Information System (GIS) server or by some other means). For a direct connection between two actors to exchange information, Geo-lookup is not really needed.
Editors note: might be changed when other location methods introduced.

i. After all the checks are done, a geo-lookup is performed to obtain country for lat/lon.

j. A copy of the message is created per country returned by geo-lookup and further copies are created per “what” value and per country. The country information is added to “where” application property.

k. The Interchange entity (data receiver) forwards messages to the attached queues based on the filter/match criteria.

3. A data consumer reads the message from a dedicated queue authorized for that particular data consumer.

# 14 Appendix B TLS profile

TLS 1.3 as specified in RFC 8446 shall be supported. TLS 1.3 provides significantly improved security, privacy, and reduced latency when compared to earlier versions of TLS. Earlier versions of TLS shall not be supported.

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

The list of trusted root certificate authorities (CA) shall be limited to the smallest possible subset of CAs and sub-Cas possible. It is recommended to send the whole certificate chain in the TLS handshake.

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

Note: Later releases and verified revisions of TLS shall be supported.

## TLS Certificates

The certificates used for authentication are standard X.509 TLS certificates [RFC 5280], these certificates have a much simpler structure than the ETSI 1609.2 certificates 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. The sub CA may belong to any of the trusted root CAs and may be a national CA or a commercial CA. The TLS certificates used shall be Organization Validated (OV) certificates where both the domain and the organisation are validated.

TLS certificates shall be version 3 certificate according to [RFC 5280]. The public key algorithm shall be id-ecPublicKey with secp256r1 or secp384r1. The security level of the signature algorithm shall be at least as strong as the public keys in the certificate.

# 15 Appendix C [Informative] Evolved network architecture for sharing information between countries/regions

This annex contains information about how to evolve the solution and use the flexible architecture with Interchange entities to meet rising demands.

In this scenario countries/regions are interconnected to share information for clients moving around in Europe. E.g. service providers have clients located in multiple countries/regions. This country/regional interconnection is needed to avoid that a service provider need to create and maintain connections to many information sources/consumers e.g. to a large number of RTAs/ROs, and that the RTAs/ROs do not need to interact with a large number of service providers. To facilitate this an Interface/protocol to federate information between countries/regions are introduced, this interface/protocol is named **II (Improved Interface)**. The network scenario is exemplified below.

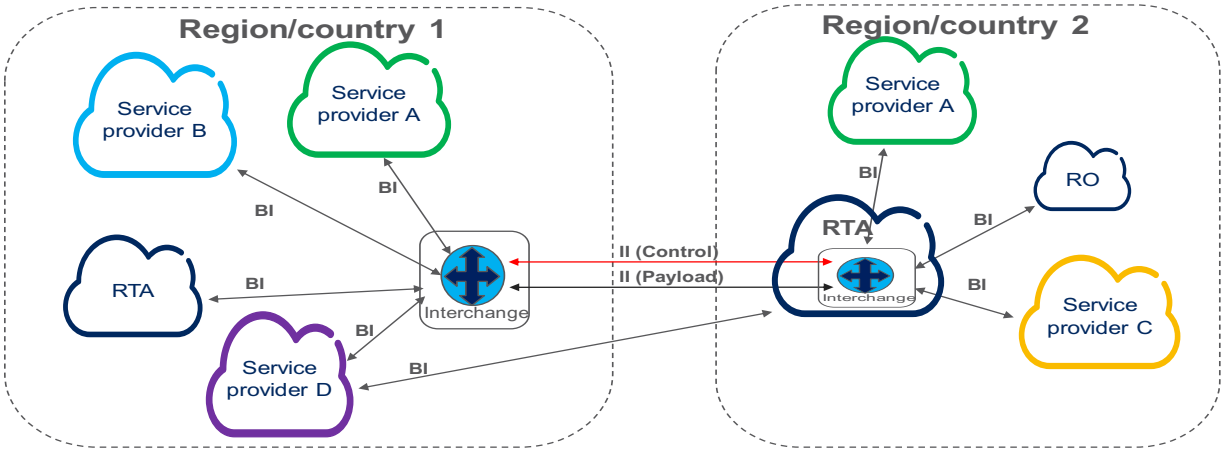


*Figure 11 Evolved architecture for country/region information sharing*

In Figure 11, a simplified illustration of the evolved network architecture scenario is illustrated with the introduction of the II between countries/regions. Compared to Figure 5, country/region 2 has introduced interchange functionality to reduce the number of direct connections between actors and to support sharing of information between countries/regions.
To exemplify, with the use of II, service provider B connected in country/region 1 can get information for country/region 2 without needing a direct connection to information sources in country/region 2. Same for service provider C, which can get information related to country/region 1 and supply that information to its clients located in country/region 1.

### 15.1.1 II protocol/profiles

- **II (Improved – Interface)**: Is the interface between Interchange entities, this interface is also known as federation interface, it has a federation data payload part and a federation control part.
  On this interface following protocols and profiles shall be used:

  **Federation data:**
  - Internet Protocol (IPv4/IPv6) and Transmission Control Protocol (TCP)
    - Supported by basically all operating systems
  - Transport Layer Security (TLS 1.3) according to RFC 8446 shall be used for the operational phase, for pilot phase deployments, TLS 1.2 can be used.
    - Profiling for TLS described in Appendix C
  - Advanced Message Queuing Protocol (AMQP) according to OASIS specification for version 1.0
    Profiling and details for AMQP on the II interface is described in Appendix TBD.
  - Federation data payload
    - Profiling and details for messages on II is described in 'TF2 docs, Editors note: add reference


Co-financed by the European Union

**Federation Control:**

- Internet Protocol (IPv4/IPv6) and Transmission Control Protocol (TCP)
  - Supported by basically all operating systems
- Transport Layer Security (TLS 1.3) according to RFC 8446
  - Profiling for TLS described in Appendix C
- Federation control transport
  - Advanced Message Queuing Protocol (AMQP) according to OASIS specification for version 1.0
    - Profiling and details for AMQP on II is described in Appendix B. Editors note: fix
- Federation Control Payload
  - JSON encoded
    Profiling and details for JSON is described in Appendix Editors note: fix

### 15.1.2 II procedures overview

On the control plane of the II the Interchange entities exchange information about supported capabilities (e.g. what protocol formats are supported), country (e.g. what RTAs that it services), what information that are federated (I.e. shared between the interchange entities), e.g. if only ETSI DENM federated, if traffic information with a certain severity is federated. Based on exchanged control information, an Interchange entity will thus, based on subscription request received from OEM/RTA/Service provider, send a request to the Interchange entity handling the certain country on the II user plane. Then when information is received in the Interchange (from the other Interchange handling the country in question), the receiving Interchange will forward information to the entity that initially started a subscription. A Service provider (or other actor) can be instructed to establish a connection to another Interchange instance, e.g. refer to Figure 11 above, 'Service provider B' can be instructed to establish a connection to Interchange in region/country 2 and subscribe to information directly from that Interchange and subsequently also provide information directly to the interchange in region/country 2.

### 15.1.3 II message flows: Establishing communication between interchange entities

Below is exemplified how Interchange entities interact when a new interchange actor is introduced in the eco system.

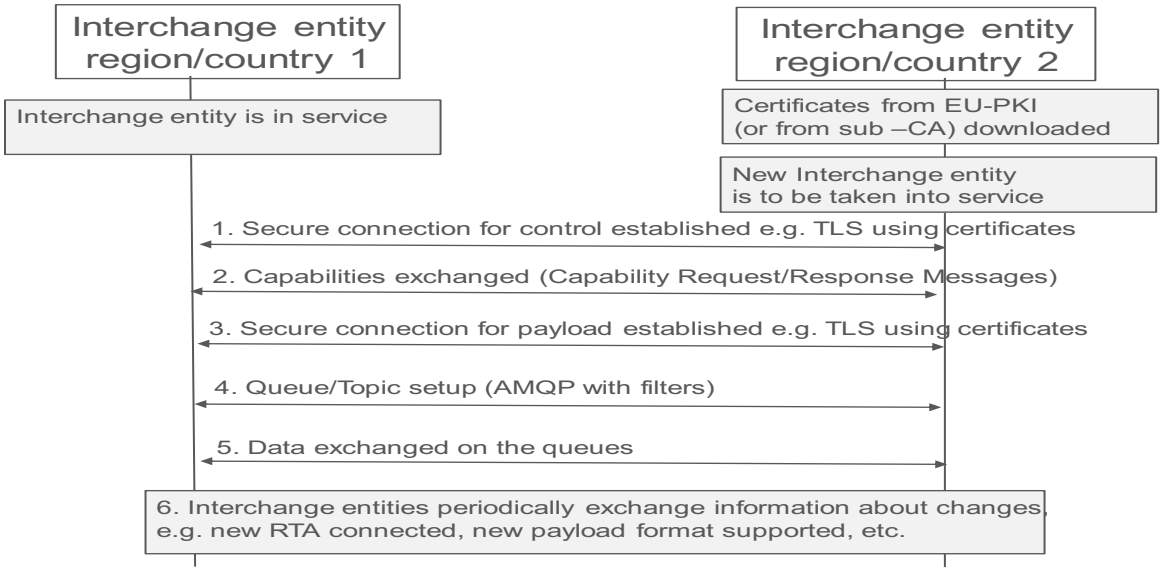


*Figure 12 Interchange entities interaction*

Certificates used for Interchange entity <-> Interchange entity authentication and protection have long validity time as per standard use of TLS, i.e. anonymous certificates are not used. This is further elaborated in chapter 5 about security.

1. Based on pre-configuration, interchange entity will establish TLS session to neighbor interchange entities. TLS with mutual authentication will then be used between the Interchange entities for the control session.
2. The new Interchange entities will send a Capabilities Request Message containing supported countries, supported message types and related versions available for federation from the interchange. The neighboring entities will answer with a Capabilities Response Message containing the supported countries, supported message types and related versions available for federation from the neighbors.
3. A TLS session is established for the payload between the Interchange entities
4. The Interchange entity based on configuration or internal intelligence can setup egress and ingress queues/topic for federated data.
5. The interchange entities can exchange ITS information according to queues/topics.

6. The Interchange informs each other when new actors are connected, e.g. that an RTA is joining the eco system and can provide information, this simplifies for a service provider (consumer) since it does not need to be informed about a new consumer nor need to establish a relation and configure its systems where to obtain information. I.e. the consumers just subscribe to information.

### 15.1.4 Evolved architecture overview

Figure 13 shows a simplified example where the different implementation models have been complemented with the interfaces to us in the backend communication. As shown in Figure 8 below, the II needs to be supported for interoperability between interchange entities. It is also


Co-financed by the European Union

recommended that the BI is used to allow a uniform implementation for backend actors, i.e. avoid that a service provider with operations in several countries need to implement several different versions depending on implementation model chosen in the countries.

As shown in Figure 13, depending on implementation model, the interchange functionality could be combined or co-located with other functionality, e.g. with a Road traffic authority that also handles communication with vehicles, RSUs and/or other actors, in such scenario the Road traffic authority would need to support both the interface to its (locally) connected vehicles, the BI to locally connected actors and the II to interact with other countries/regions.

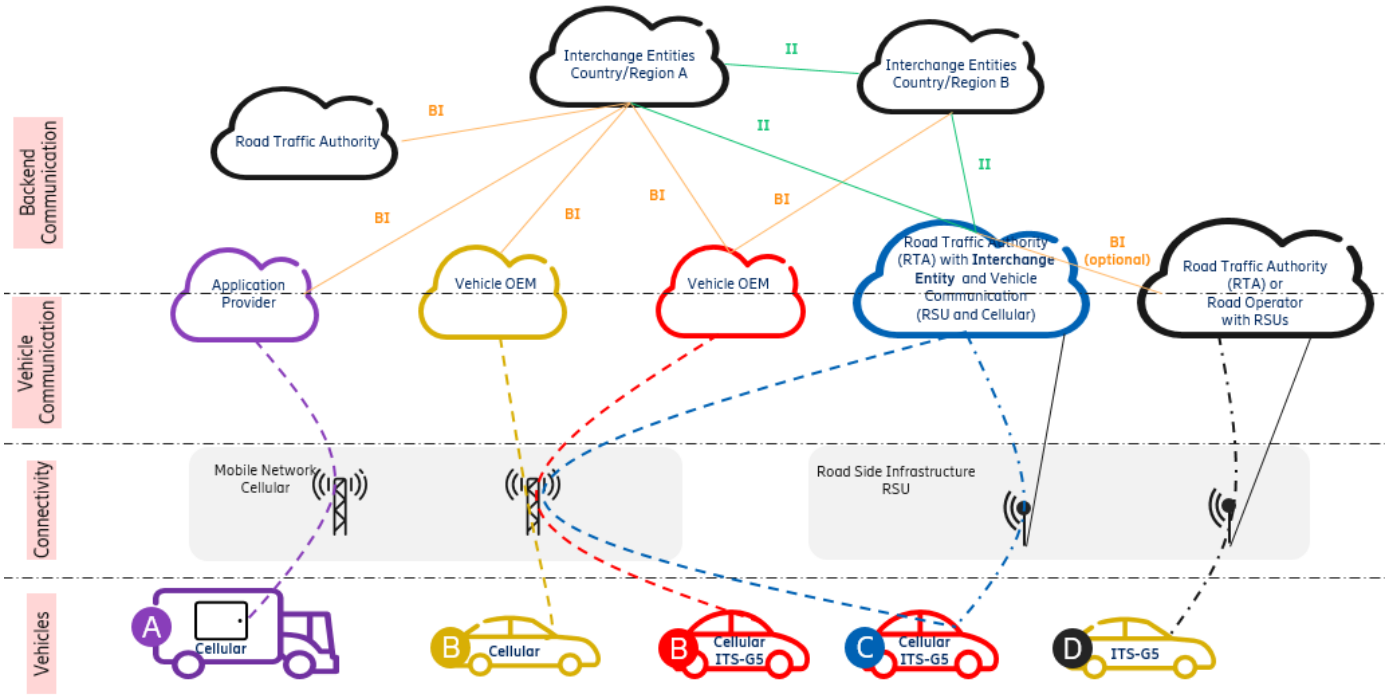


*Figure 13 Backend protocols and implementation models*



Co-financed by the European Union

# 16 Appendix D [Informative] Mapping recommendations RWW and HLN

When an actor is using DATEX for communication in internal systems, there is a need to create an ETSI message according to standards when sharing C-ITS information with other actors on the C-ITS backend, this section outlines recommendations for this translation/creation if such need arise.

## 16.1 DATEX II Standard Message Profiles

The following defines the rules for DATEX II standard representation of ITS messages in backend communication. The specific rules for representation of ITS messages for Road Works Warning and Hazardous Location Notifications are defined in a separate subsection.

The general rules for DATEX II standard representation of ITS messages are as follows.

- Messages shall be represented according to the DATEX II standard data model Level A of the selected version. Possible extensions shall be Level B extensions of that version. Level C extensions are not allowed.
- Messages should be represented according to the latest versions of the DATEX II standard data model. At the time of writing the following versions are allowed: DATEX II version 2.3 and DATEX II version 3.0.

It should be possible to check that message representations are compliant with the selected version of the DATEX II standard data model by validating the representations against standard schemas for Level A of that model.

At the time of writing, the available standard schema for DATEX II is in the form of an XML Schema.

### 16.1.1 Profiles for Road Works Warning and Hazardous Location Notifications

The rules for DATEX II message representation for Road Works Warning and Hazardous Location Notifications are as follows.

- Messages should be represented as DATEX II records of type SituationRecord of SituationPublication publications. This representation applies to DATEX II version 2.3 as well as DATEX II version 3.0.
- Messages should be compliant with the message representation defined in [SRTI]. (Section 16.3 below provides a summary of the DATEX II message representation in [SRTI].)

## 16.2 Mapping between Standard Message Profiles

The following identifies rules for mapping/conversion between different standard message representations (DATEX II and ETSI standard representations). The rules should serve as a basis for converting between standard message representations such that information content is preserved.

The rules comply with the mapping rules defined for DATEX II and DENM in [SRTI].

## 16.3 DATEX II Standard Representation for ITS Messages

The following table summarizes DATEX II standard representation for ITS messages of the use cases defined for Road Works Warning (RWW) and Hazardous Location Notifications (HLN). The table also provides representation for the use case for Road Condition Warning. The messages are represented as records of type SituationRecord in SituationPublication publications.

The representation is compliant with the definitions for safety related messages in [SRTI].

| Service | Use Cases | DATEX II SituationRecords |
|---|---|---|
| Road Works Warning (RWW) | Road Closure | ConstructionWorks |
| | | MaintenanceWorks (RoadMarkingWork, maintenanceWork) |
| | | With Impact:trafficConstrictionType (roadblocked) |
| | Lane Closure | ConstructionWorks |
| | | MaintenanceWorks (RoadMarkingWork, maintenanceWork) |
| | | With Impact:trafficConstriction-Type (roadblocked) |
| | Road Works - Mobile | ConstructionWorks |
| | | MaintenanceWorks (RoadMarkingWork, maintenanceWork) |
| | | VehicleObstruction (slowMovingMaintenanceVehicle) (Not in DATEX II 3.0) |
| | | With Impact:trafficConstrictionType (roadblocked) |
| Hazardous Location Notifications (HLN) | Accident Zone | GeneralObstruction (rescueAndRecoveryWork, UnprotectedAccidentArea) |
| | Traffic Jam Ahead | AbnormalTraffic |
| | Weather Condition Warning | PoorEnvironmentConditions (visibilityReduced, smokeHazard, denseFog, patchyFog, heavySnowfall, lowSunGlare, heavyRain, stormForceWinds, strongWinds, crossWinds) |
| | Stationary Vehicle | VehicleObstruction (brokenDownVehicle, vehicleOnWrongCarriageWay) |
| | Temporarily slippery road | WeatherRelatedRoadCondition (slipperyRoad) (In DATEX II 3.0 slipperyRoad belongs to nonWeatherRelatedRoadCondition) |
| | Animal or person on the road | GeneralObstruction (peopleOnTheRoadway, childrenOnRoadway, cyclistsOnRoadway) |
| | | AnimalsPresenceObstruction (animalsOnTheRoad, largeAnimalsOnTheRoad, herdOfAnimalsOnTheRoad) |
| | | DisturbanceActivity (attackOnVehicle) |

| Service | Use Cases | DATEX II SituationRecords |
|---|---|---|
| | Obstacle on the road | GeneralObstruction (objectOnTheRoad, obstructionOnTheRoad, shedload) |
| | | EnvironmentalObstruction (flooding, fallenTrees, avalanches, rockfalls, landslips) |
| | Road Condition Warning | WeatherRelatedRoadCondition (surfaceWater, ice, blackice, snowDrifts, icyPatches) |
| | | NonWeatherRelatedRoadCondition (mudOnRoad, looseChippings, oilOnRoad, petrolOnRoad) |

*Table 1 DATEX II v2.3 Representations of ITS Messages for RWW and HLN, based on [SRTI]*

## 16.4 Mapping between DATEX II and DENM Standard Representations

Editors note: potentially remove this section since Mapping between DATEX and DENM is implicit through the table in section 16.3, as the different use cases are linked to specific DENM causes, as specified by C-ROADS TF3. Also appendix A covers this (to be checked)

The following table lists mappings between DATEX II and DENM standard representations of ITS messages for Road Works Warning (RWW) and Hazardous Location Notifications (HLN).

The mappings are compliant with the mappings defined for safety related messages in [SRTI].

| DATEX II | DENM | | |
|---|---|---|---|
| Type of SituationRecord | Cause Code | Sub Cause Code | Description |
| ConstructionWorks | TBD | TBD | TBD |
| MaintenanceWorks (RoadMarkingWork) | 3 | 2(0) | road marking work |
| MaintenanceWorks (maintenanceWork) | 3 | 4(0) | short-term stationary roadworks |
| With Impact:trafficConstrictionType (roadblocked) | N/A | N/A | N/A |
| VehicleObstruction (vehicleOnWrongCarriageway) | 14 | 0 | wrong way driving |
| VehicleObstruction (slowMovingMaintenanceVehicle) | 3 | 3(0) | slow moving road maintenance |
| VehicleObstruction (brokenDownVehicle) | 94 | 2 | vehicle breakdown |
| GeneralObstruction (UnprotectedAccidentArea) | 2 | 7 | unsecured accident |
| GeneralObstruction (objectOnTheRoad) | 10 | 0 | hazardous location - obstacle on the road |
| GeneralObstruction (shedLoad) | 10 | 1 | shed load |
| GeneralObstruction (obstructionOnTheRoad) EnvironmentalObstruction (avalanches, landslips) | 10 | 4 | large objects |
| GeneralObstruction (peopleOnTheRoadway) | 12 | 0 | human presence on the road |
| GeneralObstruction (childrenOnRoadway) | 12 | 1 | children on roadway |
| GeneralObstruction (cyclistsOnRoadway) | 12 | 2 | cyclists on roadway |
| GeneralObstruction (rescueAndRecoveryWork) | 15 | 0 | rescue and recovery work in progress |
| EnvironmentalObstruction (rockfalls) | 9 | 1 | rockfalls |
| EnvironmentalObstruction (fallenTrees) | 10 | 5 | fallen trees |
| AnimalsPresenceObstruction (animalsOnTheRoad) | 11 | 0 | hazardous location -animal on the road |
| AnimalsPresenceObstruction (herdOfAnimalsOnTheRoad) | 11 | 2 | herd of animals |
| AnimalsPresenceObstruction (largeAnimalsOnTheRoad) | 11 | 4 | large animals |

| DATEX II | DENM | | |
|---|---|---|---|
| Type of SituationRecord | Cause Code | Sub Cause Code | Description |
| PoorEnvironmentConditions (stormForceWinds, strongWinds, crossWinds) | 17 | 1 | strong winds |
| PoorEnvironmentConditions (visibilityReduced) | 18 | 0 | adverse weather condition - visibility |
| PoorEnvironmentConditions (denseFog, patchyFog) | 18 | 1 | visibility reduced due to fog |
| PoorEnvironmentConditions (smokeHazard) | 18 | 2 | visibility reduced due to smoke |
| PoorEnvironmentConditions (heavySnowfall) | 18 | 3 | visibility reduced due to heavy snowfall |
| PoorEnvironmentConditions (lowSunGlare) | 18 | 6 | visibility reduced due to low sun glare |
| PoorEnvironmentConditions (heavyRain) | 19 | 1 | heavy rain |
| PoorEnvironmentConditions (heavySnowfall) | 19 | 2 | heavy snowfall |
| DisturbanceActivity (attackOnVehicle) | 20 | 3 | stone throwing persons |
| WeatherRelatedRoadCondition (surfaceWater, slipperyRoad) | 6 | 0 | adverse weather condition - adhesion |
| WeatherRelatedRoadCondition (ice, icyPatches) | 6 | 5 | ice on road |
| WeatherRelatedRoadCondition (blackice) | 6 | 6 | black ice on road |
| WeatherRelatedRoadCondition (snowDrifts) | 9 | 5 | snowdrifts |
| NonWeatherRelatedRoadCondition (petrolOnRoad) | 6 | 2 | fuel on road |
| NonWeatherRelatedRoadCondition (mudOnRoad) | 6 | 3 | mud on road |
| NonWeatherRelatedRoadCondition (oilOnRoad) | 6 | 7 | oil on road |
| NonWeatherRelatedRoadCondition (looseChippings) | 6 | 8 | loose chippings |

*Table 2 Mapping between DATEX II (V2.3) and DENM message representation for RWW and HLN*