NordicWay 2 Architecture, Draft

NordicWay 2 Activity 2

Deliverable 21:1

Version 1.0

Date 2019-02-22

Co-financed by the European Union
Connecting Europe Facility

Document Information

Authors

NAME	ORGANISATION
Jonas Sundberg (editor)	Sweco
Input documents:	
Datex II Interchange, NordicWay, Function Description	Ericsson
TF4 Architecture, C-Roads Hybrid Solution Description v0.0.3	C-Roads Platform, Working Group 2 Technical Aspects, Taskforce 4 Hybrid

Distribution

DATE	VERSION	DISSEMINATION
2019-01-18	0.6	A2
2019-01-23	0.7	PMB
2019-02-22	1.0	PMB for acceptance

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

Content

1 Introduction

1.1 This report

The NordicWay 2 Grant Agreement include a set of tasks related to Activity 2 Technical Coordination. Relating to system design the most important tasks are:

- Improvement of the core architecture designed under the Action NordicWay 2014-EU-TA-0060-S by bringing in the additional services being piloted under Activities 5, 8 and 9. This work will include the development of detailed definitions of each chosen service, including the definition of data value chains, definition of service levels and quality requirements and the definition and agreement on partnership models within NordicWay2 for future full scale implementation.
- Expansion of the security functionality of the Interchange Network defined under the Action NordicWay 2014-EU-TA-0060-S by including confidential channels and improving the granularity of the geo-lookup functions to accommodate use also for applications with high requirements on geographical precision (e.g. intersection level). The security framework will fit with appropriate parts of the security framework developed by the C-ITS Platform working group and will contribute to the security development within C-Roads.

This work is to be reported in two deliverables which after adoption by the Project management Board also constitute formal milestones of NordicWay 2:

- M7: NordicWay architecture and service definitions design, approved by the Project Management Board.
- M8: Final report on the NordicWay architecture and services, approved by the Project Management Board.

The deliverable for milestone 7 is for practical reasons divided into two parts; This document (D21:1) including the Architecture and Security, and a separate document developed for the Service Definitions (D21:2).

The intention of this deliverable, and the work so far in NordicWay 2, is to function as a guide for the continued work by reporting on the current status and positions taken. Considerable changes are to be expected for the Final Report, due in 2020, hence this document is not intended to provide detailed instructions on systems design or to report on final results from NordicWay 2.

1.2 Relation to C-Roads

The results reported from NordicWay 2 concerning Service Definition and Architecture (including this deliverable) are also developed as reports for C-Roads. As the documents are subject to continuous updates and are work in progress following not exactly the same time schedule, eventual differences between the two documents shall be understood as an effect of this rather than being intentional. The work objective is to have fully synchronized results from the projects.

2 NordicWay Architecture

2.1 Principles established in NordicWay

The basic principles of the architecture applied in NordicWay 2 was developed and implemented in the preceding project NordicWay[1] and reported in *Architecture, Services and Interoperability* (v1.02, March 2017).

The main purpose for NordicWay was to establish a solution that allowed for cross-border continuity and interoperability of the C-ITS use cases implemented. A mechanism was needed for exchanging

[1] 2014-EU-TA-0060-S 2015-2017

information between different service providers, and between service providers and the Traffic Data Providers e.g. in case the driver is driving abroad. The mechanism agreed between the partners of the project was the use of an intermediary NordicWay server, which is a central hub that facilitates the interchange of messages of interest between several countries, OEM clouds and TMCs. This server is referred to as the Interchange.

The server receives messages on DatexII format[2] and routes messages based on location information (e.g. lat/lon) contained in the message to subscribable channels per country. We envision every OEM subscribing only to relevant information as cars travel across borders. The idea is that every OEM cloud does not have to subscribe to all types of messages from all countries.

The mechanism supporting routing messages to separate channels per country or based on other criteria is AMQP. AMQP is a platform independent message queuing protocol and has bindings for many commonly used languages.

2.2 Development in NordicWay 2

NordicWay 2 builds on the results from NordicWay. From an architectural perspective, two important developments will be made: NordicWay 2 will expand the architecture to include aspects of federation of multiple Interchange Nodes, thus allowing for building up a (European) network of message interchanges allowing for all possible exchange of information between providers of and subscribers to information, accounting for all possible business relations.

NordicWay 2 will also further develop the number of and content of the use cases demonstrated in the project. This is reported in the *Service definition* section of this deliverable (D21:2).

[2] The server is however agnostic to the message format

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

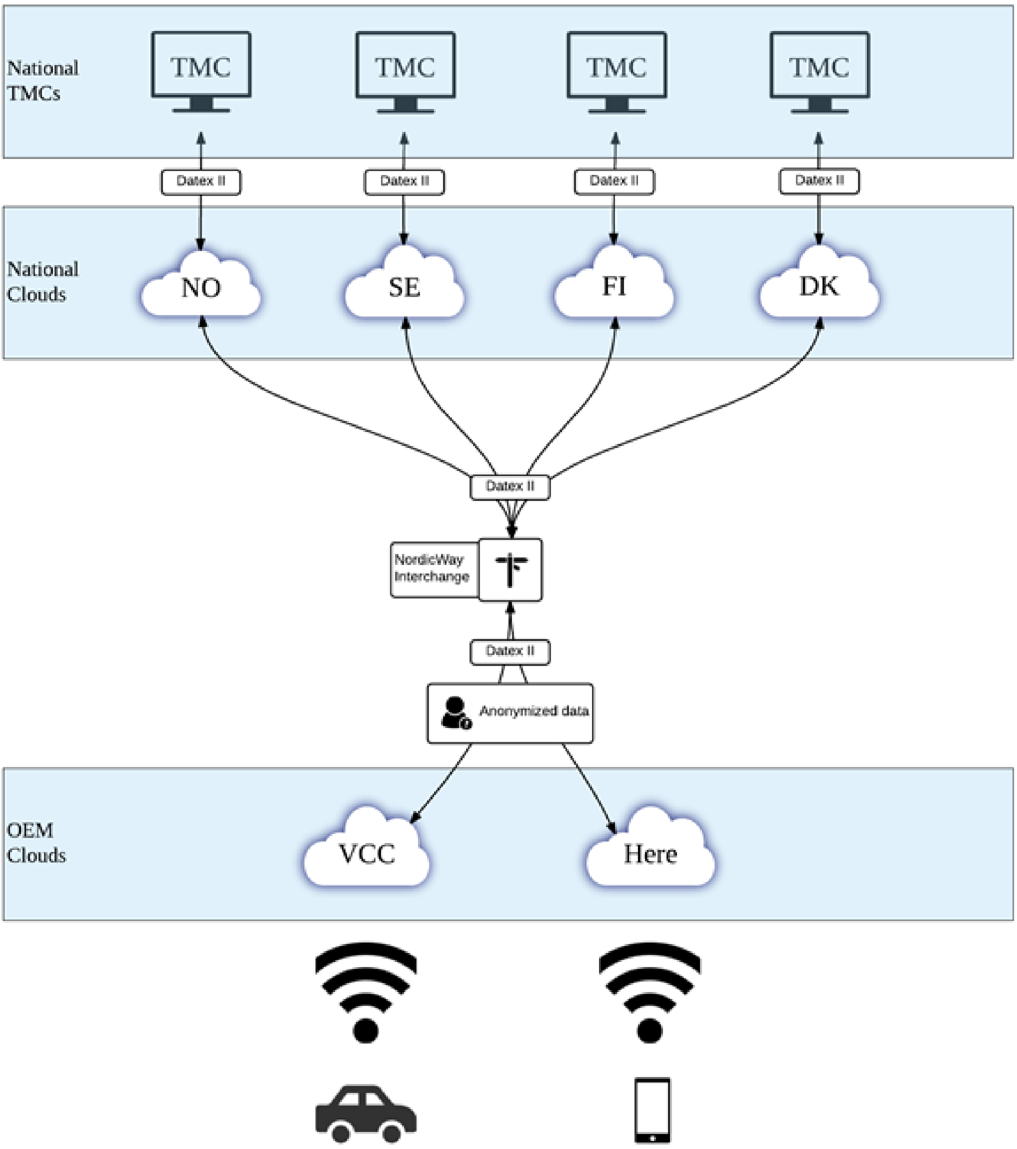

Figure 1 NordicWay Interchange node principle, NordicWay 1

2.3 Basic NW architecture for information sharing with Service providers[3]

Even though all actors could be considered to be service providers, to ease understanding in the following descriptions/examples a distinction have 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).

[3] See also Annex A

Co-financed by the European Union
Connecting Europe Facility

In this scenario 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. 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 (Backend - Interface)** is introduced**.** The network scenario is exemplified below.

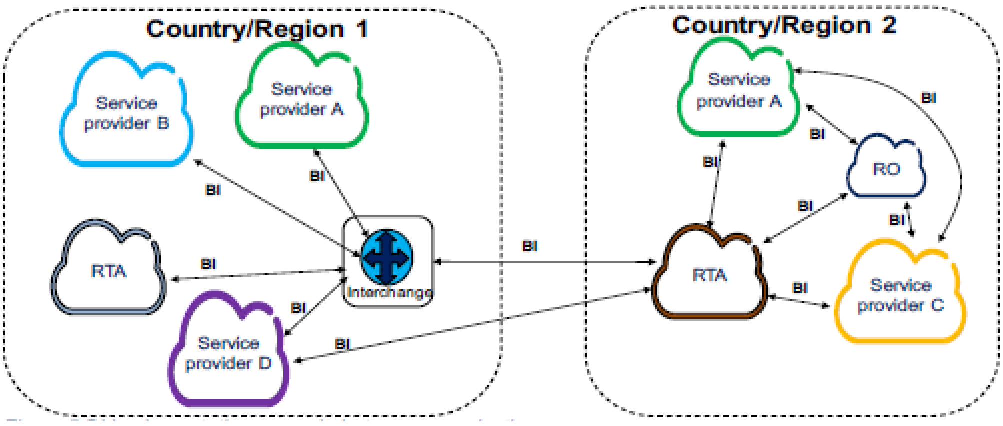

Figure 2 Basic network architecture

In Figure 2, 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 2 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.

2.3.1 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.
- Advanced Message Queuing Protocol (AMQP) according to OASIS specification for version 1.0
- Payload
  - AMQP is payload agnostic, i.e. different payload formats can be carried

2.3.2 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.

2.3.3 BI message flows: Establishment of secure sessions and application initialization

Below in Figure 3 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).

Co-financed by the European Union
Connecting Europe Facility

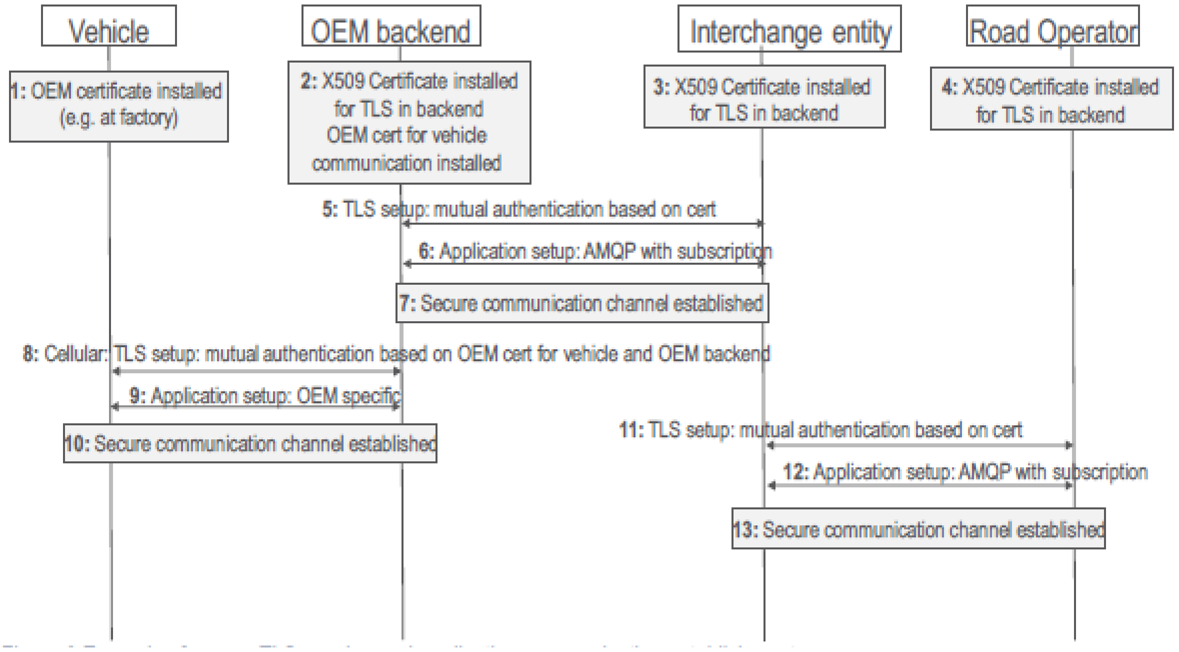
Vehicle
OEM backend
Interchange entity
Road Operator
1: OEM certificate installed (e.g. at factory)
2: X509 Certificate installed for TLS in backend OEM cert for vehicle communication installed
3: X509 Certificate installed for TLS in backend
4: X509 Certificate installed for TLS in backend
5: TLS setup: mutual authentication based on cert
6: Application setup: AMQP with subscription
7: Secure communication channel established
8: Cellular: TLS setup: mutual authentication based on OEM cert for vehicle and OEM backend
9: Application setup: OEM specific
10: Secure communication channel established
11: TLS setup: mutual authentication based on cert
12: Application setup: AMQP with subscription
13: Secure communication channel established

Figure 3 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 4.

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 2 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.

2.4 Evolved Network Architecture for sharing information between countries/regions[4]

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 CITS and will be addressed at a later stage.

3 Security

3.1 Backend trust domain

Figure 4 below show the boundaries for the C-ITS backend trust domain.

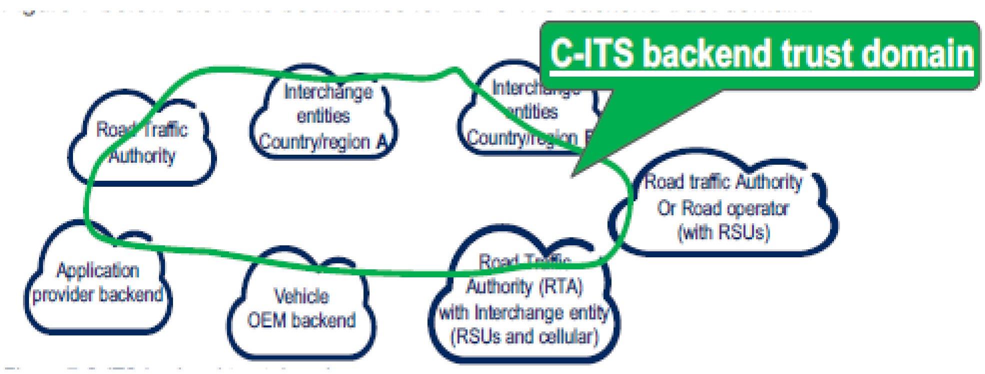
C-ITS backend trust domain
Road Traffic Authority
Interchange entities Country/region A
Interchange entities Country/region B
Road traffic Authority Or Road operator (with RSUs)
Application provider backend
Vehicle OEM backend
Road Traffic Authority (RTA) with Interchange entity (RSUs and cellular)

Figure 4 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.

[4] See also Annex B

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.

3.2 Public Key Infrastructure (PKI)

Below in Figure 5 shows an example outline of the PKI setup.

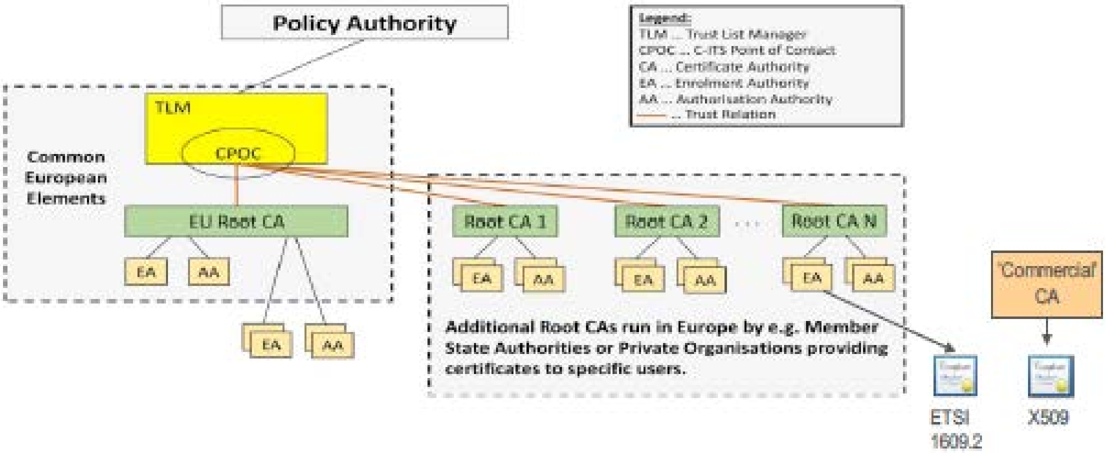
Policy Authority
Legend:
TLM ... Trust List Manager
CPOC ... C-ITS Point of Contact
CA ... Certificate Authority
EA ... Enrolment Authority
AA ... Autharisation Authority
... Trust Relation
TLM
CPOC
Common European Elements
EU Root CA
EA
AA
EA
AA
Root CA 1
Root CA 2
...
Root CA N
EA
AA
EA
AA
EA
AA
Additional Root CAs run in Europe by e.g. Member State Authorities or Private Organisations providing certificates to specific users.
'Commercial' CA
ETSI 1609.2
X509

Figure 5 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..

3.3 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[5].

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.

3.4 Privacy

A service provider handling user data must comply with 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.

4 Positioning and geographical distribution

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.

[5] Editors note: Regulations unclear, Discussions ongoing in C-Roads TF1 how to handle.

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

5 Annex A: NordicWay Interchange – architecture and functionality

5.1 Architecture

5.1.1 Requirements

The architecture of the Interchange is based on the following important requirements

a. Interoperable exchange and crowd sourcing of digital traffic information related to traffic safety like hazards, road works
b. Decoupling of actors
c. Lightweight, primarily provide message routing between actors
d. Geo based filters
e. Standardized interfaces
f. Transport security
g. Possibility to deploy on a PaaS/IaaS/Native implementation.

Figure A1 illustrates the eco-system of the involved actors.

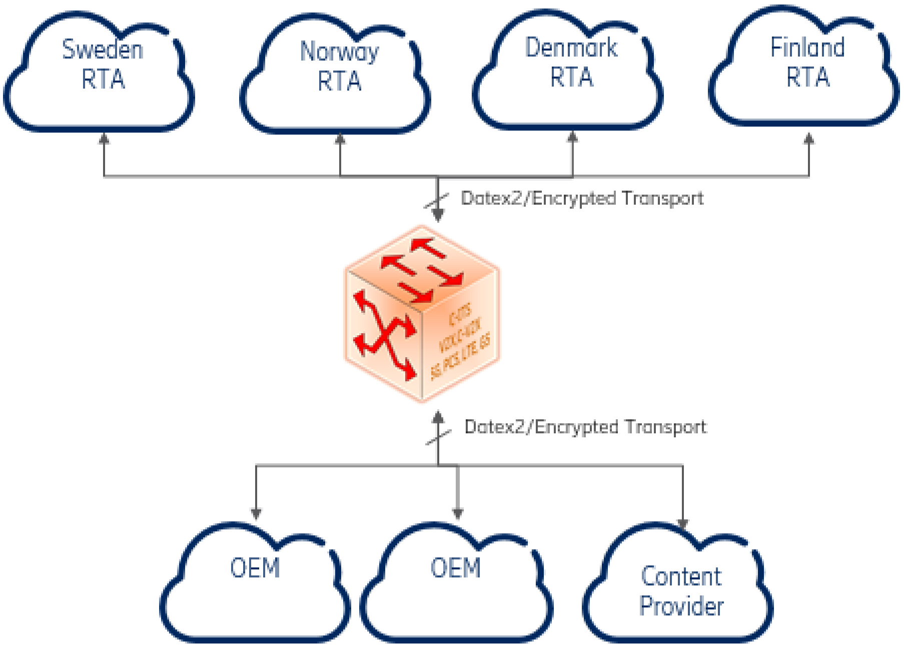

Figure A1: Interchange network overview

5.1.2 Overview

Based on the requirements outlined above, the following components are identified as the basic building blocks for the Interchange.

- AMQP Broker, since AMQP 1.0 is the chosen protocol for the cloud-cloud communication
- Geo Lookup functionality, to convert any co-ordinates, latitude and longitude, to country
- Security, for transport layer security
- User and Queue Management, for handling data producers and data consumers to the interchange.
- Interchange application, needed for handling incoming messages, performing geo-lookup and publishing the valid messages to the consumers

Figure A2 illustrates the Interchange building blocks:

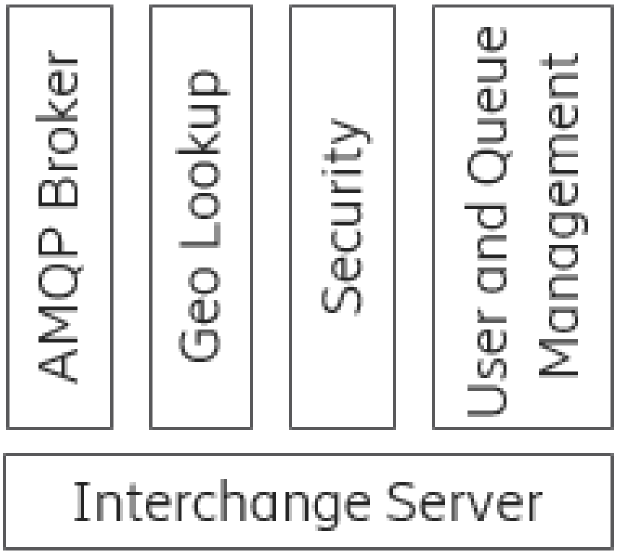

Figure A2: Interchange component overview

The software components providing the building blocks are

- AMQP broker: implemented using Apache QPID server and running in a docker container
- Geo Lookup: implemented using PostGis and running in a docker container
- Security: implemented using TLS, within the current Nordic Way scope, Ericsson provides the certificates to the onboarded partners on the Interchange.
- User and Queue Management: Ericsson provides this as-a-service within the current Nordic Way Scope
- Interchange application: Implementing the Interchange logic and is implemented using Node JS. This application is running in a docker container.
- MySQL: For logging purposes and running in a docker container.

These components will be further detailed in Chapter 5.2.

Figure A3 illustrates the high-level architecture view from software component view.

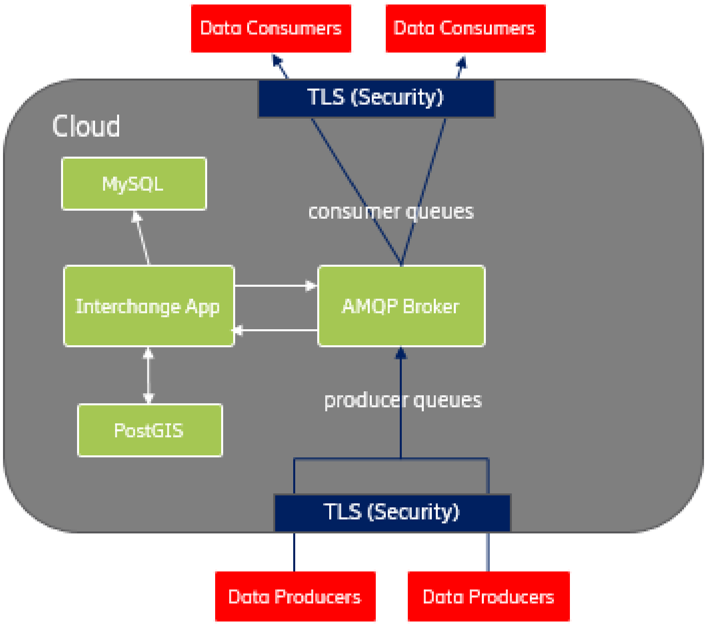

Figure A3: Interchange network and component architecture

5.1.3 Interfaces

The only external interfaces provided by the Interchange are based on AMQP and TLS. The Client Interface specification, Ref 1, document details the interface.

The payload is not modified by the Interchange. Interchange only acts on the AMQP application properties extended for the Nordic Way functionality. Details of this are available in chapter 5.2.5.

Figure A4 illustrates the layered architecture around AMQP and TLS as implemented in the Interchange.

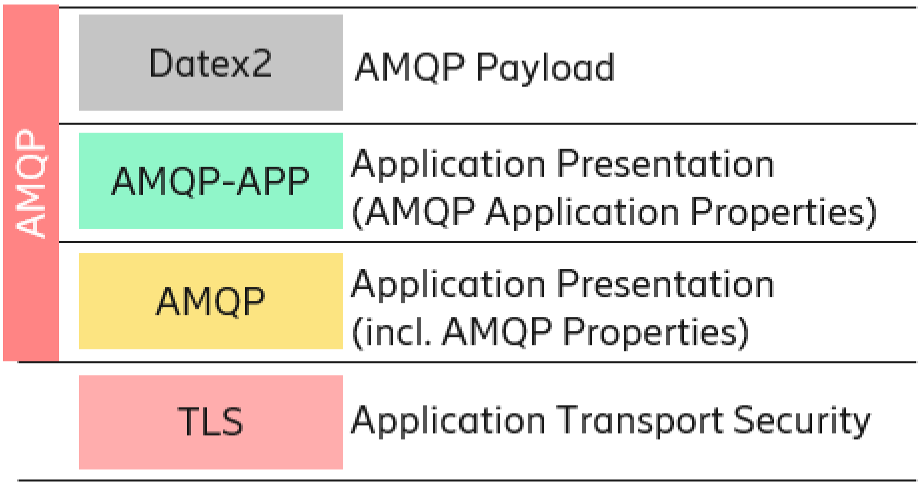

Figure A4: Interchange protocol stack

5.2 Functions & Components

This chapter details the different functions provided by the components as identified in section 5.1.2. Figure A5 illustrates how the components are connected. This figure will be further referred to in the sub-chapters below.

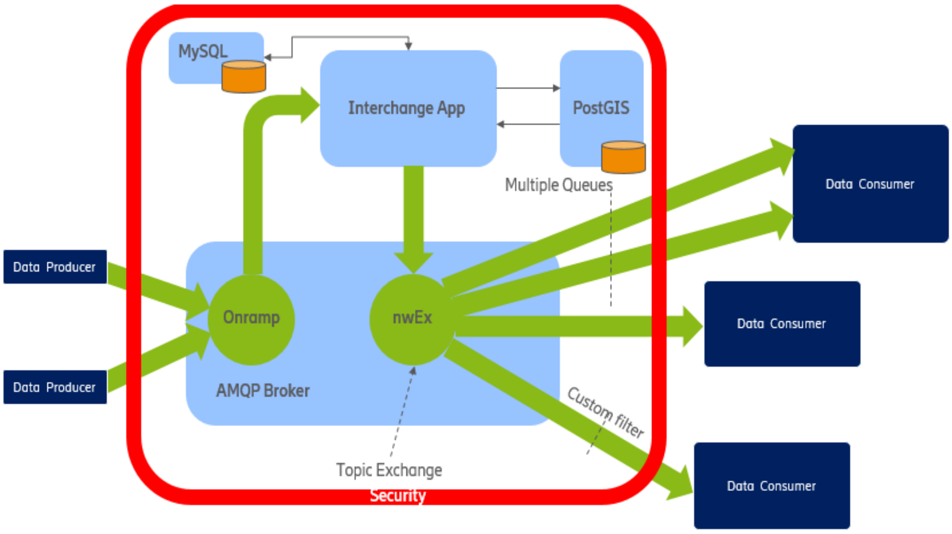

Figure A5: Interchange low-level architecture

5.2.1 AMQP Broker: QPID Server

The QPID Server executes in it’s own docker container. The QPID Server has

- onramp: one write queue for all data producers and the Interchange Application is the only consumer of the data from the queue
- nwEx: a topic exchange, to which the Interchange Application writes.
- Consumer queues: queues connected to the nwEx topic exchange, from which they get the messages matching the queue specific filter criteria.

Refer to chapter 5.2.4, for more details on queue management and how the access control is applied to the consumer queues.

5.2.2 Geo Lookup: PostGIS

The PostGIS database is running in it’s own docker container based on mdillon/postgis/9.6-alpine.

Shape files for countries are uploaded.

5.2.3 Security: TLS Certificates

Within the current setup of Nordic Way, Ericsson issues signed TLS certificates and private keys to the approved partners.

5.2.4 User and Queue Management: As-a-service

Within the current scope of Nordic Way, Ericsson provides User and Queue Management as a service to the partners.

Every Nordic Way partner is provided with separate username and password. Multiple accounts can also be created.

Each data producer will be given access to onramp queue for writing AMQP messages.

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

Each data consumer will be given access to separate queue(s) that filter out the messages from the nwEx topic exchange. This filtering is based on the match criteria provided by the user at the time of the creation of the queue. Only client that are authenticated with the username associated with a queue can read from that queue.

5.2.5 Interchange Application: Node JS application

The Interchange Application is an application developed by Ericsson and runs in it's own docker container.

The Interchange Application performs the following functions

- Read the messages written by the data producers to the onramp queue
- Validation of the AMQP messages
- Perform Geo-lookup of the valid messages
- Create multiple copies of the same AMQP message if the Geo-lookup returns multiple countries and/or the AMQP application property "what".
- Write the messages to the nwEx topic exchange
- Any failures are logged in the MySQL database

The Interchange Application scans the following in the AMQP messages

- userId: must be identical to the username used by the client and this is verified by comparing "who" and the string matching returned for "who" lookup on userId.
- lat,lon,what: the three application properties are checked, if they don't exist the messages are dropped. If the "what" does not have a value, then also the message is dropped.
- where1: the application property is updated based on the Geo-Lookup information.
- ttl: In case, the property "ttl" Is missing, then it is set to 86400000. If it is greater than 691200000, then it is set to 691200000.

5.2.5.1 Message flow

Figure A6 illustrates how a message is handled in the Interchange.

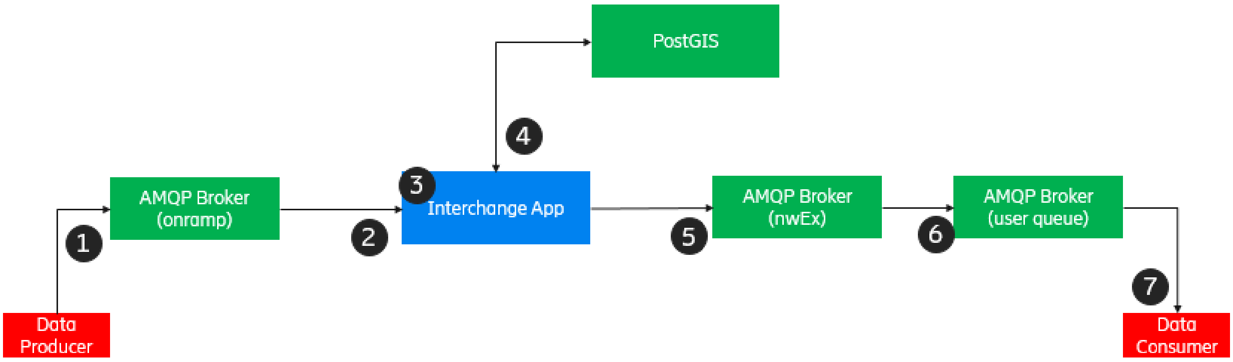

Figure A6: Message flow

1. A data producer writes a message to the "onramp" queue.
2. Interchange App reads from the "onramp" queue.
3. Interchange App applies validation of the message

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

a. Checks the presence of the 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 clients cannot handle them

d. “to” property 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 to the interchange username.

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.

4. After all the checks in (3), a geo-lookup is performed.
5. 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 “where1” application property. Each message is written to the “nwEx” topic exchange.
6. The “nwEx” topic exchange forwards messages to the attached queues based on the filter/match criteria.
7. A data consumer reads the message from a dedicated queue authorized for that particular data consumer.

5.2.6 Logging & Debugging: MySQL

In addition to QPID internal logging and debugging mechanisms, MySQL is used for making a copy of the messages for tracing and debugging purposes.

5.3 Deployment models

The Nordic Way Interchange is provided as-a-Service but can still be deployed in different IaaS/PaaS environments as needed by a customer.

In case of the current scope for Nordic Way, the Interchange is deployed on Openstack on Ubuntu Guest OS as illustrated in Figure A7.

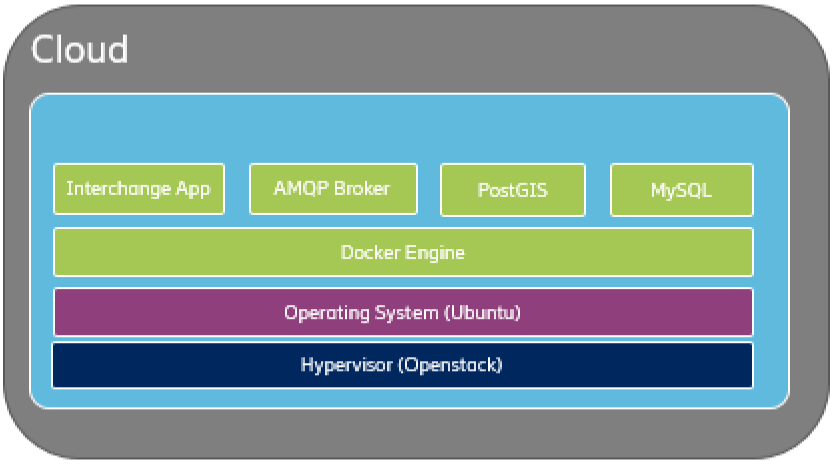

Figure A7: Interchange deployment overview

5.4 Abbreviations

AMQP	Advanced Message Queueing Protocol
IaaS	Infrastructure as a Service
OEM	Original Equipment Manufacturer
OS	Operating System
PaaS	Platform as a Service
RTA	Road Transport Authority or Road Traffic Authority
TLS	Transport Layer Security

5.5 References

Nordic Way Client Specification v0.2

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

6 Annex B [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.

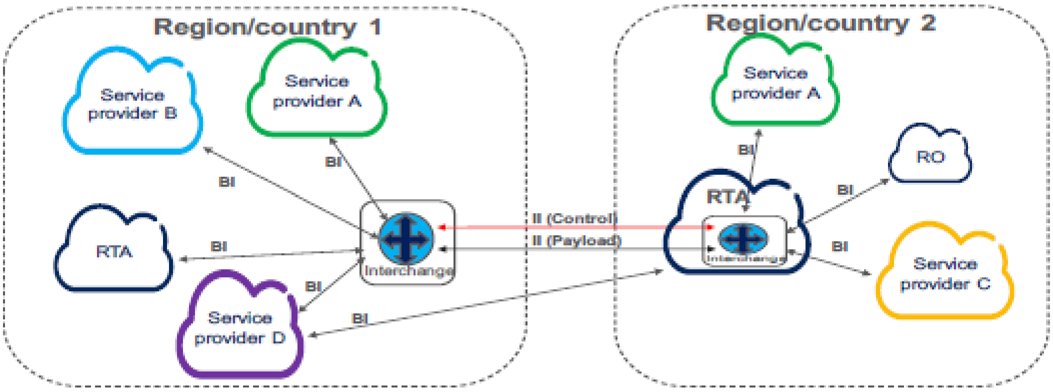

Figure B1 Evolved architecture for country/region information sharing

In Figure B1, a simplified illustration of the evolved network architecture scenario is illustrated with the introduction of the II between countries/regions. Compared to Figure 2, 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.

6.1 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.
- 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 C-Roads TF2 docs,

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
- Federation control transport
  - Advanced Message Queuing Protocol (AMQP) according to OASIS specification for version 1.0
- Federation Control Payload
  - JSON encoded

6.2 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 B1 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.

6.3 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.

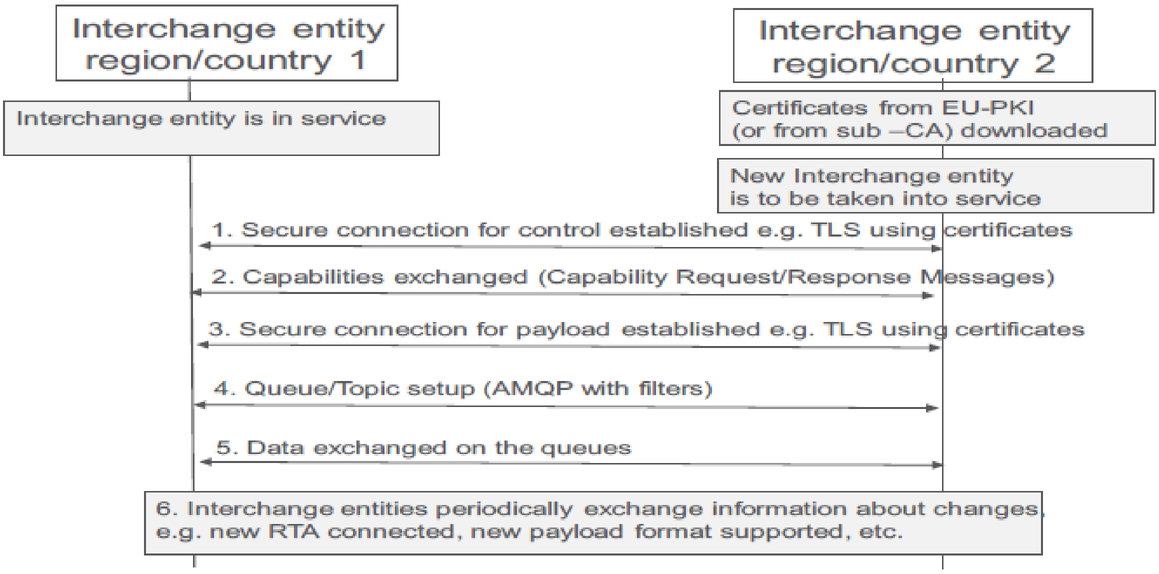
Interchange entity region/country 1
Interchange entity region/country 2
Interchange entity is in service
Certificates from EU-PKI (or from sub –CA) downloaded
New Interchange entity is to be taken into service
1. Secure connection for control established e.g. TLS using certificates
2. Capabilities exchanged (Capability Request/Response Messages)
3. Secure connection for payload established e.g. TLS using certificates
4. Queue/Topic setup (AMQP with filters)
5. Data exchanged on the queues
6. Interchange entities periodically exchange information about changes, e.g. new RTA connected, new payload format supported, etc.

Figure B2 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 3 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.

6.4 Evolved architecture overview

Figure B3 shows a simplified example where the different implementation models have been complemented with the interfaces to us in the backend communication. As shown in the figure below, the II needs to be supported for interoperability between interchange entities. It is also 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 B3, 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.

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained herein.

Co-financed by the European Union
Connecting Europe Facility

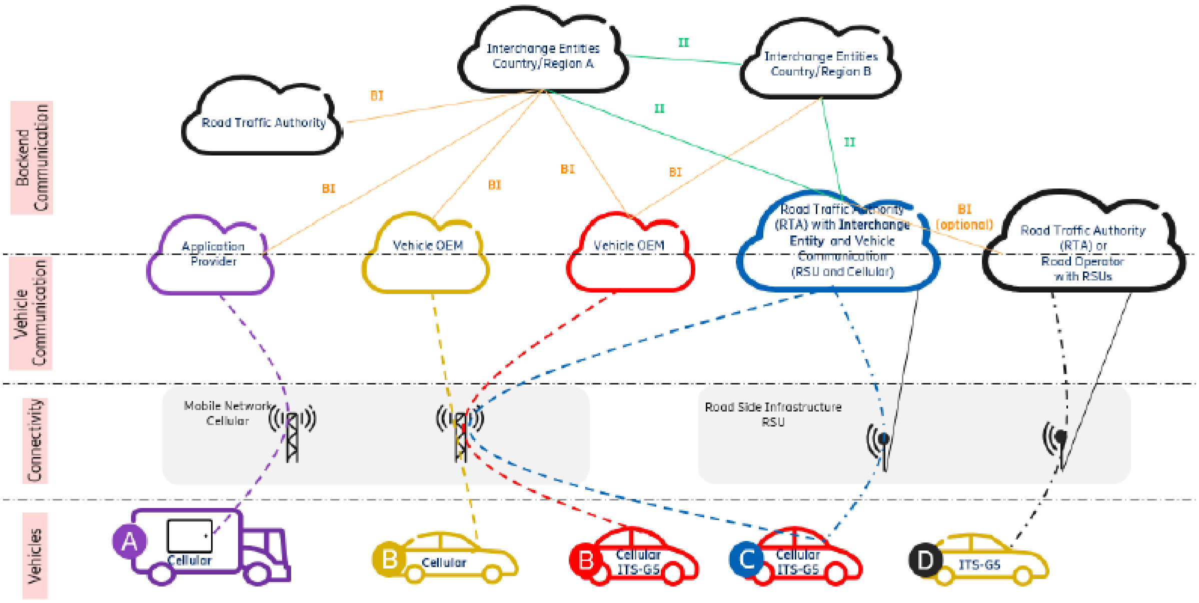
Backend Communication
Vehicle Communication
Connectivity
Vehicles
Interchange Entities Country/Region A
Interchange Entities Country/Region B
II
II
II
Road Traffic Authority
BI
BI
BI
BI
BI
Application Provider
Vehicle OEM
Vehicle OEM
Road Traffic Authority (RTA) with Interchange Entity and Vehicle Communication (RSU and Cellular)
BI (optional)
Road Traffic Authority (RTA) or Road Operator with RSUs
Mobile Network Cellular
Road Side Infrastructure RSU
A
Cellular
B
Cellular
B
Cellular ITS-G5
C
Cellular ITS-G5
D
ITS-G5

Figure B3 Backend protocols and implementation models