DIRIZON

Data-exchange concept for NRAs in the light of connected automated driving

Deliverable 5.1

November, 2020

Project Nr. 867492

Project acronym: DIRIZON

Project title:

Advanced options for authorities in light of automation and Digitalisation horizon 2040

Deliverable Nr 5.1 – Data-exchange concept for NRAs in the light of connected automated driving

Due date of final deliverable: 30.06.2020

Actual submission date: 26.11.2020

Start date of project: 01.09.2018 End date of project: 30.11.2020

Author(s) this deliverable:

Christian Lüpges, Josef Kaltwasser, Jörg Freudenstein, AlbrechtConsult, Germany

Frank Berkers, TNO, The Netherlands

Christian Kleine, Matthias Mann, HERE, Germany

Mark Tucker, ROD-IS, Ireland

Version: Final

Executive summary

The digitalisation of road networks and the rapid developments in automated driving will affect the core activities that (national) road authorities carry out and provide them with new and more efficient ways to achieve their goals for road safety, traffic efficiency, the environment and customer service. In this context, digitalised data plays a key role and enables the connectivity needed to improve efficiencies in managing, maintaining and operating the road network. Equally, digitalisation, along with connectivity, are crucial prerequisites to enable connected and cooperative automated driving. Digitalisation of road assets can provide a number of benefits to road authorities including new (business) opportunities resulting from data sharing, the improvement of enhanced traffic management with Intelligent Transport System (ITS) equipment, improved asset management thus allowing for more reliable performance monitoring of assets and more efficient maintenance processes. Road Operator business practices will need to adapt to exploit these opportunities

To support road authorities in their digital transition and in their interaction with other actors in cooperative automated driving, the Conference of European Directors of Roads (CEDR) commissioned and funded the “advanced options for authorities in light of automation and DIgitalisation hoRIZON 2040”, (DIRIZON) project in the Transnational Research Programme Call 2017 on “Automation”. The DIRIZON project’s goal is to assist the aforementioned road authorities in identifying how these developments will affect their operations and their interaction with others. In this respect, DIRIZON will determine the implications of digitalisation and automated driving on specific core topics and their consequences on data needs and requirements for data-exchange.

The focus of WP5 was on the development of data exchange options for Use Case 3 “Infrastructure Support for Automated Driving” as the most complex use case, which also covers the others to show the technical options, considering the evolvement over the time. Therefore, some research on innovative projects and initiatives related to the topic of data exchange was carried out. In the end recommendations and conclusions for a future strategy were derived.

The investigations started with the thesis that any type of future connected automated driving scenario will generate a need for substantial improvements in data exchange between road authority backend systems, service provider backends and OEM backends (cloud-to-cloud services). Appropriate services would pave the way for providing data services directly into vehicles, mobile devices or aftermarket devices used inside vehicles and, vice versa, providing sensor-data back to the connected backends.

WP5 had also a further look on current data exchange concepts and their characteristics. The focus was on National Access Points, C-ITS, Data Task Force and International Data Spaces.

The latter is a very innovative and industry proven concept an seems to be of high value for NRAs, Service Providers and OEMs. The originator of the IDS concept, the IDS Association is an alliance of multiple organizations with the aim of establishing a distributed platform concept for secure and trusted data sharing maintaining data sovereignty. The concept offers new possibilities to trustful access even sensitive mobility data sources (e.g. fleet data) in order to use them e.g. for traffic condition monitoring, traffic prediction models, future AI applications.

In short, it revolves around so called ‘connectors’ that allow to make even existing data sharing systems interoperable with others, and therefore allow for building forward on local, regional or national deployments, without foreclosing the opportunity of an interconnected and interoperable European data landscape (for mobility).

It is important to notice that on the one hand this distributed approach in principle deviates from the somewhat central system design approach NRAs took in designing systems, e.g. NAPs – and on the other hand how decentralized CEDR and other European governing organisations actually already function.

The results of WP4 has shown that the role of National Access Points (NAP) in the field of automated driving is still not unanimously accepted. But WP5 emphasized, that the European Commission has requested the creation of NAPs as a prerequisite for the standardised handling of mobility data in Europe (see ITS Directive 2010/40/EU).

A further obstacle to the use of the European NAPs for internationally operating companies such as vehicle manufacturers and navigation service providers is the still large number of platforms in Europe. Around 30 NAPs, some of which are implemented in significantly different ways, have to be served in this way in order to be able to offer services internationally. Apart from a few exceptions, they do not offer any possibilities for direct data exchange. Further harmonisation, or rather the networking of the European NAPs with Mobility Data Space concepts, would be welcomed from many sides.

Therefore, 2 options were proposed and assessed how a future distributed data exchange concept could be realised. Both take into account the current heterogeneous system landscape in the individual EU member states. Option 1 envisages a networking of road operators with service providers and OEMs by means of IDS connectors. Option 2 requires a functional extension of the NAPs, which so far only have to provide metadata. Under this option, the NAPs will exchange data and are internationally networked with other NAPs. National road operators will exchange data with their national NAP in charge. However, the international interconnection of the NAPs would allow service providers and OEMs to access the data offered by the whole network through only one access point to a NAP. Both options are shown in Figure 1.

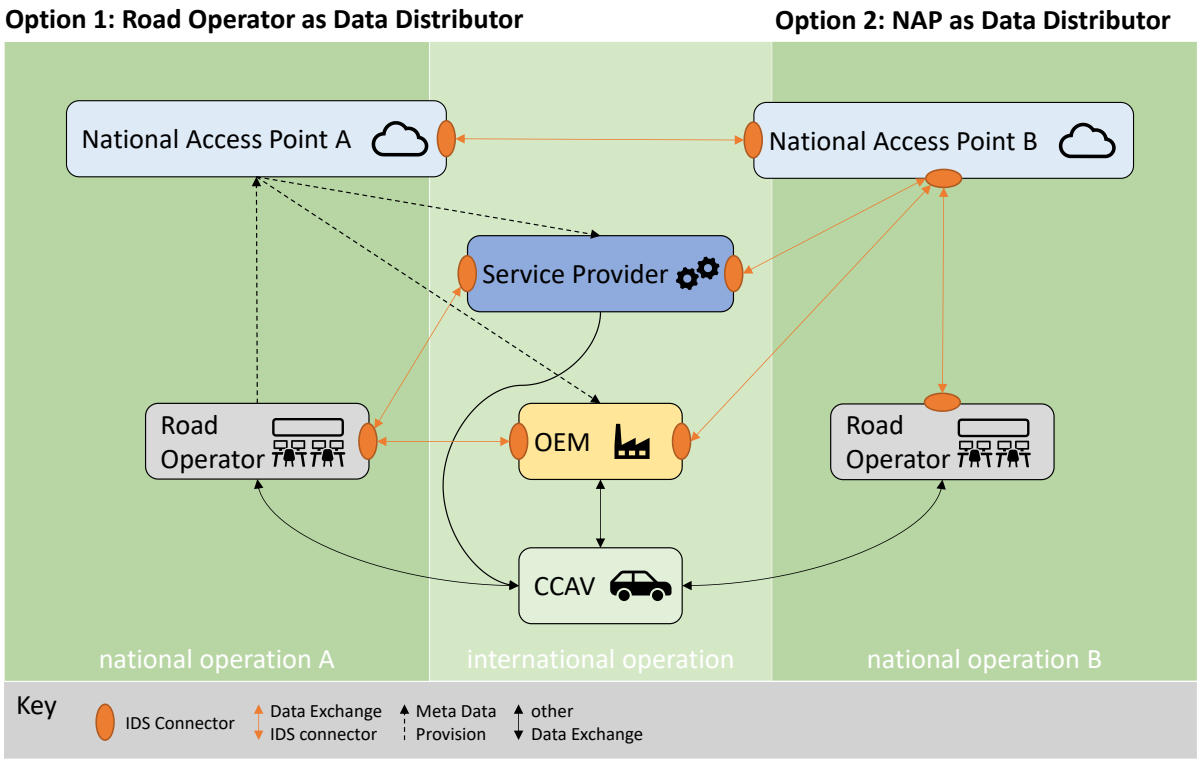

Figure 1: Data-exchange between NRAs, Service Providers and OEMs based on IDS

On closer examination, both options have advantages and disadvantages. Option 2 could provide the blueprint for a distributed European Mobility Dataspace, which would greatly facilitate access to mobility data and open up previously unused data sources in Europe. In fact, some effort is needed to upgrade the NAPs. The vast amounts of data resulting from the transfer of international data streams via individual NAPs must be taken into account. Accordingly, the NAP system must be scalable according to the burden. In addition, further investigation is needed to determine what latencies occur during an international data transfer. Under certain circumstances, too high latencies could preclude the exchange of data from which safety-relevant traffic messages are to be derived, so that other solutions or at least solutions that reduce the load on the network (e.g. pre-processing or filtering) must be found for this.

Option 1 could be implemented more quickly but requires the willingness of internationally operating service providers and OEMs to implement and manage a large number of connectors to the individual data sources. Because of the "proximity" to the data source, the problem of high latencies is expected to occur less frequently, if at all.

Both options have in common that the data, such as the following are provided harmonised as far as possible:

- Static data which considers the digitized information about the road and traffic regulations.
- Traffic data that include for example traffic volume, speed, occupancy, and travel times per lane, plus vehicle types and the SAE levels.
- Events or conditions that are primarily safety-related and are covered by the SRTI.
- Dynamic regulations that include dynamic speed limits; road, lane and bridge closures; and road works.

There should be broad agreement on the data models to be used. A recurring point of discussion is also the provision of data in a defined quality or at least the provision of quality information in parallel with the data provided, enabling the recipients to evaluate the data.

Despite the high effort, it might be preferable to have a common approach for selecting one of the deployments of Option 2, at least for the long-term considering the Commission’s NAP future plans (see section 5.1). Support for a mixed concept could be a good way to start off, as long as it is unclear if a common approach, which most countries agree to, could be realised and migrate in a later stage. The impact of latencies under the Option 2 on the exchange of safety related data also needs further investigation. This could have an impact on the routing of data and whether time savings can be achieved by pre-processing.

However, the IDS concept (be it in option 1 or 2) offers a vast potential in accessing data sources and integrating them into the emerging intelligent distributed network via standardised connectors while maintaining data sovereignty. It will be able to include e.g. additional data providers and specialised service providers, who can generate enormous benefits by integrating or merging additional data types and sources. Existing cooperation between companies for the exchange of industrial data has already proven this (see D.6.1, Smart Supplier Network). Initial projects are underway in the mobility sector (see section 5.9).

A German research project i.e. is investigating such possibilities by applying the IDS concept on the German NAP, following successful and operational implementations of the concept, e.g. in manufacturing. Operation of the so-called “Mobility Data Space” within the project is planned for 2022 and will provide the first comprehensive findings on the application of the IDS concept in the mobility sector.

Due to the fact that there is no real implementation and no evaluation of the system's ability to perform the intended task yet, the requirements and the feasibility of the IDS concept should be evaluated and an information exchange with the project should be arranged. Hence, as a first step and short-term recommendation is therefore to learn from this national pilot and start similar activities if applicable.

Since the IDS, taking into account data security and data sovereignty, it seems to have the potential to support trusted smart networks, it should be further examined whether data exchange with regard to CCAM is a feasible option. The current European dataspaces activities underpin this thought. Therefore, as a second step, a pilot project similar to the PoC of the Data Task Force should be considered here and should be discussed with the OEMs and Service Providers soon.

From a political perspective, water has already reached the mills. The sectoral Data Spaces are explicit part of the European Commission’s Digital Strategy and includes mobility as a sector. Therefore, the role of the NAPs needs to be strengthened, which is planned following a concept paper of [DG Move, 2020]. It states that in addition to the review of the ITS Directive and its Delegated Regulations the creation of this European Mobility Data Space includes the establishment of a stronger coordination mechanism to federate the NAPs established under the ITS Directive through an EU-wide CEF PSA.

In Germany, the automotive industry is politically urged participate in a MDS and to share their data with other transport providers. In order to initiate a Hybrid Full European Scenario and develop a long-term MDS strategy (regarding the proposed Option 2), it is necessary to use the current momentum and involve the automotive industry at the earliest time.

Project information

Project title	advanced options for authorities in light of automation and **DI**gitalisation ho**RIZON** 2040.		
Acronym - Logo	DIRIZON		
CEDR Topics addressed	CEDR Call 2017: Automation: ☐ A. How will automation change the core business of NRA's? ☒ B. What new options do NRAs have from digitalisation and automation? ☐ C. Practical learnings for NRAs from test sites.		
Project Coordinator	Max Schreuder TNO	**Email**	Max.schreuder@tno.nl
Address	The Hague - New Babylon Netherlands	**Tel.**	+31 (0) 88 866 32 79
Partners	TNO	**Country**	NL
	Roughan & O'Donovan Innovative Solutions (ROD-IS)		IRL
	AlbrechtConsult		DE
	AustriaTech		AT
	HERE (Associated Partner)		DE
Start date **End date**	01/09/2018 30/11/2020	**Duration (in months)**	24
Project Website	https://www.dirizon-cedr.com		

Table of contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Full Title
3GPP	**3**rd **G**eneration **P**artnership **P**roject
5G	**5**th **G**eneration technology standard for broadband cellular networks
AI	**A**rtificial **I**ntelligence
AMQP	**A**dvanced **M**essage **Q**ueuing **P**rotocol
API	**A**pplication **P**rogramming **I**nterface
BASt	Federal Highway Research Institute
CAD	**C**onnected and **A**utomated **D**riving
CAM	**C**ooperative **A**wareness **M**essage
CAV	**C**onnected **A**utomated **V**ehicle
CCAM	**C**onnected and **C**ooperative **A**utomated **M**obility
CEDR	**C**onference of **E**uropean **D**irectors of **R**oads
CEF	**C**onnecting **E**urope **F**acility
CEN/TC	**E**uropean **C**ommittee for **S**tandardization/ **T**echnical **C**ommittee
C-ITS	**C**ooperative **I**ntelligent **T**ransport **S**ystems
C-Roads	**C**ooperative **R**oads
CSP	**C**loud **S**olution **P**roviders
D2D	**D**evice-**to**-**D**evice
DTF	**D**ata **T**ask **F**orce
EC	**E**uropean **C**ommission
EP	**E**xchange **P**attern
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
EU	**E**uropean **U**nion
EU-EIP	**E**uropean **I**TS **P**latform
FCD	**F**loating **C**ar **D**ata
FEP	**F**unctional **E**xchange **P**rofile
GDPR	**G**eneral **D**ata **P**rotection **R**egulation
GLOSA	**G**reen-**L**ight **O**ptimal **S**peed **A**dvice
HD	**H**igh-**D**efinition
HPC	**H**igh **P**erformance **C**omputing
I2X	**I**nfrastructure **to** everything
ICT	**I**nformation and **C**ommunications **T**echnology
IDACS	European CEF project, **ID** and **D**ata **C**ollection for **S**ustainable Fuels in Europe
IDS	**I**nternational **D**ata **S**paces

Abbreviation	Full Title
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
INFRAMIX	Horizon 2020 project, preparing road infrastructure for mixed vehicle traffic flows
IoT	**I**nternet **o**f **T**hings
ISA	**I**ntelligent **S**peed **A**ssistance
ISAD	**I**nfrastructure **S**upport for **A**utomated **D**riving
ISO	**I**nternational **O**rganization for **S**tandardization
ITS	**I**ntelligent **T**ransportation **S**ystem
LTE	**L**ong-**T**erm **E**volution, standard for wireless broadband communication for mobile devices
MaaS	**M**obility **a**s **a** **S**ervice
MDM	**M**obility **D**ata **M**arketplace
MDS	**M**obility **D**ata **S**pace
MEC	**M**ulti-access **E**dge **C**omputing
METR	**M**anagement for **E**lectronic **T**raffic **R**egulations
MMTIS	**M**ulti **M**odal **T**raveller **I**nformation
MQTT	**M**essage **Q**ueuing **T**elemetry **T**ransport
NAP	**N**ational **A**ccess **P**oint
NB	**N**ational **B**odies
NRA	**N**ational **R**oad **A**uthority
ODD	**O**perational **D**esign **D**omain
OEM	**O**riginal **E**quipment **M**anufacturer
PEB	**P**rogramme **E**xecutive **B**oard
PIM	**P**latform **I**ndependent **M**odel
PoC	**P**roof **o**f **C**oncept
PSA	**P**rogramme **S**upport **A**ction
PSM	**P**latform **S**pecific **M**odel
QoS	**Q**uality **o**f **S**ervice
REST	**R**epresentational **S**tate **T**ransfer
RO	**R**oad **O**perator
RSU	**R**oad**s**ide **U**nits
RTTI	**R**eal-**t**ime **T**raffic **I**nformation
SAE	**S**ociety of Automotive **E**ngineers
SIRI	**S**ervice **I**nterface for **R**eal Time **I**nformation
SRTI	**S**afety-**R**elated **T**raffic **I**nformation
SSTP	**S**ave and **S**ecure **T**ruck **P**arking
STOMP	**S**imple **T**ext **O**riented **M**essaging **P**rotocol

Abbreviation	Full Title
TRIAS	**T**ravellers' **R**ealtime **I**nformation and **A**dvisory **S**tandard
UC	**U**se **C**ases
UVAR	**U**rban **V**ehicle **A**ccess **R**egulation
V2I	**V**ehicle **to** **I**nfrastructure
V2V	**V**ehicle **to** **V**ehicle
V2X	**V**ehicle **to** Everything
VMS	**V**ariable **M**essage **S**igns
WG	**W**orking **G**roup
WP	**W**ork **P**ackage

Definitions

Term	Definition
ACTOR	An entity (human or otherwise) that interacts with the system for the purpose of completing an event.
ACTOR (PRIMARY)	An actor that is necessary for the deployment of a use case. It has a goal with respect to the system - one that can be satisfied by its operation. It not only has a primary interest in the use case but can may also be the initiator of the Use Case.
ACTOR (SECONDARY)	A third-party actor from which the system needs assistance to achieve the primary actor's goal.
AUTOMATED DRIVING	A traffic system in which vehicles are capable of sensing its environment and operating and manoeuvring in traffic to achieve a goal, with little or no human input. It is supported by connectivity consisting of Vehicle-to-Infrastructure (V2I) communication, Vehicle-to-vehicle (V2V) communication, Vehicle to Everything (V2X) communication, Infrastructure to everything communication (I2X).
AUTOMATED DRIVING SYSTEM	The hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a level 3, 4, or 5 driving automation system (SAE J3016 June 2018)
DEVICES	The components of an Information Technology (IT) network that permit the communications needed required for data applications and services (such as servers, routers, detection systems etc.).
DIGITAL INFRASTRUCTURE	A digital infrastructure includes and facilitates V2I, V2X and V2V communication
DIGITALISATION	The implementation of digital technologies, which when combined with Information and Communication Technology (ICT) tools, assist in making transport modes more interoperable and smarter
DIGITISATION	The process of converting physical information into a digital format.
OPERATIONAL DESIGN DOMAIN (ODD)	A description of the specific operating conditions in which the automated driving system is designed to properly operate. It includes but is not limited to roadway types, speed range, environmental conditions (weather, day/ night time, etc.), prevailing traffic law and regulations, and other domain constraints (SAE J3016 June 2018).
PHYSICAL INFRASTRUCTURE	All infrastructure on the road including, but not limited to, grass verges, roadway widths, cross sections, safety barriers, signage, lines, power requirements ducting and C-ITS based devices.
PUBLIC KEY INFRASTRUCTURE (PKI)	A set of dedicated policies, procedures and technology that are needed to deal with digital certificates in a public key cryptography scheme. This includes Certificate Authorities (CA) communication for initial enrolment of ITS stations, certificate requests and re-keying and certificate renewal (ENISA, 2019 & C-Roads, 2018c)

Term	Definition
SYSTEM	It comprises a set of sequences of actions and variants that are performed within it and lead to value of an actor. It can be a complex combination of various components that interact each other to satisfy individual objectives.
SYSTEM SECURITY	It consists of all functions required for a secured message generation, i.e. signature generation, key and certificate handling, as well as authentication (verification) of received messages (C-Roads, 2018c).
USE CASE	A function of the system, the desired behaviour (of the system and actors), specification of system boundaries and definition of one or more usage scenarios. It combines all possible scenarios that can occur when an actor tries to achieve a certain technical objective (business goal) with the help of the system under consideration.

1 Introduction

1.1 Project Background

The CEDR Transnational Research Programme was launched by the Conference of European Directors of Roads (CEDR). CEDR is the Road Directors' platform for cooperation and promotion of improvements to the road system and its infrastructure, as an integral part of a sustainable transport system in Europe. Its members represent their respective National Road Authorities (NRAs) or equivalents and provide support and advice on decisions concerning the road transport system that are taken at national or international level.

The participating NRAs in the CEDR Call 2017: Automation are Austria, Finland, Germany, Ireland, Netherlands, Norway, Slovenia, Sweden and the United Kingdom. As in previous collaborative research programmes, the participating members have established a Programme Executive Board (PEB) made up of experts in the topics to be covered. The research budget is jointly provided by the NRAs as listed above.

The digitalisation of road networks and the rapid developments in automated driving will affect the core activities that (national) road authorities carry out and provide them with new and more efficient ways to achieve their goals for road safety, traffic efficiency, the environment and customer service. In this context, digitalised data plays a key role and enables the connectivity needed to improve efficiencies in managing, maintaining and operating the road network. Equally, digitalisation, along with connectivity, are crucial prerequisites to enable automated driving. Digitalisation of road assets can provide a number of benefits to road authorities including new (business) opportunities resulting from data sharing, the improvement of enhanced traffic management with Intelligent Transport System (ITS) equipment, improved asset management thus allowing for more reliable performance monitoring of assets and more efficient maintenance processes. Road Operator (RO) business practices will need to adapt to exploit these opportunities

To support road authorities in their digital transition and in their interaction with other actors in cooperative automated driving, the Conference of European Directors of Roads (CEDR) commissioned and funded the "advanced options for authorities in light of automation and DIgitalisation hoRIZON 2040", (DIRIZON) project in the Transnational Research Programme Call 2017 on "Automation". The DIRIZON project's goal is to assist the aforementioned road authorities and Road Operators in identifying how these developments will affect their operations and their interaction with others. In this respect, DIRIZON will determine the implications of digitalisation and automated driving on specific core topics and their consequences on data needs and requirements for data-exchange.

1.2 WP5 Scope in DIRIZON

Work Package 5 (WP5), "Towards a Digital Platform", focuses on a growing technical cooperation between NRAs, service providers and OEMs. In order to make this cooperation efficient in the long term, WP5 will provide a suitable data exchange concept depending on the requirements of the use cases by focussing on connected stakeholder backends (cloud-to-cloud services). Initially a single and uniform platform for all NRAs was planned. However, following consultation with relevant stakeholders during the DIRIZON workshop in Brussels on 26th November 2018, it was agreed that a uniform architecture for the exchange of traffic data would be unlikely in a dynamic future of the countries concerned due to the heterogeneous landscape and preferences (see also section 1.4)

WP5 starts with the thesis that any type of future connected automated driving scenario will generate a need for substantial improvements in data exchange between road authority backend systems, service provider backends and OEM backends (cloud-to-cloud services). Appropriate services would pave the way for providing data services directly into vehicles, mobile devices or aftermarket devices used inside vehicles and, vice versa, providing sensor-data back to the connected backends. Assuming that such cooperating backends in combination with an appropriate business model in the sense of a joint venture (shared costs principle) will maximise benefits, WP5 will examine an innovative technical concept of such a collaboration.

1.3 Problem description

Digitalised data facilitates new activities and changes the manner in which they are carried out. The way in which individuals, government, and corporations operate has changed and is changing drastically: cars, e-scooters and bikes can be booked via app in short notice and used immediately, modern vehicles are connected with their manufacturers or with service providers to use specific services. Behind these activities, data plays a key role, especially the need for responsible handling of the data. I.e. the General Data Protection Regulation (GDPR), which went into effect on May 1st 2018, had far-reaching consequences for all personalised data.

In the light of these developments National Road Authorities (NRAs) are also preparing for digitalisation. Digitalisation will affect the core activities that NRA carry out, offers new (business) opportunities and provides new and more efficient ways to achieve goals for road safety, traffic efficiency, environment and customer service. In the end NRAs must digitise their road networks to enable new opportunities which will in turn change the way NRAs interact with existing but also new stakeholders.

NRAs are not just starting with digitalisation, already many activities are taking place with respect to the digitalisation of the road network. Digitalisation of road assets can provide a number of benefits to road authorities including new (business) opportunities resulting from data sharing, the improvement of enhanced traffic management with ITS equipment, improved asset management thus allowing for more reliable performance monitoring of assets and more efficient maintenance processes.

The C-Roads Member States envision a growth of Connected and Cooperative Intelligent Transport Systems (C-ITS) services in the future and encourage the telecommunications industry as well as the automotive industry to further investigate communication options in due collaboration with road authorities. This collaboration helps to realise future and attractive use cases complementing existing ones – also in terms of Connected and Cooperative Automated Mobility (CCAM).

The Management for Electronic Traffic Regulations (METR) becomes more and more relevant and is currently being addressed in more detail within CEN/TC 278 WG17. Within WG17 it has been found that currently legal responsibilities and authorisation schemes vary a lot between countries, states and cities. Rules are time-and-place referenced similar to a digital map. This means that in the near future it will be necessary to digitise regulation, maintain it and make it available in a secure undistorted way, e.g. via a cloud service, so that the sovereign character is preserved.

Optimisation of traffic management and vehicle intelligence is isolated and hence the solution is to break-out from the silo and create distributed functionality based on machine-machine cooperation ('the whole is more than the sum of its parts'). The use of vehicle sensors is an important aspect which has the potential to provide road operators with data for the road network where it was not available before, and on top of that can reduce the costs of providing traffic management services. Continuing discussions, for example with OEMs about automated vehicle needs with respect to the physical and digital road infrastructure are required, as the sensor technology quality is evolving.

Facilitating the sharing of data via a platform is an ambition, even more with other platforms, whether from OEMs or service providers. This will require public commitments for gradual investments and an agreement on which data will be shared by whom. This includes also the liability question, boiling down to the question who is responsible when something is wrong with the data and mishaps occur. To achieve this, insights into which data and of what quality are needed to be collected, security and access to the platform, governance, privacy issues and requirements for business models for sustainable continuation of the platform are necessary.

1.4 Methodology and Structure of the Report

DIRIZON looks to the future in which connected and cooperative automated driving (CAD) is supported by both digitalisation and connectivity which are crucial prerequisites to enable automated driving. The timeframe of the project – up to 2040 -- means that vehicles of different levels of automation will use the road at the same time. Equally, vehicles that are not connected and without automation will also use the road network. DIRIZON looks specifically to the requirements that automated vehicles will place on data needs and data quality requirements. It is assumed that the data provision for automated vehicles is adequate for the human driver (assuming it is provided in a correct and usable form) and thus the latter will not be addressed. For automated vehicles, the information will be provided in an appropriate digitized and machine-readable form.

The findings of the DIRIZON workshop, which took place in Brussels on 26 November 2018 against the background of the current discussions on the implementation of the Proof of Concept for the exchange of Safety Related Traffic Information (SRTI), had an impact on the methodology used in this Work Package. The main results of the workshop are therefore summarised below.

The discussions during the workshop and the results of the vote confirm the heterogeneity of the historically grown and nationally shaped system landscapes and also the associated different ambitions and ideas of the countries represented in CEDR.

The agreement on a uniform platform architecture for the exchange of traffic data between NRAs, service providers and OEMs seems rather unlikely. The further investigations in the context of data exchange must take up the heterogeneity of the national system landscapes and examine various options for a more individually organised data exchange between the mentioned stakeholders. Governance, security mechanisms (e.g. authenticity of the data source) and technical design options will play a major role.

With respect to business models for the NRA the data-exchange platform is also affected by the various opinions. However, the 'common' opinion is that NRAs are willing to take a leading, initiating role in the ecosystem and see a clear, yet specific role for themselves in content aggregation. Dealing with the ecosystem and expected data change would require medium governance. This would mean that NRA would first introduce an ecosystem and invite other stakeholders, such as OEMs and service providers, to join. Later, however, this ecosystem must be operated and maintained in partnership.

The NRAs currently do not see the necessity to present themselves as a single seamless platform. Stimulating service innovation on the platform is seen as public responsibility, yet not exclusive to the NRAs.

This seems to point in a direction where the data access for service provides is arranged on a national but internationally coordinated level. It will not pursue a 'one-stop shop' strategy. NRAs will create some NRA specific/unique data driven services on top of these platforms. NRAs will participate in international governance bodies and pro-actively set these up, if needed. Yet such governance body will probably be focused on consensus rather than decision making powers.

For these reasons, the methodology had to be adjusted, and the objective of WP5 is now to provide a data exchange concept covering different data exchange options to enable a collaboration between NRAs, OEMs and Service Providers rather than creating a concept for a single and unified platform as such.

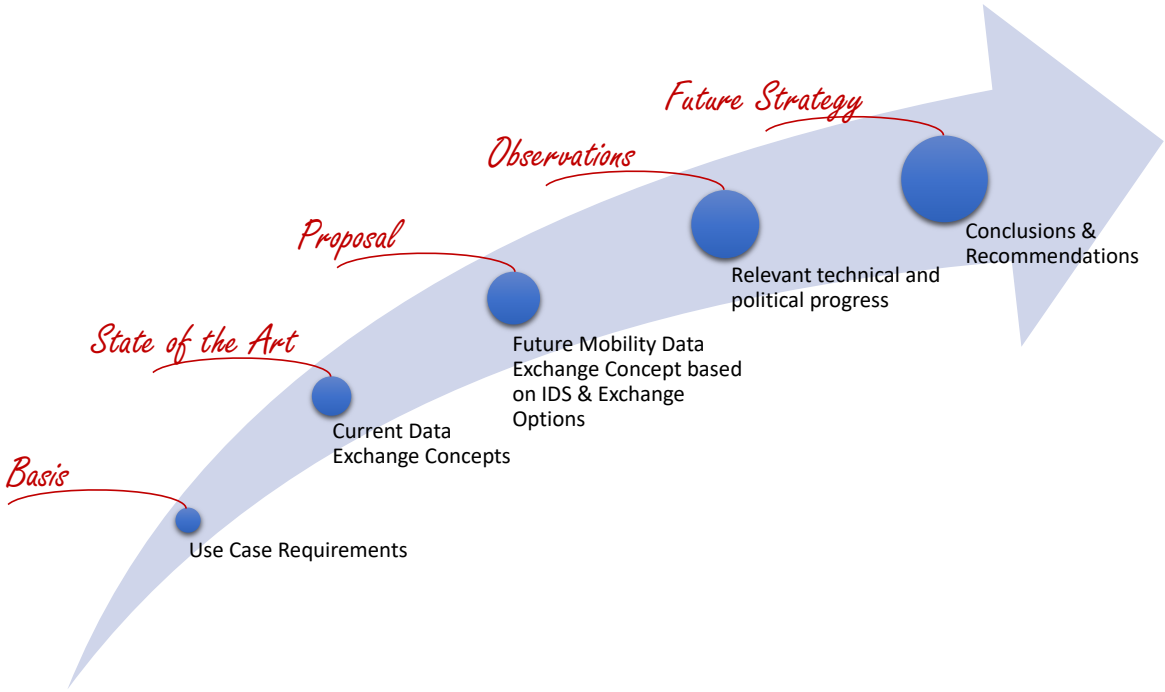

Figure 2: Report structure

In order to provide these data exchange options, the methodology comprises the following steps (see Figure 2):

- Collect use case requirements from the previous DIRIZON deliverables as basis
- Checking state of the art distributed data exchange concepts and identification of an appropriate future data-exchange
- Proposal for a future mobility data exchange concept, which prepares the foundation and technical options to implement Use Case 3 "Infrastructure Support for Automated Driving" as the most complex use case.
- Consider current technical and political progress that is relevant for the implementation of the proposed future mobility data exchange concept.
- Derive recommendations and conclusions for a future strategy.

2 Use Cases requirements

As described in Deliverable D3.1 [Malone et. al, 2019] DIRIZON approached the broad topic of digitalization by identifying three use cases (UC). The use cases provided the specificity needed to answer the questions posed within the project.

1. Provision of High-Definition (HD) maps for automated mobility
2. Distribution of digital traffic regulations
3. Infrastructure support services for cooperative automated driving

The three use cases cover many but not all the possible aspects of data related to digitalisation and automation, for example, the use case of road infrastructure maintenance using digitalized information.

The three use cases are conceptually linked, as illustrated in Figure 2 and the DIRIZON project sees the use cases as being different layers all within a High-Definition (HD) map.

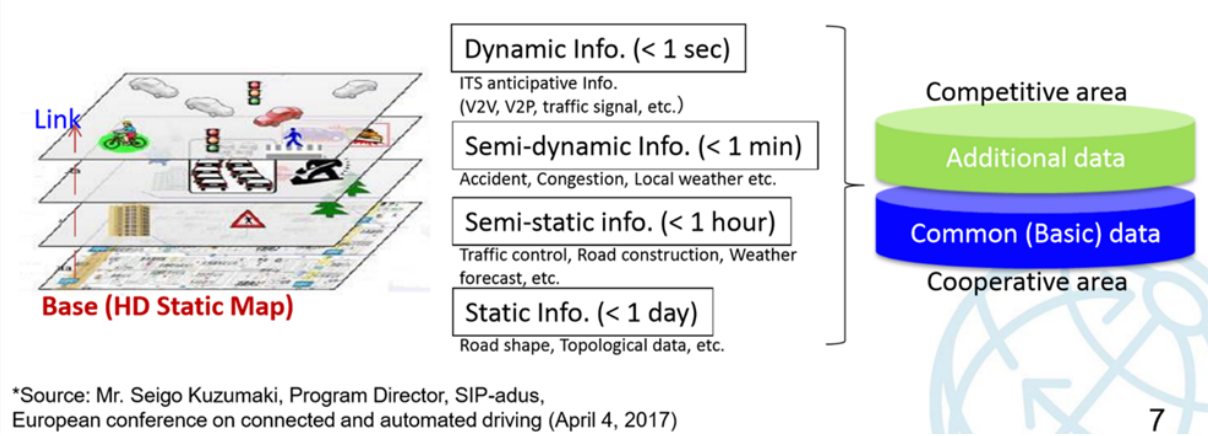

Figure 3: Visualization of the layers and data types for a High-Definition (HD) map. Source: presentation of Jun Shibata at the SIS 37, 12th ITS European Congress Strasbourg, June 21, 2017 [Shibata, 2017]

The basis or base layer is the static data in the HD map. The next layer, the distribution of digital traffic regulations adds traffic regulations in digital and machine-readable form. The top layer, infrastructure support for connected and cooperative automated driving (ISAD) is digitized information, on top of the HD map and the digitized traffic regulations layers, to support CAD functioning. This UC covers vehicles in a mixed environment, supporting connected automated vehicles (CAVs) by extending their Operational Design Domain (ODD), and improving safety, traffic flow and environmental impacts. Figure 2 illustrates the layers of a HD map. It shows layers that differ according to how static or dynamic these data are. Conceptually, the HD map integrates layers of different types of data, which can come from different use cases.

D3.1 [Malone et. al, 2019] derived data types and data requirements (quality criteria) using the conceptual framework of the layered HD map shown in Figure 2 for the three UCs with regard to CAV:

- Static data which considers the digitized information about the road and traffic regulations. These include the road model, road classification, location of tolling stations, lane model including speed limits, access conditions, and other static traffic regulations, the HD localization model (beacons, landmarks), the locations of, for example, parking spaces and service areas, charging points, public transport stop, and delivery areas.

- Traffic data that include for example traffic volume, speed, occupancy, and travel times per lane, plus vehicle types and the SAE levels. The concepts in INFRAMIX require knowledge of SAE-levels in the traffic stream [INFRAMIX, 2018]. It is not clear if these are of individual vehicles or at an aggregate level.
- Events or conditions that are primarily safety-related and are covered by the SRTI. These include temporary slippery road, animal etc on the road, unprotected accident area, short-term road works, reduced visibility, wrong-way driver, unmanaged blockage of a road, and exceptional weather conditions. This list can be expanded to include additional services, like end-of-queue warning.
- Dynamic regulations that include dynamic speed limits; road, lane and bridge closures; and road works.

WP5 examines the technical aspects of a collaboration between NRAs, OEMs and Service Providers. Therefore, the requirements for the data to be exchanged in the UCs are analysed with regard to the data exchange options, which considers mainly the technical requirements, rather than the content-related requirements (e.g. geographical coverage, accuracy, etc.). Hence, only the following criteria will be considered:

- Timeliness/ Latency: the total time between the detection of an event or a change, and the delivery to the user.
- Refreshment rate: The rate at which the data are updated in the vehicle, regardless if there has been a change in the data provided or not. This criterion is expressed in refreshments per unit of time. It can be seen as the sum of latency and timeliness.
- Availability: Percentage of the time that the service is available with fresh data. Expressed as a percentage of the time. It can be interpreted as “up time” of the system.

Table 1, identifies the preferred data types and requirements for the use cases in respect of CAV [Malone et. al, 2019]

	Timeliness/ Latency*	**Refreshment**	**Availability**	**Source of information**
Static data	Within a day	Weekly/ Daily	98% (=51/52 weeks of the year)	Estimate of HD map developer: If the newer data are not available, the old map data is available.
Traffic data	<5 minutes	30-60 s**	95% (347 days/year)	[INFRAMIX, 2018], pp 55, 58; [EU-EIP, 2018]
Safety-related events or conditions	<2 minutes	<1 minute	99.9% (365 days / year)	SRTI [EU-EIP, 2018].
Dynamic traffic regulations	<2 minutes	<18 s	99.9% (365 days / year)	Based on SRTI [EU-EIP, 2018] p.16: H 4 stars, Refreshment rate has been calculated
* Consistent with refreshment ** To support ISAD level A				

Table 1 Data types and requirements for the use cases in respect of CAV

3 Current data exchange concepts

3.1 Intelligent Transport Systems and National Access Points

Intelligent Transport Systems (ITS) are advanced applications which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and 'smarter' use of transport networks.

ITS integrates telecommunications, electronics and information technologies with transport engineering in order to plan, design, operate, maintain and manage transport systems. The application of information and communication technologies to the road transport sector and its interfaces with other modes of transport are aiming to make a significant contribution to improving environmental performance, efficiency, including energy efficiency, safety and security of road transport, including the transport of dangerous goods, public security and passenger and freight mobility.

Advances in the field of the application of information and communication technologies to other modes of transport should now be reflected in developments in the road transport sector, in particular with a view to ensuring higher levels of integration between road transport and other modes of transport.

In the recent years the facilitation of the (cross-border) electronic data exchange between the relevant public authorities and for example stakeholders as ITS service providers, the private digital map producers became more and more important in order to enable EU-wide interoperable and in particular safety relevant travel and traffic services to end users.

To speed up the development the EC has published several Delegated Regulations supplementing the ITS Directive 2010/40/EU. These legal documents imply action to several stakeholders. Amongst others Member States shall manage National Access Points (NAP) to facilitate access to the data.

A NAP is a web-based portal handling data concerning Safe and Secure Truck Parking (SSTP Delegated Regulation (EU) No 885/2013), Real Time Traffic Information (RTTI, Delegated Regulation (EU) 2015/962), Safety Related Transport Information (SRTI, Delegated Regulation (EU) No 886/2013) and Multimodal Travel Information (MMTI, Delegated Regulation (EU) 2017/1926). National Bodies (NB) have been assigned to carry out the assessment of compliance of NAP data and services suppliers. Currently, round 30 NAPs exist are implemented in significantly different ways, e.g. database, data warehouse, data marketplace, web portal etc. [EU EIP, 2020].

An important harmonisation item is Metadata, describing the datasets in NAPs, in structured and agreed manner. European NAP partners, under the coordination of EU EIP, have developed an update of the "Coordinated Metadata Catalogue" [Coordinated Meta data Catalogue, 2019]. This work is a blueprint for Metadata structures at each individual NAP in Europe. It defines a common, minimum Metadata set, in particular 32 Metadata elements, including their description, types and obligation levels. The Metadata Catalogue is considering all data and information domains of the EU Directive and the respective Delegated Regulations. The current update of the "Catalogue" also covers multi-modal travel data and services, according to Delegated Regulation (EU) No 2017/1926.

In fact, only a few NAPs transmit data themselves. However, the data must be provided via the standards DATEX II, NETEX, SiRi, etc. In the road transport sector, DATEX II, among others, has become well established. It has already been used operationally for many years for national and international traffic data exchange. DATEX II is a multipart standard maintained by the CEN Technical Committee 278, Road Transport and Traffic Telematics.

Initially, DATEX II has been developed to grant data exchange between Traffic Control (and Management) Centres, Traffic Information Centres and Service Providers. Based on a first DATEX II profile the data exchange could be established via the HTTP Application Layer Protocol (see Appendix, Section 8.2.3). As a further development a concept of Functional Exchange Profiles (FEP) and implementing Exchange Patterns (EP) (see Appendix, Section 8.1) have been introduced to define the set of consistent features enabled by a certain abstract technology which may fulfil a set of such consistent requirements.

ITS applications do usually not exchange sensitive and protectable data. Therefore, it should be noted that DATEX II does not provide explicit security mechanisms. Nevertheless, it is possible to protect the data exchange on protocol level and, if necessary, by a public key infrastructure. Where data is exchanged between road operators and service providers, it may be necessary to agree on bilateral data exchange policies or explicit contracts.

3.2 Cooperative Intelligent Transport Systems

The European ITS Directive 2010/40/EU contains a priority area (IV) on linking the vehicle with the transport infrastructure. Traditionally, the ever-increasing infrastructure intelligence monitors vehicles as moving chunks of metal, whereas the increasingly intelligent vehicles treat infrastructure as a stretch of tarmac with some graphical annotations (markings, signs). It was an obvious research topic since the 1980's (DRIVE, PROMETHEUS) to try to connect these two intelligences and create a whole that is more than the sum of its parts.

One major challenge was to find a proper technical connectivity platform. When the research started, cellular mobile networks were far from providing the required service level. The initial approach taken was to focus on short-range ad-hoc radio connectivity, with promising results achieved in tests based on WLAN technology (media access based on the IEEE 802.11 set of standards). When basic arrangements for a global use of a spectrum in the 5.9 GHz could be achieved, the way was clear towards deployment.

On the vehicle side, the Car2Car Communication Consortium was founded in 2002 *"with the objective of developing European standards for C-ITS, as prerequisite for interoperability of systems improving road safety and road efficiency"*. The European Commission launched calls that were inviting the creation of a comparable cooperation platform for the infrastructure, to agree on interoperability specifications as a mandatory requirement for European deployment: C-ROADS. In parallel, the EC worked on a proposal for a Delegated Regulation.

What happened in between was that new generations of cellular mobile network technology had identified the potential benefits of integrating this type of direct device-to-device communication into the context of the radio access to cellular networks. The first D2D features appeared in 3GPP's Release 12 in 2015. Mobility/Automotive applications were seen as one of the most promising fields of application, so the role of general D2D was specialised into Cellular V2X – combining D2D and cellular approaches – in sub sequent releases.

Hence, this new group of actors (Mobile Network Operators, supply industry, chipset manufacturers) made a strong effort to promote their technology as an alternative and highlight its advantages. They were concerned the proposed Delegated Act of the European Commission was preventing their technology from entering the market and due to their argumentation, it was eventually rejected by the European Council, which created a vacuum that reduced the speed of deployment for a while.

A C-ITS Deployment Group was founded by those who continued their deployment plans, and now we see quite a few large, ITS-G5 (WLAN) based C-ITS deployments being on their way on the infrastructure side, together with the first, ITS-G5 enabled mass production vehicle (VW Golf 8) entering the market.

If we analyse data exchange and sharing concept underlying C-ITS, we must take note that it has very special technical characteristics. Communication is only available in spatial proximity (a few hundred meters for direct communication, extensibility only via 'multi-hop' forwarding) and it is a uni-directional data broadcast. Relevance of received information is determined by all receiving stations in radio range themselves, as part of their message processing. Transactional communication patterns are not possible, unless implicitly realised by broadcasting corresponding messages[1].

This very specific communication technology has been proven to be well suited for vehicle-vehicle as well as vehicle-infrastructure communication for safety-related applications that react in real-time on events and actors in the near vicinity. It is not well suited to serve general purpose ITS applications that look at a wider horizon, e.g. navigation, or that require direct transactional communication patterns, e.g. booking services. It should further be noted that although much effort has been put into providing a complex IT security infrastructure for C-ITS, the underlying mechanism only addresses a limited set of security aspects, in particular authentication. They do not provide any type of protected privacy, since all communication is unencrypted.

There is a current strive to extend the principles of C-ITS communication (in particular the agreed services, use cases and corresponding message types and the certificate-based authentication of message senders) to vehicles that do not have ITS-G5 or Cellular V2X radio equipment. The principle idea is that most of such vehicles nevertheless have mobile internet connectivity in one way or another, e.g. because the vehicle itself is connected to a backend of the OEM or because the driver operates a smartphone app during the trip that receives information from a service provider. The basic idea is that a much larger amount of vehicles could be reached via this path, which would accelerate the deployment of C-ITS services and the achievement of the expected benefits can be expected earlier. Nevertheless, since the C-ITS paradigms had been developed very much tailored to the very specific communication pattern of short-range radio broadcast described above, it is still to be seen whether this approach is viable compared to the various other ways of using the (mobile) internet for the same purpose that do already exist or are being developed in parallel.

3.3 Data Task Force Proof of Concept

All European Transport Ministers, the European Commission and current industry partners established the Data Task Force (DTF) during the High-Level Meeting on Connected and Automated Driving on 15 February 2017 in Amsterdam. The DTF is looking at means for data sharing of Safety-Related Traffic Information (SRTI), *"improving road safety by means of the large-scale use of vehicle data."*. The Data Task Force launched a proof of concept to collect data for road safety [Felici, 2019].

The Data Task Force classify SRTI related data is defined in levels, Table 2:

Level 1	• Single sensor reading, raw sensor data • This information does not leave the vehicle and is not part of the data distribution
Level 2	• From one vehicle, one or multiple sensors used to create OEM specific interpretation of basic observations (safety relevant events), e.g. “traction loss” or “heavy rain” (available at OEM backend)

[1] As an example, signal setting can be requested by broadcasting a Signal Request Message, the traffic signal might react on reception and broadcast a Signal Status Message in response.

	• Data necessary for providing the road safety related minimum universal traffic information service and collected via any private and/or public source • Role of partner: **Sources**
Level 2'	• From multiple data sources (multiple vehicles) in one feed • Enriched version of Level 2 Data created by cross referencing the data (L2) across multiple vehicles, vehicles from different brands and/or through data harmonization and cleansing of the Data (L2) • Role of partner: **Aggregators**
Level 3	• Information: Any extracted, aggregated and processed road safety related traffic information, offered by public and/or private road operators and/or service providers to end users through any delivery channels • Role of partner: **Data creators (service creators), service distributors**

Table 2 SRTI related data levels

Level 3 as defined by the Data Task Force has the scope of SRTI as defined in the Delegated Regulation (EU) 886/2013 in eight categories:

1. temporary slippery road
2. animal, people, obstacles, debris on the road
3. unprotected accident area
4. short-term road works
5. reduced visibility
6. wrong-way driver
7. unmanaged blockage of a road
8. exceptional weather conditions

The Proof-of-Concept of the Data Task Force was a first test environment to collect in-vehicle data for the purpose of creating such SRTI Level 3 information. The evaluation of what can be achieved by this approach is still on-going, but first results hint at significant benefit that can be expected.

The PoC does not yet include data quality checking or information on the level of automation of the vehicle. Future activities can incorporate these challenges as well as lessons learned from the Proof-of-Concept.

The MoU – originally set up to expire June 3rd, 2020 – has been extended to October 2020. In December 2020 the Data for Road Safety initiative announced that it is aiming for the long term deployment of a Safety-Related Traffic Information (SRTI) ecosystem [DTF, 2020].

In technical terms, the PoC signatories documented the technical agreements they could achieve. Whilst this should not be seen as final or limiting, it is definitely worth noting that the PoC partners could agree in general to use SENSORIS as a promising standard for the provision of vehicle data (L2 and L2'), whilst the flow of SRTI information back towards the OEM backends was agreed to use a flow via the National Access Points, coded in DATEX II as indicated by the Delegated Regulation. It is also interesting to note that those partners receiving L2/L2' fleet information and processing L3 SRTI out of this actually can now provide information that have a geographic scope that goes beyond National borders. It is an interesting and ongoing debate how such data publications should be published in a landscape of National Access Points.

3.4 International Data Spaces

A further level of networking is represented by cloud services, which use their resources to generate scalability for data management business models. This makes it possible, for example, to operate computationally intensive forecast models, AI applications or data-intensive analyses on a customer-specific basis, which would not be affordable for a single conventional platform. In addition, the awareness has raised to rethink data management. Until now, much effort has been put into pre-selecting data (no sensitive data), categorising and segmenting the data and transmitting it to interested stakeholders according to a harmonised data model. At the same time, the stakeholders have so far had little opportunity to customize data in a required and flexible manner (e.g. via APIs, see chapter 8.2.4).

Furthermore, e.g. transport companies or fleet operators are reluctant to make more extensive mobility data available to third parties. The reasons for this are manifold. Either trustful and beneficial partnerships for data exchange are lacking, or established data formats and interfaces are not yet available and therefore some areas not yet covered. More sensitive data, such as passenger flow data generated by vehicles or personal mobile devices, seem to be collected and processed by transport companies, navigation service providers, fleet operators or mobile phone companies. However, their cross-organisational use, processing and linkage with other data has so far hardly taken place due to their sensitivity with regard to data protection, informational self-determination and protection of business secrets.

The International Data Spaces (IDS) initiative has addressed amongst others this issue.

The IDS was conceived by the Fraunhofer-Gesellschaft in 2015 to create a secure data space for the sovereign management of data assets for companies in various industries and has therefore its origins not in the mobility domain. Following industry's positive response to the initiative, the International Data Spaces Association e.V. was founded in 2016. At the time of writing this deliverable more than 101 companies and institutions of various industries and sizes from 20 countries including several Fortune 500 companies, global acting medium-sized companies, software, and system houses are members of the association.

The IDS is a peer-to-peer network, a virtual data space that supports the secure exchange and the linking of data in business eco-systems on the basis of standards and by means of common governance models. The IDS is mainly specified in the IDS reference architecture (IDS-RAM) and aims at meeting the following requirements [IDS-RAM, 2019]:

- Trust
  Trust is the foundation of the IDS. Each participant is certified before being granted access to the trusted business ecosystem.
- Security and Data Sovereignty
  All components of the IDS are based on state-of-the-art security measures. Apart from the architecture, security is mainly guaranteed by certification of each technical component used in the IDS. To ensure data sovereignty, a data owner in the IDS attaches usage restriction information to his or her data before it is transferred to a data consumer. To be able to use the data, the data consumer must fully accept the data owner's usage policy.
- Data Ecosystem
  The architecture of the IDS does not require central data storage. Instead, it follows the idea of decentralizing data storage, which means that the data remains physically with the data owner until it is transferred to a trusted party. This approach requires a comprehensive description of each data source and the value and usability of the data for other companies, combined with the ability to integrate domain-specific data vocabularies. In addition, brokers in the ecosystem provide real-time data discovery services.

- Standardised Interoperability
  The IDS Connector, being a significant component of the architecture, is implemented in different variants and can be acquired from different vendors. Nevertheless, each Connector is able to communicate with any other Connector (or other technical component) in the ecosystem of the IDS.
- Value Adding Apps
  The IDS allows to inject apps into the IDS Connectors in order to provide services (i.e. services for data processing, data format alignment, and data exchange protocols) on top of data exchange processes according to the usage policy.
- Data Markets
  The IDS enables the creation of innovative, data-driven services that make use of data apps. It also fosters new business models for these services by providing clearing mechanisms and billing functions, and by creating domain-specific broker solutions and marketplaces.

It is worth noting that if these requirements have been correctly turned into features - and this can be assumed, since there are numerous use cases in the industry - the IDS concept seems to bring along many mechanisms natively, which were previously technically combined manually, e.g. at project level.

4 Future Mobility Data Exchange Concept

4.1 Why IDS?

In order to enable seamless and interoperable exchange of data between NRAs, service providers and OEMs, throughout Europe or beyond, an approach is needed which allows to interconnect their existing platforms and different system landscapes.

With the increasing need in recent years to provide mobility data (also due to the ITS Directive) or to exchange data between NRAs and service providers or meanwhile also with OEMs, the requirements for the technical implementation also grew. The following requirements are to be noted at this point in time:

- Interoperability, such that different implementations can successfully engage in a data exchange process;
- Support legacy implementations which are based on existing (exchange) specifications, in order to maximize investments already made by stakeholders;
- Address other user profiles, not only road operators, and thus make this concept available to a broader community;
- Reuse of existing (communications) standards, in order to reduce implementation complexity and take benefit of proven and already existent solutions for common ICT problems;
- Ensure data security to protect the exchanged data against misuse through unauthorized actors;
- Ensure data sovereignty through usage control as a new aspect to make data available that have to be treated from a e.g. GDPR point of view.

The latter two requirements in particular have so far been difficult to implement with the current exchange concepts in the mobility sector, which in principle aim at creating a secure data space (to express it in IDS words). For example, the introduction of a PKI in the context of C-ITS has been a time-consuming process, and many stakeholders are still struggling with its implementation. The issue of data sovereignty is becoming increasingly clear when co-operating i.e. with OEMs. I.e. the co-operation agreement for the PoC explicitly defines who, when and how the data provided may be used.

Thus, why not use a proven data exchange concept that natively supports the mentioned requirements and in particular the last two requirements and enables the consideration of the heterogeneity of historically grown and nationally shaped system landscapes, the associated different ambitions and ideas of the countries represented in CEDR?

The IDS concept seems to be a very well suitable concept to take up the national diversity by offering various options for a more individually organised data exchange between the mentioned stakeholders. At the same time, the IDS concept offers the opportunity to develop a smart trusted dataspace on an international level. Therefore, DIRIZON wants to use this concept and show the potential in the following.

4.2 IDS Reference Architecture

The IDS Reference Architecture [IDS-RAM, 2019] defines an appropriate and industry proven reference architecture. Focusing on the generalization of concepts, functionality, and overall processes involved in the creation of a secure “network of trusted data”, the IDS-RAM resides at a higher abstraction level than common architecture models. It provides an overview which is supplemented by more detailed specifications in which the various components of the IDS (Connector, Broker, App Store, etc.) are defined in detail.

In accordance with common system architecture models and standards, the IDS-RAM model uses a five-layer structure that expresses the concerns and views of different stakeholders at different levels of granularity as simply shown in Figure 4:

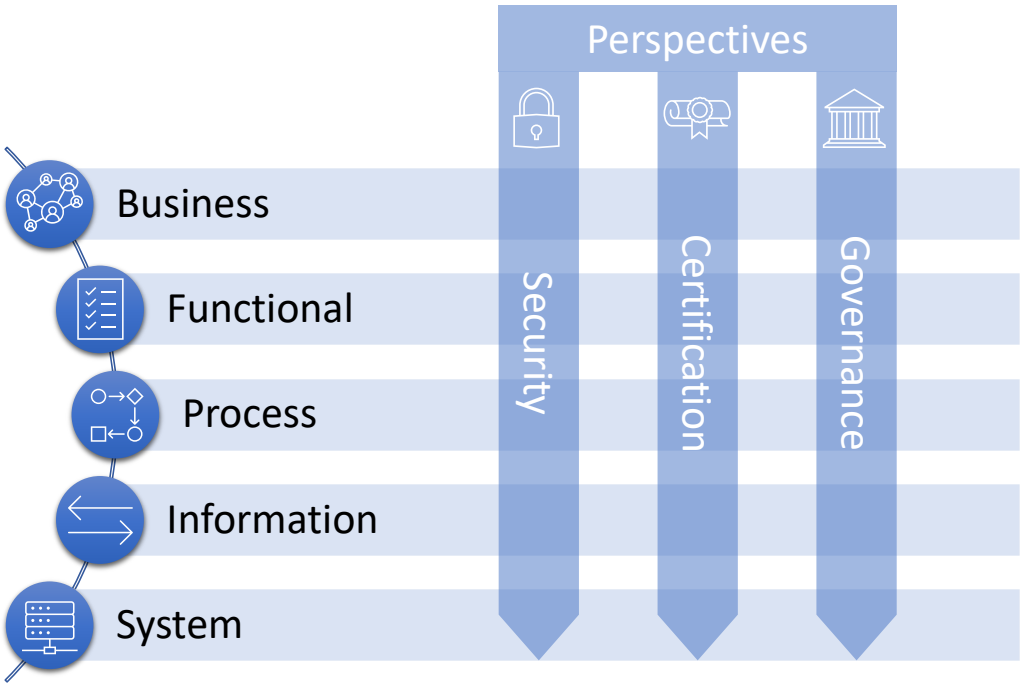

Figure 4: IDS-RAM: Layers and Perspectives

The Business Layer specifies and categorizes the different roles which IDS users can assume, and it specifies the main activities and interactions connected with each of these roles.

The Functional Layer defines the functional requirements of the IDS and the concrete related features.

The Process Layer specifies the interactions taking place between the different components of the IDS, using the Business Process Modelling Notation, which provides a graphical notation for specifying business processes in a diagram based on a flowcharting technique very similar to activity diagrams.

The Information Layer defines a conceptual model which makes use of linked-data principles for describing both the static and the dynamic aspects of the IDS’s elements.

The System Layer is concerned with the decomposition of the logical software components, considering aspects such as integration, configuration, deployment, and extensibility of these components.

In addition, the Reference Architecture Model comprises three perspectives that need to be implemented across all five layers: Security, Certification, and Governance.

With the Security Perspective on the different layers means are provided to identify actors, protect communication and data exchange transactions, and control the use of data after it has been exchanged. For these purposes, the IDS defines a (trusted) Connector (see Section 4.3). The IDS Connector ensures that the specifications and requirements of the Security perspective materialize in everyday interactions and operations in the IDS.

The Certification Perspective provides means for each layer to certify i.e. actors and core components to ensure data sovereignty. Data sovereignty can be defined as a natural person's or legal entity's capability of being in full control of its data. Therefore, any organization or individual seeking permission to access the IDS is certified, and so are the core software components (e.g. the IDS Connector) the actors use to securely exchange data with one another. While the certification of organizations and individuals focuses on security and trust, the certification of components also refers to compliance with technical requirements ensuring interoperability.

The Governance Perspective defines the roles, functions, and processes from a governance and compliance point of view. It thereby defines on each layer requirements to be met by the business ecosystem to achieve secure and reliable interoperability.

In the following, we will refrain from explaining the IDS-RAM in detail and exhaustively according to its given structure. Interested readers can obtain further details from [IDS-RAM, 2019]. In order to illustrate the potential of the IDS in terms of transferability to the mobility domain and to recommend it as a future innovative data exchange concept, it is sufficient from a DIRIZON point of view to emphasise further essential aspects.

4.3 Relevant IDS Key Aspects for a Mobility Data Exchange Concept

Within the IDS concept each actor can assume a role, which has to fulfil basic tasks. The majority of roles require certification of the organization that wants to assume that role, including certification of the technical, physical, and organizational security mechanisms the organization employs. Certification of organizations that want to participate in the secure data space is considered a fundamental measure to establish trust among all actors, in particular with regard to roles that are crucial for the overall functioning of the secure data space, such as the Broker, Service Provider, the App Store, the Identity Provider, or the Clearing House.

These roles are defined in Table 3 below:

Role	Description
Data Owner	As the legal situation regarding data ownership is very complicated, the term 'Data Owner' is not used in a legal understanding. Moreover, an operational data management perspective has been taken, defining a Data Owner as a legal entity or natural person creating data and/or executing control over it. This enables the Data Owner to define Data Usage Policies and provide access to its data. Usually, a Data Owner assumes the role of the Data Provider at the same time. However, there may be cases in which the Data Provider is not the Data Owner in particular when the data is technically managed by a different entity than the Data Owner, such as in the case of a company using an external IT service provider for data management. In cases in which the Data Owner does not act as the Data Provider at the same time, the Data Owner needs to authorize a Data Provider to make its data available via a contract, which should include a (digital) data usage policy for the data provided.

Data Provider	The Data Provider makes data available for the sake of data exchange. As mentioned, the Data Provider and Data Owner could be combined roles. To submit metadata to a Broker, or exchange data with a Data Consumer, the Data Provider uses software components that are compliant with the Reference Architecture Model of the IDS. To facilitate a data request from a Data Consumer, the Data Provider should provide metadata about the data to a Broker (see below). However, a Broker is not necessarily required for a Data Consumer and a Data Provider to establish a connection, as i.e. shown in Figure 5.
Data Consumer	The Data Consumer receives data from a Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets in a meta data catalogue provided by a Broker. Alternatively, the Data Consumer can establish a connection with a Data Provider directly (i.e., without involving a Broker Service Provider, see). In cases in which the information to connect with the Data Provider is already known to the Data Consumer, the Data Consumer may request the data (and the corresponding metadata) directly from the Data Provider. Like a Data Provider, the Data Consumer may log the details of a successful (or unsuccessful) data exchange transaction at a Clearing House, use Data Apps to enrich, transform, etc. the data received, or use a Service Provider to connect to the International Data Spaces (if it does not deploy the technical infrastructure for participation itself).
Data User	A Data User is the legal entity that has the legal right to use the data of a Data Owner as specified by the usage policy. The Data User could be identical with the Data Consumer.
Broker	The Broker is an intermediary that stores and manages information about the data sources available in a secure data space. In principle it is a data marketplace, which serves to make data sources and their terms of use known and visible. The activities of the Broker mainly focus on receiving and providing metadata. It must provide an interface for Data Providers to send their metadata, which should be stored in an internal repository (e.g. a metadata catalogue like on a NAP) for being queried by Data Consumers in a structured manner. Metadata must be made available in a machine-readable format so that in future devices such as automated vehicles, smartphones or IoT devices can find and use them independently.
Clearing House	A Clearing House is a logging component that logs transactions in a distributed system environment and subsequently makes them available to the parties for quality analysis, conflict resolution and billing purposes. It might still be possible that the two roles “Clearing House” and “Broker” are assumed by the same organization, as both roles require acting as a trusted intermediary between the Data Provider and the Data Consumer.

Identity Provider	An Identity Provider acts as a central point of contact to verify the trustworthiness of actors, such as data providers and data consumers as well as connectors and data apps and enables secure communication based on this. The Identity Provider consist of a Certification Authority which manages digital certificates for the participants within the secure data space.
App Store	The App Store provides Data Apps. These are applications that can be deployed inside the Connector, the core technical component required for an actor to join the secure data space. Data Apps facilitate data processing workflows i.e. for processing mobility-relevant data.
Vocabulary Provider	The Vocabulary Provider manages and offers vocabularies (i.e., ontologies, reference data models, or metadata elements) that can be used to annotate and describe datasets (i.e. a meta data catalogue), which represents the domain knowledge i.e. about traffic and mobility data formats like i.e. DATEX II and NeTEx.

Table 3: Trusted IDS Roles

Participation in the secure data space is carried out via the technical Connector component, which a Data Provider or Data Consumer operates or has operated on its behalf. The Data Space is created across the interconnected Connectors and is therefore not a central platform, but an extendable network of at least two distributed actors, which Figure 5 illustrates. Before transmission to the target connector, the data set to be provided is extended by a set of rules for data usage, the so-called "usage policy". It remains in the target connector and is securely protected against direct access by the data recipient. To be able to manage the data anyway, the data set must be used within the connector by so-called "Data Apps", for example for data analysis or fusion.

These apps can include further data, e.g. from Databases of the Data Consumer, whose operation takes place outside the Connector. A usage control layer in the Connector guarantees that the data app complies with the rules specified in the usage policy, so that only aggregated results leave the connector. All steps for using and processing the data within the data space can be logged. Thus, a data provider gains knowledge of all activities regarding its data [Pretzsch et. al, 2020].

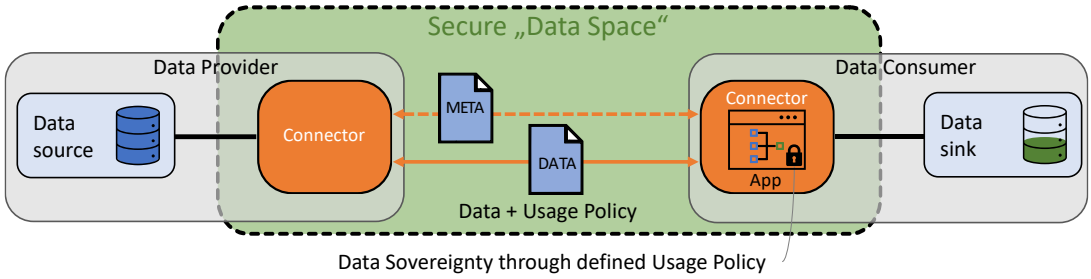

Figure 5: Functional principle to ensure data sovereignty

Beyond the minimal example above, a data space can consist of dozens or even hundreds of participants and they can join over time. Such a decentralised governed, physically distributed and growing system of data sources and services requires a Broker who provides a Meta Data Catalogue in which data sources and services can be published and searched by Data Consumer both manually and automatically. Figure 6 shows that the role of a Broker (and additional ones) can be overtaken by a NAP for example.

The NAP-Connector allows data to be exchanged between Data providers and Data Consumer, which enables data brokering, and therefore allows Data Consumers to subscribe to data publications and receive the data records provided by the Data Provider in real time. In addition to this brokerage function, the NAP connector can execute data apps to merge the data provided to the NAP, for example, to create new virtual data sources. In this way, assuming additionally the role of a Data Provider, existing NAPs can be extended to receive sensitive and protectable (mobility) data from i.e. road operators, service providers, OEMs and other data sources (even other data platforms) and to process it according to the transfer processing rules to data apps for data enrichment and data exploitation. The example shows also that a NAP can assume further roles (e.g. Vocabulary Provider, App Store, Identity Provider and Clearing House), if necessary. Due to the harmonisation activities of the European NAP partners, under the coordination of EU EIP, a “Coordinated Metadata Catalogue” should be available to be implemented in the NAP environment.

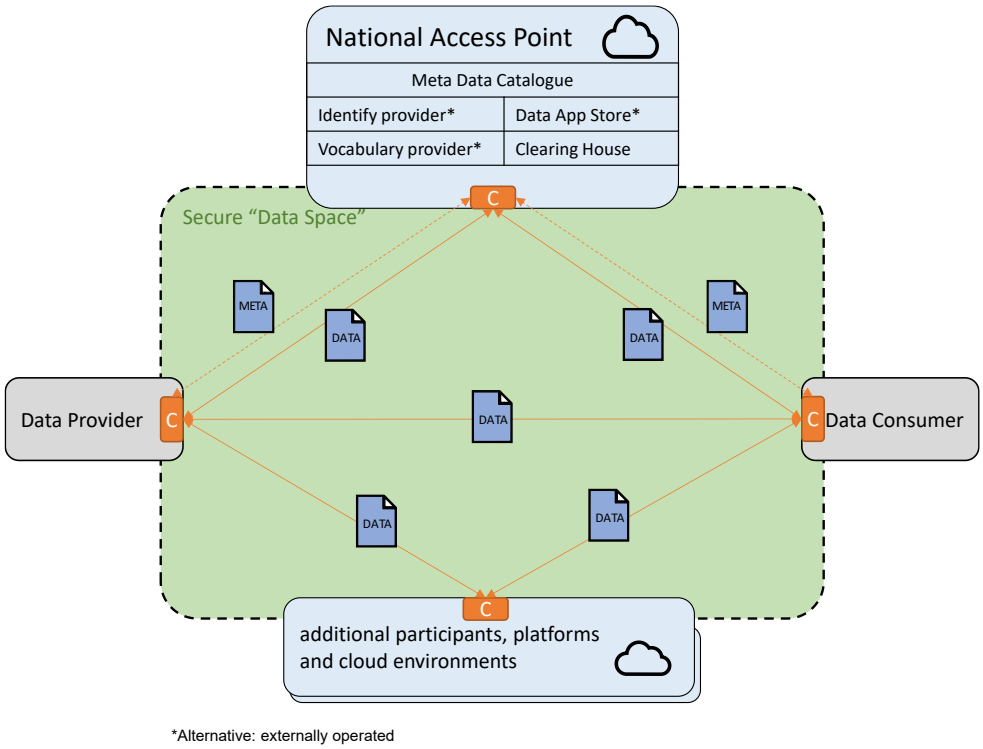

Figure 6: NAP within the distributed data exchange concept

Finally, in the sense of governance, the important role of the main components in the Mobility Data Exchange Concept is also associated with other organizational considerations [Pretzsch et. al, 2020]:

- Ensuring the non-discriminatory exchange of mobility data requires the neutrality of the operator of the main components. This can be fulfilled, for example, by a public body or by community organisations such as associations.
- The financing of the operation of the main components must be ensured - not least to create confidence within a Mobility Data Exchange Concept. If the operator is required to pay user fees to cover costs, the attractiveness of participating for all actors is reduced. Financing models such as the promotion of data services can also be at the expense of neutrality.

- The harmonisation and continued maintenance of data formats and models provided by the Vocabulary Provider must be a continuous process. An exchange and coordination with the relevant stakeholders is important to identify changing requirements for data formats and models and to develop solutions. Defined processes can facilitate stakeholder involvement.
- Since Licence and Usage Policies are new for many actors in the mobility sector, models should be offered for them.

4.4 Mobility Data Exchange Concept

4.4.1 Concept Options

Due to the complexity of the IDS concept and the lack of practical examples in the transport sector, the Mobility Data Exchange Concept is limited to the application of the reference architecture at the highest levels. It includes and reflects in principle the aforementioned IDS key aspects. It is not primarily a question of how exactly it is implemented. Rather, it is about how the national heterogeneous system landscapes can be linked to a smart mobility data network that includes service providers and OEMs.

Figure 7 below provides a simplified functional architectural view (IDS RAM business layer) of the use of the IDS Connector. In this simplified view, the main focus is on the high speed network communication (backbone communication) between the stakeholders' platforms. The multiple ways of data-exchange between vehicles and other actors are not addressed. This figure should be interpreted for multiple countries (national operation) collaborating with international operating service providers, OEMs and vehicles. That means Service providers, OEMs and vehicles are able to operate across countries while Road Operators and NAPs are operating nationally. For the sake of simplification, a limited number of actors are shown in the diagram. For example, the app stores and vocabulary providers envisaged in the IDS Reference Architecture were not considered.

The IDS Connector is identified as the interface between road authorities, data providers and service providers, in any combination, to support data distribution via a trusted Data Space.

Data described in chapter 2 originate from the road operator, a road authority (or a third party on behalf), and the information needs to be provided to service providers and/or OEMs via backbone channel. Data described in chapter 3.3 originate from OEM respective their connected fleet. However, the flow of the data and its processing depend on which actor assumes the roles of Aggregator and Service Creator/Service Distributor.

According to the Delegated Regulations supplementing the ITS Directive 2010/40/EU all Member States shall manage NAP to facilitate access to the data. The NAPs therefore also play a central role in the approach presented. They can take various forms, such as a database, data warehouse, data marketplace, repository, register, web portal or similar depending on the type of data concerned and provide discovery services, making it easier to fuse, crunch or analyse the requested data sets.

That means also that data-exchange can happen on different ways, expressed by Option 1 "Road Operator as Data Distributor" and Option 2 "NAP as Data Distributor". The distinction between these options has been made to illustrate the flexibility, differences and the consequences for the operating actors connected via IDS connectors on the backbone. A basic requirement, however, is that the metadata for the data offers can be sought via a harmonised metadata catalogue. Such a "Coordinated Metadata Catalogue" has already been harmonised between the European NAP partners, under the coordination of EU EIP, as mentioned in Section 3.1.

In the following sections the two options are described. It is also possible to mix these options as shown in the diagram. However, for clarity here the advantages and disadvantages of the separate options are highlighted. An appropriate assessment will be given in section 4.4.2.

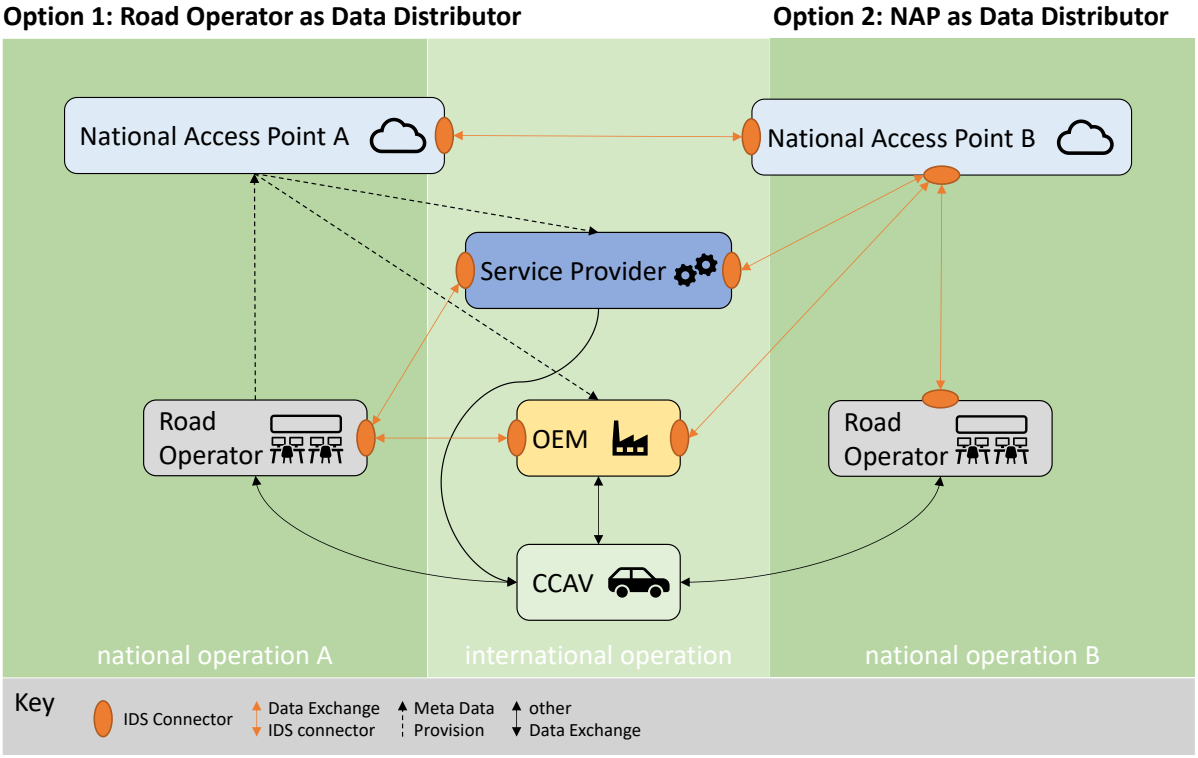

Figure 7: Data-exchange between NRAs, Service Providers and OEMs based on IDS

Option 1 “Road Operator as Data Distributor” is shown the left part of Figure 7.

Every country operates a NAP that serves at least national meta data (as NAP A). Internationally acting Service Providers and OEMs from different countries need to connect directly to all NAPs in countries where they have customers and where NAPs represent a metadata broker to investigate where to find required data sources (e.g. the Road Operators). After that they need to set up an IDS connection to each data source to establish the mobility data exchange. In this option, there would be no need to connect the different NAPs to each other.

Option 2 “NAP as Data Distributor“ is visualised in the right part of Figure 7.

NAP B represents in this case a metadata and mobility data broker which is interconnected with other NAPs via an IDS connection (theoretically just to one other NAP of the same kind). Service Providers and OEMs will (only) need to connect once to a single NAP in an IDS Network. Every NAP of kind B exchanges required data with other NAPs to serve those to the connected parties. Road Operators and potential other data source are connected to their national NAP also via an IDS connection.

4.4.2 Assessment

While the capabilities of the IDS concept have already been explained in the sections before, this section highlights the advantages and disadvantages of the two variants presented above, as summarised in Table 3

Aspect	Option 1 Road Operator as Data Distributor	Option 2 NAP as Data Distributor
Description	Service Providers and OEMs connect to all national data sources, like Road Operators.	Service Providers and OEMs connect only once to one NAP. NAPs are interconnected with each other and therefore part of a NAP network.
Technical complexity for Service Providers and OEMs	Service Providers and OEMs have many IDS connections to national data sources in each country where they are providing services to their customers.	Service Providers and OEMs have access to all information available via a single connection.
Technical complexity for NAPs	NAPs only have to serve metadata data for their own country.	The number of clients is limited, and changes to this list will happen less frequently. The NAP has to transfer requested data from all countries involved.
Technical complexity for Road Operators	Road Operators will have many more data exchange partners than in Option 2, as all Service Providers and OEMs from all countries will connect to them. This also creates a more dynamic operational environment.	Road Operators will just have to implement an IDS Connection to their national NAP.
Scalability	Road Operators have to serve more exchange partners than in the Option 2 and therefore have higher scalability requirements.	The number of clients is limited per NAP, but data need to be exchanged with other NAPs, which could cause a hight data volume. Hence, scalability on number of clients is good, but on the amount of data it is poor. In adverse situations, a large volume of data is exchanged, which is not necessarily used in reality (e.g. missing filter mechanisms).

Reliability/ Latency	As this is a locally managed solution latency and reliability to Service Providers and OEMs can be monitored and managed at a practicable level.	Due to the emerging chain of partners exchanging data with each other, the risk of higher latencies is high.
Consistency of service	As each Road Operator is responsible for his own data and has local knowledge and context. The service they are able to provide should be easier to manage and should be consistent. Service Providers and OEMs are in direct contact with the road operator and might give direct feedback.	Service Providers and OEMs are not in direct contact with their data sources. Therefore, a commonly defined and trusted service consistency must be available. Alternatively, information on consistency (e.g. quality of service) must be provided to assess the usability of the data.
Organisational complexity	For Service Providers and OEMs this option requires a huge effort to connect with Road Operators and other potential data sources all over Europe and to manage all relations.	The organisational complexity is limited. National nodes only have to deal with local customers, and with a (limited) set of other national nodes. The legal responsibility for the data provided could become an issue, as national nodes will serve data from many sources, also sources that they have no contact with directly themselves.
Business model aspects	This option focusses on a Road Operator driven scenario (see NRA driven scenario, [Berkers et. al, 2020])	This option allows a more marked driven or hybrid scenario (see marked driven or hybrid scenario, [Berkers et. al, 2020]).

Table 4 Assessment: Road Operator or NAP as Data Distributor

Depending on how strict the options will be implemented by different Member States, it is possible to have deployments based on the different options and still have international interoperability. Option 1 is the basis or starting point that needs to be supported by individual Member State to provide data from road authorities on a central level per Member State.

Option 2 can be deployed as soon as NAPs provide services beyond metadata provision. In other words: A precondition for Option 2 is, of course, that mobility data will generally be exchanged via the NAPs and not just metadata related to them.

It should be noted that pan-European Service Providers and OEMs are not tied to a single country and are free to connect to multiple national data sources. The aggregation of national data should be offered by each NAP (e.g. supported by national government).

Concepts based on Option 1 will likely evolve and can be deployed and supported at the same time. Consequently, it will become more complex to figure out what information can be obtained where. Also, if information will be provided at different places, service providers subscribing to this information need to ensure that they are able to identify duplicates and ensure they can handle that correctly. This requires the operation of well described national metadata catalogues.

Therefore, it might be preferable to have a common approach for selecting one of the deployment of Option 2, at least for the long term considering the Commission's NAP future plans (see section 5.4.1). Support for a mixed concept could be a good way to start off, as long as it is unclear if a common approach, which most countries agree to, could be realised and migrate in a later stage. The impact of latencies under the Option 2 on the exchange of safety related data also needs further investigation. This could have an impact on the routing of data and whether time savings can be achieved by pre-processing.

The move from Option 1 to 2 will depend also on the benefits for Road operators Service Providers and OEMs. Service Providers and OEMs could be reluctant to invest in a large number of interfaces, which would be required in Option 1 and rather prefer Option 2.

5 Relevant technical and political progress

5.1 General Consideration

The following Sections consider current technical and political progress in terms of the communication with CAV, Data content and important measures towards the Mobility Data Space that is relevant for the implementation of the proposed Future Mobility Data Exchange Concept. It is not to be expected that communication with CAV and the type of content to be exchanged will have a direct impact on the concept, but they should be taken into account in the overall consideration in the sense of implementing Use Case 3.

The described Measures towards the Mobility Data Space (see Section 5.4) do indeed have a direct influence on the acceptance and political weight of the concept, since these implement the regulatory foundation and, in parallel, the first comprehensive findings are being gathered in corresponding projects.

5.2 Communication with CAV

5.2.1 ETSI ITS-G5

As already described in section 3.2, the challenge of deploying C-ITS in real operation is addressed by two major initiatives. The Car 2 Car Communication Consortium is primarily concerned with vehicle-to-vehicle (V2V) aspects, whereas the C-ROADS platform focuses on vehicle-to-infrastructure and in particular infrastructure-to-vehicle applications. Such kind of more or less institutionalised cooperation is needed for C-ITS, since the radio interface – between vehicles as well as between vehicle and infrastructure – has to provide plug-and-play interoperability. A vehicle manufactured in one European country may be sold in another, used to drive into a third and then have to communicate with a roadside unit manufactured in a fourth. Hence, the communication specifications need to be uniform, at least European-wide. OEMs would certainly prefer even world-wide specifications, but it is known from other types of devices, standards and services that regional clusters like America, Europe and Asia are reality today, and they seem to be manageable.

Now even a European-wide specification is hard to achieve and continues to be hard to maintain. It must be noted that both type of technology 'carriers' – i.e. vehicles as well infrastructure – have their own lifecycles and deployment plans of new services or service evolution require aligned roadmaps on both sides of the radio channel. And of course, agreed innovation has to be backwards compatible or at least describe a suitable migration path.

Vehicle industry and infrastructure operators have meanwhile reacted on first concrete, real-world deployments going on by launching the required cooperation groups. This holds at least for C-ITS based on the ITS-G5 short-range radio channel, where both groups have established procedures to subsequently publish releases of 'specification profiles'. These specifications refer to the underlying standards but add the required profiling and additional specifications needed to actually turn this into a specification that allows implementation of interoperable services.

These specifications are now being cross-checked against each other in terms of compatibility, but also, they are assessed from the perspective whether one stakeholder group can confirm that receiving applications can be developed against the other's specification. It is a stated target that specifications by the end of 2020 should allow for a range of Day 1 Use Cases that can be deployed in a real-world, commercial environment. The expectation is that the Volkswagen group will extend its range of ITS-G5 enabled models and other OEMs will follow suit if this proves to be successful.

But it should also be noted that many OEMs have strongly announced they would not implement ITS-G5. Whether that means that they do not intend to implement any type of short-range, direct communication or whether it only means that they want to wait for Cellular V2X entering the market seems to vary. It can be definitely assumed that both strategies have at least some followers.

Sticking to traditional-style cellular communication only actually means in almost all cases that the communication is in essence mobile internet, and it has no deep embedding into the carrier network used – which is indeed this case in almost all cases a modern 3G/4G/5G cellular radio network. This type of communication is already well proven in commercial context and widely available, but it is limited in coverage, scalability, and real-time behaviour. The cellular coverage still has white spots (especially outside urban areas), intense communication patterns with many vehicles can quickly overload radio cell capacity and applications requiring second or below-second latency reach the limits of what is technical possible today. Nevertheless, many I2V Day 1 use cases are in the range of what is technical possible, e.g. road works warning. V2I data on the other hand can be provided via OEM or other fleet backends in near real-time, see section 3.3. Some applications actually do stretch the technical limits, e.g. AUDI operates Green-Light Optimal Speed Advice (GLOSA) services in some German cities, based only on the connectivity of the vehicle with the OEM backend.

The hope for Cellular V2X, as an alternative device-to-device (D2D) communication technology instead of ITS-G5, is mainly fed by the assumption that emerging technologies – in particular 5G, (section 5.3) combine short-range device-to-device and cellular technologies to create synergies. The D2D options allow services not limited to cell coverage – under certain conditions – and cellular coverage allows to combine these with backend services. It is worth noting that this type of symbiosis is also used for the first C-ITS enabled mass market vehicle using ITS-G5, where backend connectivity is used to provide the vehicle with the digital certificates needed for ITS-G5 communication.

The open question at this moment is certainly the future of "Hybrid C-ITS", i.e. the question whether it is feasible and sensible to try to transfer the communication patterns established for short-range radio D2D communications to vehicles that do not have the required radio equipment, but are connected to a backend (OEM or service provider) via mobile internet. Note that this question as such is totally independent of the radio access technology used, i.e. it is valid for the ITS-G5 environment in the same way as for the Cellular V2X environment.

There are indeed various aspects to consider regarding this question. Firstly, one would wonder whether such an approach is not actually duplicating existing information flows. Operators of vehicle fleets – be they OEMs or service providers – do already collect information relevant for vehicles from various platforms, including the National Access Points defined in the EU Delegated Regulations. These established feeds do contain content that is overlapping with Day 1 use cases of C-ITS, e.g. information about road works, traffic regulations, hazard warnings, etc. In some cases, the applications appear almost identical, e.g. Mercedes-Benz offers roadworks warning in the scope of short-term roadworks for some regular vehicle types in Hessen, based on GPS based positioning of the safety trailers used for closing lanes. The data is collected by the road operator in real-time (even for moving works like grass-cutting) and provided via the National Access Point to the Mercedes-Benz backend. The application for the driver is a warning when approaching the roadwork area, exactly as it would be the cases for the Road Works Warning C-ITS use case.

5.2.2 5G

As the last section already pointed at, the next (fifth) generation of cellular radio technology – denoted as "5G" – is expected to extend the technical options that cellular radio can offer for Cooperative, Connected and Automated Mobility (CCAM). It is worth noting that this is not – at least not only – referring to the usual 'next generation' expectations regarding better coverage, higher bandwidth, and less latency. Indeed, the promoters of 5G emphasize that 5G offers more than human communication and mobile internet, it actually is supposed to support vertical sectors by providing *"communications to help digitise the economy and contribute towards global digital transformation"* (source: The 5G Infrastructure Private Partnership). The mobile network – and its operators – would hence start taking an active role in these vertical sectors, where one is called "Automotive" and is expected to be one of the first to emerge for larger scale 5G deployment.

5G contains technical features that allow dedicating logical 'slices' of the network to specific verticals, hence virtually creating a dedicated cellular network for the respective applications. It also foresees network entities starting to take dedicated roles in the application domain for the vertical, e.g. domain functionality operated 'close' (in a communication sense, also but not primarily in a physical sense) to the individual vehicle according to an architecture called Multi Access Edge Computing (MEC), formerly also known as Mobile Edge Computing. This proximity enables low latency and high-performance applications, as they are expected to emerge from C-ITS services and will have increasingly challenging requirements in the scope of Infrastructure Support for Automated Driving (ISAD).

What is worth noting is that MEC application servers will presumably have to be operated by the Mobile Network Operator, i.e. the MNO is no longer simply offering 'communication channels' as a service but actually becoming an active partner in the Mobility/Traffic/Automotive eco system providing services.

This expected, disruptive change has significant impact on future stakeholder cooperation. We should recall that functional safety considerations of vehicles and infrastructure have traditionally been addressed mainly in isolation. CCAM scenarios challenge this approach, since the connected and cooperating vehicles and infrastructure more and more become components of a single, distributed system.

Also, system operation might increasingly become a cooperation effort. 5G architectures and envisaged high capacity scenarios require small cells and hence a high cell controller density. Rolling out dedicated infrastructure might raise prohibitive commercial challenges, which might be possible to mitigate if power, mounting and backbone communication infrastructures existing along motorways – usually financed, owned and operated by the road operator – could be re-used. Concrete analyses regarding aspects like legal context, liability and levels of service, business models ensuring mutual benefit, etc. are certainly still missing, but at least initial liaison contacts in new stakeholder constellations have been launched.

Currently, the Horizon 2020 research project ICT4CART addresses most of the aforementioned challenges and adopts a hybrid communication approach where all the major wireless technologies (in particular ITS-G5 and 5G) are integrated under a flexible network architecture.

5.3 Data Content

5.3.1 Spatial ITS Data

The TN-ITS Platform, established in 2013, evolved from work performed in several EU-funded projects dating back to 2004. The platform is concerned with the exchange of information on static road data, i.e. data that is more or less permanent in nature and, unlike dynamic road data, does not change frequently. Static road data includes for example speed limits, traffic signs, road classifications, road directions and vehicle restrictions.

Static data nevertheless occasionally changes, and as European countries use a variety of data formats, this data cannot easily be used in digital maps of service provides such as mapmakers. TN-ITS provides a harmonized framework for the provision and exchange of the relevant spatial ITS data in the form of a data chain structure and a common data exchange format.

The TN-ITS exchange framework enables a data chain for timely provision of information on changes in road attributes and other elements of the physical road network infrastructure, including public transport elements and geometry, for inclusion in digital maps for ITS applications. The framework comprises collection and maintenance of road network spatial data at road authorities in an adequate digital map infrastructure and using adequate procedures, extraction at regular intervals of information on related changes, publication of such changes as sets of updates, implementation of the updates by ITS map providers in their digital maps, and provision of updates of ITS maps to end-users at similar regular intervals. The framework builds the TN-ITS exchange specification, adequate methods for location referencing, quality control and feedback, a discovery service to find sets of updates, and on any further specifications or tools that may be developed.

The cornerstone of TN-ITS is the TN-ITS Specification, which will be transformed into a standard by the European Committee for Standardization (CEN): CEN TS 17268, and describes both which data and how this data is to be exchanged.

In addition to defining and maintaining the specification, the TN-ITS Platform furthermore provides guidelines, tools and services to support the implementation of the data chain, which is shown in Figure 8.

The first part of the data chain focuses on the Member States' authorities, who will maintain the road database and identify any changes in the data. These changes will then be transformed into the common data exchange format, the TN-ITS specification, which will subsequently be published by the Member State, through a TN-ITS interface, as an update.

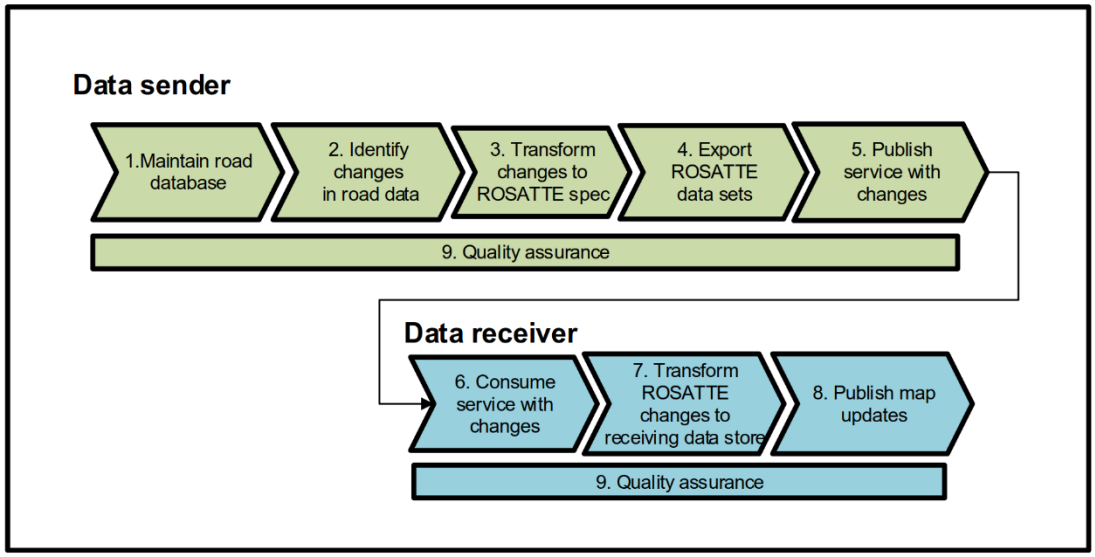

Figure 8: TN-ITS Generic Process Flow [TN-ITS, 2017]

Map makers and other parties will in the second part of the data chain then 'consume' this update: they incorporate the update into their own data and publish an updated map for consumers to use. The two parts of the data chain are furthermore complemented by quality assurance and a feedback loop between the data providers and data receivers.

The TN-ITS GO project in 15 EU members states aims to establish TN-ITS as the de facto methodology for road authorities to exchange map updates. This process enables data user to update their maps in a faster and more efficient way, which means the end-user gets much more up to date information and will be guided in more efficient and safer manner. The TN-ITS also supports HD Maps and Assistance systems like Intelligent Speed Assistance (ISA), as fresh and reliable maps are critical for these applications.

The TN-ITS service can bring great impact to the further development of Intelligent Transport Systems in the EU increasing the safety in road movements. Moreover, the TN-ITS service can close the gap between road authorities and map providers, which is very important for the deployment of CCAM and covered by DIRIZONS Use Case 1 [Malone et al., 2019]. Additionally, the new EU vehicle safety standards which are now in the final stages of being agreed, include a requirement for Intelligent Speed Assistance to be fitted as standard from 2022 (European Transport Safety Council, 2019 and Regulation (EC) 2019/2144). The TN-ITS service is under consideration to be a part of this new safety standard to further assist drivers to maintain their speed within the speed limits. Regarding the challenges of the TN-ITS implementation, it is noted that the quality of the service is strongly connected to the internal processes of the road authority.

5.3.2 ISAD

The environmental perception of automated vehicles is limited by the range and capability of onboard sensors. Road infrastructure operators already employ numerous traffic and environmental sensors and provide information that can be perceived by automated vehicles. In order to classify and harmonize the capabilities of a road infrastructure to support and guide automated vehicles, the EU research project INFRAMIX supported a simple classification scheme, similar to SAE levels for the automated vehicle capabilities. This project focused on the transition period, where both conventional and automated vehicles will share the roads. The main objective project was to design, upgrade, adapt and test both physical and digital elements of the road infrastructure to achieve a "hybrid" road infrastructure for future automated transport systems.

Amongst others the project developed and introduced 5 Infrastructure Support levels for Automated Driving (ISAD), which can be assigned to parts of the network in order to give automated vehicles and their operators guidance on the “readiness” of the road network for the coming highway automation era.

ISAD Levels are meant to describe road or motorway sections rather than whole road networks. This reflects common practice of infrastructure deployment: Traffic control systems (sensors and VMS) are usually deployed on motorway sections where traffic often reaches the capacity limit (bottlenecks), whereas other motorway sections need no fixed installations of traffic control systems because traffic flow is rarely disrupted.

This shall build the basic capability to extend the electronic horizon, based on a combination of data from vehicles and the infrastructure, to contain dynamic information about traffic flow (e.g. speed and density of vehicles, if possible in certain situation even separately for trucks and private cars) as a basis for individualized speed and lane recommendations. Estimation tools (to be developed) for extending the electronic horizon will receive info provided by connected vehicles and will fuse them with measurements stemming from a minimum number (necessary for flow observability) of spot sensor measurements; and will deliver in real-time reliable estimates of traffic density and traffic flow by segment and even by lane, as well as travel times and incident detection. The tools will provide a necessary tool for real-time traffic control tasks with various requirements regarding the estimation granularity (e.g. estimation per lane), the estimated variables or the underlying architecture [Lytrivis, P., et al., 2018].

Additional research needs to be carried out and a joint approach between telecom and vehicle industry as well as cross-border pilot projects and the adaptation of road traffic rules in Member States can all support to reach a consensus in this field. The FFG project Lex2Vehicle that started in September 2020 will follow this up, as described in the following section.

Traffic regulations describe the concrete constraints under which a vehicle is allowed to move on the road, covering aspects like speed, allowed vehicle characteristics like width, height, weight and permissible movements like lane change, right/left turn, overtaking, etc. Traffic regulations apply independent of the automation level, so they can provide an important input to the ODD assessment.

Traffic regulations are implemented traditionally in the ISAD level E world via “road signs” placed on, above or near the road, where the term sign includes road markings. Vehicles detect traffic regulations via sensors (e.g. cameras), but the detection probability may be limited in difficult environments (adverse weather conditions, sign “forest” in urban scenarios), hence the currently valid traffic regulations at the same time form an important part of the ISAD content. In future Level 5 scenarios independent of traditional visualisation means more dynamic traffic regulations become possible – e.g. Urban Vehicle Access Regulation (UVAR) based on certain vehicle criteria that only apply if certain conditions are met – which would make traffic regulations as an element of ISAD mandatory.

Elaboration of ODD and ISAD should be performed collectively in a pre-competitive environment between automotive and infrastructure sectors. ISAD could provide important elements for ODD definitions, regarding digital infrastructure (e.g. availability of electronic traffic regulation) as well as physical infrastructure (e.g. about road marking quality or standardised road layouts in roadworks).

5.3.3 Digital Traffic Regulations

Regardless of how quickly highly automated vehicles will become established in Europe, in the long term mixed traffic with human road users and automated vehicles will dominate the road scene. In order to ensure the safety and efficiency of transport in the long term, road traffic legislation is needed that takes account of both human road users and automated vehicles. The legally standardised traffic rules thus need to be transformed and translated into codes suitable for automated driving systems; conversely, the legal regulations need to be adapted to take account of the special features of automated driving in road traffic law.

Lex2Vehicle that runs 18 months started in September 2020 will therefore cover the following: from the mere digital provision of traffic law instructions for automated vehicles to a combination of road traffic law as well as technical conceptualisation and standardisation, which in the age of digitalisation will equally meet the requirements of mixed operation. Dedicated traffic law orders for automated vehicles in the context of infrastructure-side support of automated driving (ISAD) represent an essential partial aspect in this context.

Within the EU, road traffic law is primarily regulated by the member states and, despite the commonly underlying international Vienna Convention on Road Traffic, there are sometimes considerable differences. On the other hand, there are technical standards and norms for which (not only in the field of automated driving) Europe-wide validity is a basic requirement. In this area of conflict, it is now necessary to develop content-related, legal, technical and organisational framework conditions and structures which continue to allow for national peculiarities while at the same time ensuring that the legal requirements for human road users and the unambiguousness of automated vehicles are comprehensible throughout Europe. For both groups, it must be possible, even after crossing the border, to behave in accordance with the rules in the road traffic of the destination country without any special effort.

Special attention must be paid to existing standardisation initiatives and their consideration. These include, for example, the CEF Programme Support Action for DATEX II and TN-ITS, in which regulations ordered by the transport authorities are the subject of standardisation. In addition, there are also traffic restrictions ordered by the traffic authorities as part of C-ITS messages within the framework of the C-Roads Infrastructure Deployment. With potentially closer coupling of traffic and connectivity in the future (e.g. 5G technology), the portfolio of standards to be considered (ETSI, IEEE, ISO, 3GPP, etc.) will grow significantly.

Due to the thematic scope, it will not be possible to cover all relevant aspects conclusively. Therefore, the project's aim is to show a way forward in the form of a draft programme, so that road traffic law in Germany, Austria, Switzerland and potentially beyond arrives semantically consistent at human road users and automated vehicles.

5.4 Towards a Mobility Data Space

5.4.1 Stronger NAPs in Future

On 19 February 2020, the Commission adopted the European Strategy for data, which provides in particular for the establishment of EU-wide common, interoperable data spaces in strategic sectors including a Common European mobility data space (MDS).

The MDS is expected to facilitate access, pooling and sharing of data from existing and future transport and mobility databases. Concretely, such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of common rules developed for the space.

The spaces will include:

- the deployment of data-sharing tools and platforms;
- the creation of data governance frameworks;
- improving the availability, quality and interoperability of data – both in domain-specific settings and across sectors.

A concept paper of [DG Move, 2020] states that in addition to the review of the ITS Directive and its Delegated Regulations which will further contribute to data availability, reuse and interoperability, and in addition to other transport related actions, the creation of this MDS includes the establishment of a stronger coordination mechanism to federate the NAPs established under the ITS Directive through an EU-wide CEF Programme Support Action (PSA).

Several Delegated Regulations adopted under the ITS Directive aim at improving the accessibility of ITS travel and traffic data through the creation of NAPs.

In the framework of the Directive, further legislation related to the accessibility of transport data (e.g. urban access regulations, recharging points, vehicle data etc.) and possibly extending the geographical coverage of the specifications is being prepared, in line with the updated working programme of the ITS Directive adopted in December 2018. This would reinforce the need for coordinated actions at Commission and Member States' level.

To support the implementation of these legislations and deploy NAPs many actions have been launched at EU and Member State levels, i.e.

- A NAP/NB harmonisation group created at the initiative of several Member States to start working on common issues related to the implementation of the Delegated Regulations.
- Monitoring of the deployment of the NAPs (CEF-funded project EU-EIP).
- Defining metadata and quality requirements for data stored on NAPs (Member State activities and CEF-funded project EU-EIP).
- CEF programme support actions (PSAs)
    - To define common tools for the exchange of data like DATEX II for dynamic data (-> end 2020), TN-ITS GO for static data (-> end 2021) and DATA4PT for Transmodel, NeTex and SIRI (public transport) (->End 2023).
    - To implement Regulation 2017/1926 on multimodal travel information services: individual PSAs for 17 Member States (phasing out->2021)
    - For ITS Architecture (FRAME NEXT) (-> June 2021).
    - For Data collection (IDACS) related to recharging/refuelling points for alternative fuels (->End 2021).
- Several Member States created a Data Task Force together with the industry (vehicle manufacturers, digital maps providers, service providers) to facilitate access to vehicle data, for the creation and dissemination of road safety-related traffic information.

CEF PSAs and support to standardisation have been first answers to help Member States tackling some of these challenges.

However, many of these actions, such as CEF PSAs, have a limited lifetime, are not really coordinated, and currently there is no place where Member States experts, NAPs operators and National Bodies/competent authorities can concretely work together on common issues related to the development, operation and evolution of NAPs for the implementation of the ITS and its further contribution to the Common European mobility data space.

Moreover, new challenges such as data collection activities and negotiations with private data providers and/or global players would benefit from being addressed jointly.

There is a need to:

- Clearly empower NAPs as the backbone for ITS data infrastructure, to which all current and future activities should be linked, also in view of the new Working Programme of the ITS Directive. In particular, strong coordination with the current PSAs is expected for their remaining duration (without changing their current setting/organisation), and
- Facilitate national & EU wide operational co-ordination for the implementation of the European specifications through:
    - Facilitating the monitoring of the availability and accessibility of data;
    - Coordinating the development and evolution of the NAPs in order to assure real compatibility and interoperability of the features;
    - Designing and developing common tools related to data accessibility and exchange (standards, profiles, metadata, definitions, quality requirements etc.), to be used on a voluntary basis by Member States in addition to the legal specifications for the implementation of the delegated regulations;
    - Implementing a process driven approach by identifying common needs and developing common tools, which can also be taken into account by the EC and the related Member States expert groups when considering possible amendments/adaptation of the specifications;
    - Addressing jointly the challenges posed by global players in the field on issues related for example to compliance with the legislation, licencing and standardisation;
    - Planning and coordinating data collection/creation initiatives, with prioritisation given to datasets for essential services. Intelligent Speed Assistance, CCAM or MaaS could be good candidates for such services;
    - Planning and coordinating promotional activities within the transport sector to increase the exposure of NAPs and promote their role as backbone of the ITS infrastructure.

Therefore, the Commission will launch in Q4 2020 a multi-annual EU wide CEF Programme Support Action (PSA) to address these needs via a stronger coordination mechanism to federate the NAPs.

5.4.2 EU Data Spaces

On 19th February 2020, the European Commission published the Communication COM 2020/66, which presents the Commission's European Data Strategy. This strategy explicitly promotes the creation of Europe-wide data spaces in various sectors, including mobility:

"A Common European Mobility Data Space to make Europe a leader in the development of an intelligent transport system, including networked vehicles and other transport modes. Such a data space will facilitate the access, aggregation and sharing of data from existing and future transport and mobility databases; [...] "

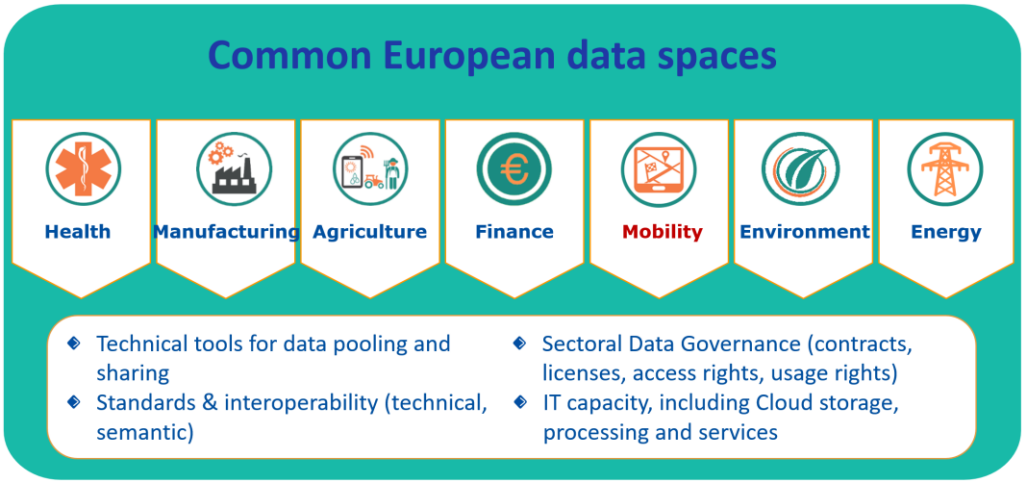

Figure 9: Common EU Data Spaces presentation, Digital Transport and Logistics Forum, 07/05/2020

As a prerequisite for the standardised handling of mobility data in Europe, the European Commission has requested the creation of National Access Points (NAPs). The legal basis for this is the ITS Directive 2010/40/EU. The Member States are thus obliged to provide a platform on which at least the metadata description of the country's mobility data can be published. In addition to the ITS Directive, various delegated regulations define the obligation of data providers to publish mobility data via the NAP.

While the legislative initiatives listed above oblige private sector companies to provide data on a large scale, companies see this as a potential risk to business secrets and customer data. Sharing sensitive data in a secure data space such as the Mobility Data Space would help to address this. This would give data providers confidence that the data they provide is only used in accordance with defined usage and licensing conditions and that the usage is controlled and verified by the data provider.

A further obstacle to the use of the European NAPs for internationally operating companies such as vehicle manufacturers and navigation service providers is the still large number of platforms in Europe. Around 30 NAPs, some of which are implemented in significantly different ways, have to be served in this way in order to be able to offer services internationally. Further harmonisation, or rather the networking of the European NAPs with Mobility Data Space concepts, would be welcome from many sides.

This could be a first step towards a common European Mobility Data Space, as envisaged in the European data strategy of the EU Commission COM 2020/66. Overall, the Mobility Data Space has the necessary concepts to facilitate "the access, consolidation and sharing of data from existing and future transport and mobility databases" with this data space.

5.4.3 Launch of the Mobility Data Space

The German mFund research project “Mobility Data Space” one of the first project, which is aiming for the introduction of a data space that, in addition to secure exchange, enables the development of real-time traffic data and sensitive mobility data, as well as networking existing data platforms. In this way, comprehensive mobility data can be made available on a (inter-) national level in the future.

Based on the distributed system architecture of the International Data Spaces Association e. V., the Mobility Data Space provides an ecosystem in which data providers can define and control the conditions under which their data is used by other players. This shall create data sovereignty and trust and shall give users certainty about the origin and quality of the data. By making public and private sector data interoperable via regional and national data platforms, the Mobility Data Space becomes a digital distribution channel for data-driven business models and unfolds completely new possibilities for data access, linking and utilization.

Within the Mobility Data Space project the mentioned concept (e.g. the use of IDS connectors, see chapter 4) will be applied for the German Mobility Marketplace (MDM) the German NAP, driven by the Federal Highway Research Institute (BASt) in conjunction with regional platforms driven by local authorities and private fleet operators. Further details can be found in [Pretzsch et. al, 2020]. Through this, new municipal traffic data and nationwide mobility data will be made available for secure and sovereign processing on the platforms. The municipal platforms will be linked to the MDM to make regional data available and usable on a national level as well.

For this purpose, both will be extended by a secure and protected execution environment for services or data apps in which mobility data can be provided and refined under guarantee of data sovereignty. In this way, more sensitive mobility data such as Floating Car Data (FCD) will be usable for the first time. The MDM and the municipal platforms will be linked to form a distributed data space, thus forming a federal mobility data ecosystem. Based on this, complex real-time use cases will contribute to the reduction of environmental pollution, traffic liquefaction and multimodal commuter notification. For further information reference can be made to [Pretzsch et. al, 2020].

In particular regarding the exchange of real-time data it is worth noting that the project will give first insights what role latencies play within the secure data space.

Although application in the mobility domain is promising, it is still in an early phase. The IDS concept however has been around for a while, and the IDSA is a well-established association. The example of the Smart Connected Supplier Network provides more detail about an IDS implementation in context of high-tech manufacturing industry. It establishes interoperability between existing platforms serving different manufacturing companies, and thereby linking a large sector. This implementation is well beyond the project phase. It has established an operational legal entity, a foundation, to manage the standard and the implementations. It is currently being considered for a Europe-wide deployment in the manufacturing industry [Helmer], [Blankendaal et. al], [SCSN]. Reference can also be made to D6.1 Business Model Options Chapter 4.4, [Berkers et. al, 2020].

In Germany it appears, the question of whether or not to introduce the MDA no longer exists. According to a report, a first pilot project will be launched in spring 2021. Chancellor Angela Merkel is urging BMW, Daimler and VW to share their data treasures with other transport providers – at least for a fee. New products such as intelligent navigation services or networked mobility services are to be developed [Handelsblatt, 2020].

5.4.4 Federated and Open EU Data Infrastructure

Closely linked to Common European Data Spaces is the initiative of introducing a European Federated and Open Data Infrastructure. With GAIA-X, representatives from politics, business and science from France and Germany, together with other European partners, created a proposal for the next generation of a data infrastructure for Europe: “a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation. This project is the cradle of an open, transparent digital ecosystem, where data and services can be made available, collated and shared in an environment of trust.”

GAIA-X is a European project with the aim to develop common requirements for a European data infrastructure. Openness, transparency and the ability to connect to other European countries are central to GAIA-X. Representatives from seven European countries are currently involved in the project. Other European partners are also invited to join the project and to contribute to its development. Many dialogues are already underway and will be further intensified. Furthermore, GAIA-X is in continuous exchange with the European Commission.

Within project, the foundations for a federated, open data infrastructure based on European values shall be developed. It will connect centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. The resulting federated form of data infrastructure strengthens the ability to both access and share data securely and confidently.

GAIA-X will align network and interconnection providers, Cloud Solution Providers (CSP), High Performance Computing (HPC) as well as sector specific clouds and edge systems. Mechanisms are developed to find, combine and connect services from participating providers in order to enable a user-friendly infrastructure ecosystem. Hence, the project will identify the minimum technical requirements and services necessary to operate the federated GAIA-X Ecosystem.

Technical implementation of these Federation Services will focus on the following areas:

- the implementation of secure federated identity and trust mechanisms (security and privacy by design);
- sovereign data services which ensure the identity of source and receiver of data and which ensure the access and usage rights towards the data;
- easy access to the available providers, nodes and services. Data will be provided through federated catalogues;
- the integration of existing standards to ensure interoperability and portability across infrastructure, applications and data;
- the establishment of a compliance framework and Certification and Accreditation services; and
- the contribution of a modular compilation of open source software and standards to support providers in delivering a secure, federated and interoperable infrastructure.

6 Conclusions & Recommendations

Mobility Data Exchange Concept as blueprint for the Common European MDS

In terms of technical implementation, be it in Option 1 or 2 presented in Section 4.4, the IDS concept offers a vast potential in accessing data sources and integrating them into the emerging intelligent network via standardised connectors while maintaining data sovereignty. It will be able to include e.g. additional data providers and specialised service providers, who can generate enormous benefits by integrating or merging additional data types and sources. Existing cooperation between companies for the exchange of industrial data has already proven. Reference can be made to [SCSN]. Initial projects are underway in the mobility sector, in particular the Mobility Data Space project (see Section 5.4.1) that will provide first insights in the implementation and the exchange of mobility data in an secure an sovereign exchange environment.

The solution is provided by the Mobility Data Exchange Concept, which represents an open mobility data ecosystem where data providers can define and control the conditions under which their data may be used and exploited by other actors. This creates data sovereignty and trust for the data providers as well as certainty about the origin and quality of the data for the data user.

Based on the IDS' technical capabilities for secure and sovereign data exchange, the Mobility Data Exchange Concept could provide an international ecosystem for:

- the connection of relevant stakeholders like OEMs and service providers as well as local, regional, and national data sources and platforms
- the provision of comprehensive mobility data at a national and international level:
    - real-time traffic data (e.g. SRTI, sensor data, LSA switching times), if the latency allows,
    - sensitive mobility data (e.g. vehicle and smartphone generated data, mobile phone movement patterns),
    - regulations (e.g. static and dynamic regulations like speed limits and access regulations),
    - map-based data to enable HD-Maps (e.g. lane model including speed limits, parking spaces and service areas).
- new business opportunities and data-driven business models:
    - developers: data apps for mobility services and Applications including distribution via a data AppStore,
    - IT service providers: hosting of components and data apps in cloud environments and related consulting services,
    - end users: benefits by encouraging the development of innovative mobility applications and services through the wide availability of mobility data sources.
- the facilitation of CCAM due to the fact that all stakeholders can exchange mobility data securely and according to their requirements.

From a political perspective, water has already reached the mills. The EU wants to create Europe-wide data spaces in various sectors, including mobility. Therefore, the role of the NAPs needs to be strengthened, which is planned following a concept paper of [DG Move, 2020]. It states that in addition to the review of the ITS Directive and its Delegated Regulations the creation of this MDS includes the establishment of a stronger coordination mechanism to federate the NAPs established under the ITS Directive through a EU-wide CEF PSA.

In Germany the automotive industry is urged participate in a MDS and to share their data with other transport providers.

Learn from national IDS pilots

With regard to the Mobility Data Space, the MDM has not yet been implemented in an IDS-compliant manner. However, at the time of writing this document, the tendering process for an MDM upgrade is ongoing. The metadata directory will be machine-readable, a connector will be implemented, and the components Mobility Vocabulary Provider, Identity Provider, and Clearing House will be added, as well as a Data App environment. The operation of the Mobility Data Space Ecosystem is planned for 2022. The approach is an innovative and promising concept. Due to the fact that there is no real implementation and no evaluation of the system's ability to perform the intended task yet, the requirements and the feasibility of the IDS concept should be evaluated and an information exchange with the project should be arranged. Hence, as a first step and short term recommendation is therefore to learn from this national pilot and start similar activities if applicable.

Combine the IDS Concept with the DTF PoC

Since the IDS, taking into account data security and data sovereignty, it seems to have the potential to support trusted smart networks, it should be further examined whether data exchange with regard to CCAM is a feasible option. The current European dataspaces activities underpin this thought. Therefore, as a second step, a pilot project similar to the PoC of the Data Task Force should be considered here and should be discussed with the OEMs and Service Providers soon. On 15th June 2020 ACEA published a discussion paper [ACEA, 2020]. It conveys messages and think paths from the vehicle manufacturers in view of a dialogue with the road authorities, road operators and cities regarding physical and digital infrastructure requirements, harmonised traffics rules and regulations, specifics for urban mobility and the role of road authorities. In terms of digital requirements, they addressed in general the 3 DIRIZON use cases. The requirements do not deviate from the previous findings in DIRIZON. The paper initially seems to focus on direct communication between digital infrastructure and CAV. A data-exchange via backbone between i.e. road authorities NAPs, service providers and OEMs is not addressed i.e. to exchange the required data, to cover the increasing data volume or to create alternative data-exchange channels. In order to initiate a Hybrid Full European Scenario (see [Berkers et al., 2020], Section 5.4.3) and develop a long-term MDS strategy, it is necessary to use the current momentum and involve the automotive industry at the earliest time.

7 Sources

[Dizdarevic et. al, 2019] Jasenka Dizdarević, Francisco Carpio, Admela Jukan, and Xavi Masip-Bruin. 2019. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Comp ut. Surv. 1, 1 (February 2019), 30 pages. https://doi.org/0000001.0000001

[DG MOVE, 2020] DG MOVE, Coordination mechanism to federate the National Access Points established under the ITS Directive, June 2020

[DTF, 2020] Data for Road Safety moves from 'Proof of Concept' to long term deployment, Press release, December 2020

[EU EIP, 2020] Monitoring and Harmonisation of National Access Points

[Lytrivis, P., et al., 2018] P. Lytrivis, E Papanikolaou, A. Amditis, M. Dirnwober, A. Froetscher, R. Protzmann, W. Rom and A. Kerschbaumer, "Advances in Road Infrastructure, both Physical and Digital, for Mixed Vehicle Traffic Flows", Proceedings of the 7th Transport Research Area 2018, April 2018.

[IDS-RAM, 2019] B. Otto et al., International Data Spaces Association, Reference Architecture Model, Version 3.0 April 2019

[ISO 19468:2019] ISO/TS 19468:2019 Intelligent transport systems — Data interfaces between centres for transport information and control systems — Platform independent model specifications for data exchange protocols for transport information and control systems

[Pretzsch et. al, 2020] S. Pretzsch, H. Drees, L. Rittershaus, Mobility Data Spaces – Secure Data Space for the Sovereign and Cross-Platform Utilisation of Mobility Data, Mobility Data Space Project, Fraunhofer IVI, March, 2020

[Shibata, 2017] Shibata, J. "Digital Infrastructure for Automated Driving" 2017. Available at: https://connectedautomateddriving.eu/wpcontent/uploads/2017/08/Final-20170621-SIS37-ITS-European-Congress-Jun-Shibata.pdf (accessed April 25, 2019).

[Helmer] S. Helmer, Digitising data streams between companies

[Blankendaal et. al] J. Blankendaal et. al, Fieldlab The Smart Connected Supplier Network

[SCSN] Smart connected supplier network

[ACEA, 2020] ACEA, roads of the future for automated driving, June, 2020

[Berkers et. al, 2020] F. Berkers et al., "Final proposal for business models options for data-exchange in context of CAD", Deliverable 6.1, DIRIZON project, October 2020.

[Malone et. al, 2019] Malone, K. et al., "Digitalisation and Automation: Implications for use cases, Identification of Stakeholders and Data Needs and Requirements", Deliverable D3.1., DIRIZON project, January, 2020.

[INFRAMIX, 2018] Lyrtrivis, P. et al., "Requirements Catalogue from the Status Quo Analysis", Deliverable 2.1 of INFRAMIX, Grant Agreement Number 723016, February, 2018.

[Coordinated Meta Data Catalogue, 2019] P. Lubrich, L. Hendriks, J. Jaderberg, C. Lüpges, B. Witsch, et al, EU EIP SA4.6, November 2019

[TN-ITS, 2017] TN-ITS, Reading instructions Data-Receiver, 2017

[Handelsblatt, 2020] D. Delhaes, „Merkel drängt Autokonzerne: BMW, Daimler und VW sollen Datenschatz teilen", Handelsblatt, 28th Oktober 2020

8 Appendix: Technical Descriptions

8.1 Design and Exchange Patterns

8.1.1 Abstract Model

Model driven approach is chosen to describe Exchange: this leads to describe exchange systems by means of abstract model which are named Platform Independent Model: To be most flexible, FEPs and EPs are defined in a Platform Independent Model (PIM), i.e. technology independent. Thus, the specific technology in which FEPs and EPs are embedded at the end (e.g. http/get XML, WebServices) are part of the Platform Specific Model (PSM) and not described in this chapter.

Modelling of exchange features is done by describing interaction among systems and subsystems which are described as Exchange Patterns, those interactions implements system capabilities as features which fulfils exchange requirements requested by specific Business Scenarios which are used to specify specific use of Exchange.

Since simple data exchange process is no longer sufficient for resolving all business needs, this Technical Specification encompasses more business functions as the stakeholders consolidate their systems and look at new ways to address the requests they encounter with the tools they already know and have in place.

8.1.2 Exchange Pattern (EP) and Functional Exchange Profile (FEP)

8.1.2.1 Overview

In [ISO 19468:2019], an **Exchange Pattern (EP)** is defined as “the basic exchange architecture template, described by UML communication diagrams, which identifies the actors in the exchange framework and the available interactions among them, which enable data exchange functionalities as a set of exchange features”.

Exchange patterns interactions can be described by means of UML sequence diagrams and state machine diagrams, in a way that messages triggering conditions are fully identified and defined as well as any state update based on the subsequent interaction, i.e. exchanged messages and interaction derived conditions.

In [ISO 19468:2019], a **Functional Exchange Profile (FEP)** is defined as a “selection of data exchange features for a particular business scenario”, with business scenario being a “high level description of the interactions that can exist within a system being analysed or between the system and external entities (called actors) in terms of business functions”.

Requirements may vary depending on data exchange application i.e. Use Cases to be fulfilled, so there could be many reasons to consider or not any requirement based both on the gathering of data at Supplier System and the usage of Delivered data in the Client.

FEPs are identified to ensure interoperable services with the restriction of determining one FEP per business scenario for a specific exchange pattern, which are abstract model of available technical platforms. One business scenario can be supported by more then one FEP which can be enabled by several EP.

Requirements address the following items:

- Information provision,
- Communications,
- Security,

- Financial aspects.

Exchange is defined through Features which implement the Information Exchange and fulfils Data Exchange requirements.

Depending on many possible Exchange Platforms considered for implementation, a subset of features and relative requirements are possible to be implemented. To fulfil a set of requirements many Platforms are possible, but to be interoperable client and supplier shall implement the same platform with the same pattern. Allowing a wide variety of possible Exchange Patterns, the best suitable for an application may be chosen, according to requirements which fulfilment is granted by the selected Exchange Pattern.

Based on the requirements of a specific Business Scenario, a set of appropriate exchange features have to be combined into a Functional Exchange Profile.

The following schema represent the domains of PIM and PSM introducing Exchange Pattern EP and Functional Exchange Profile FEP.

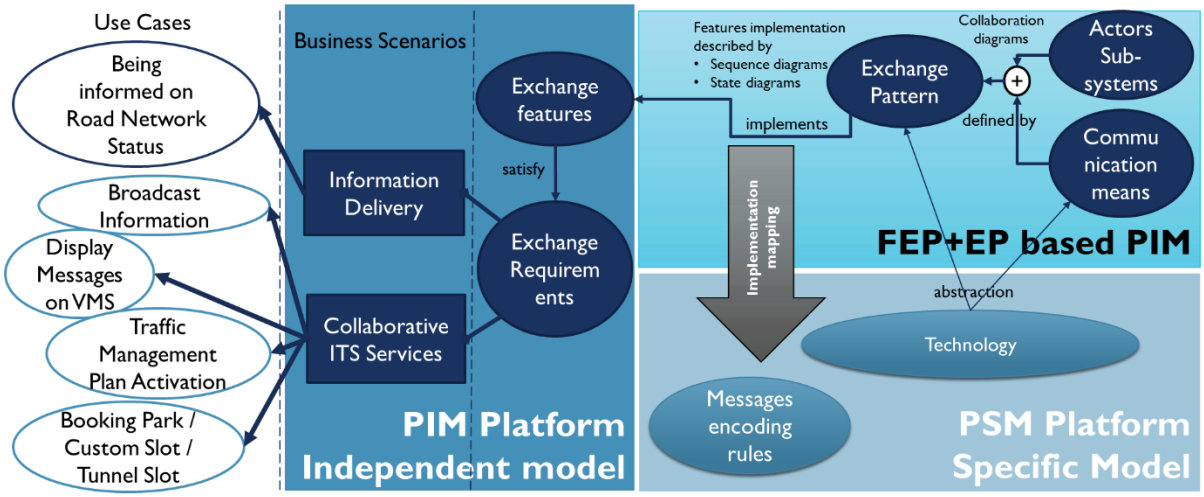

Figure 10: Platform independent and platform specific model
[Source: http://docs.datex2.eu]

[ISO 19468:2019] describes the following FEP/EP on PIM level:

- Snapshot Pull
- Snapshot Push
- Simple Push
- Stateful Push

8.1.2.2 Snapshot Pull

A supplier exchange system provides a mechanism to retrieve currently available and valid data (i.e. a snapshot of information) from an action taken at client side, which will invoke this specific mechanism offered by the supplier.

A snapshot pull supplier exchange system realises a snapshot pull supplier interface which provides a method which implements the snapshot pull mechanism. A snapshot pull client exchange system realises a snapshot pull client interface which invokes the "pullSnapshotData" method provided by the snapshot pull supplier interface to retrieve snapshot data.

In a typical FEP+EP framework, the client “pulls” messages from the supplier. In the pull request, the client delivers no information to the supplier. In return, the supplier delivers a "MessageContainer" information which includes “ExchangeInformation”. The client takes the initiative to retrieve the data based on application level requirements which determine the needed exchange operating mode (e.g. on occurrence, condition triggered or periodic).

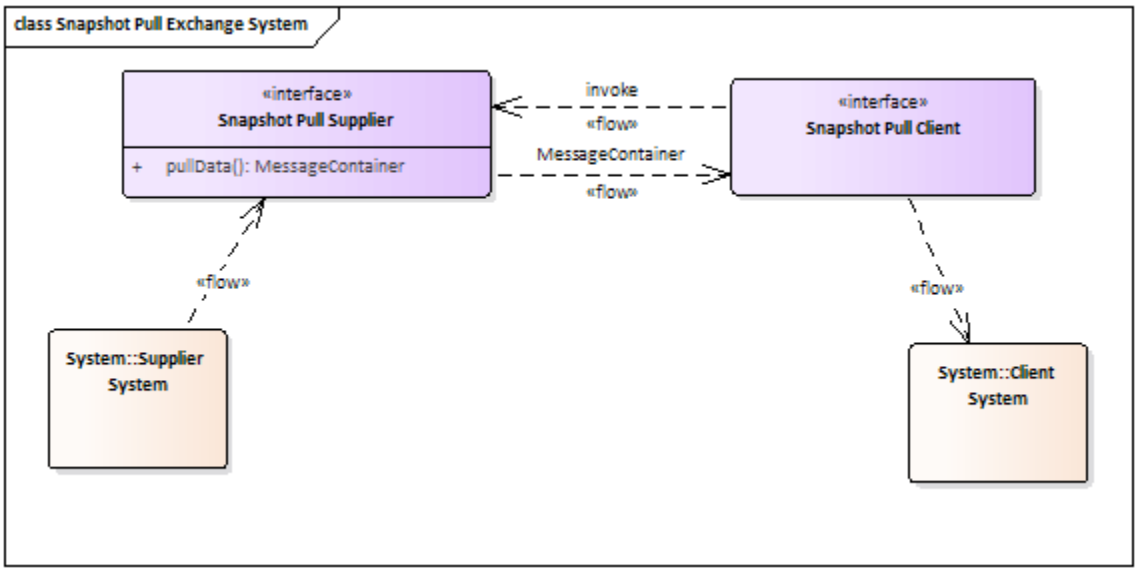

Figure 11: Snapshot Pull, Source: http://docs.datex2.eu

8.1.2.3 Snapshot Push

A client provides a mechanism to receive data from action taken at a supplier site invoking specific resources / methods offered by the client. The snapshot push client provides a mechanism to the snapshot push supplier to push currently available data, also called “snapshot” of information, i.e. current information at supplier system or last retrieved information for sampled data.

A snapshot push Client exchange system realises a snapshot push client interface which provides a putSnapshotData method. A snapshot push supplier exchange system realises a snapshot push Supplier interface which invokes the putSnapshotData Method provided by the snapshot push Client interface to deliver snapshot data.

In a typical FEP+EP framework, the supplier “pushes” messages to the client. The client acknowledges the received message by a return information to the supplier. This return information is coded as “ExchangeInformation”.

The supplier takes the initiative to deliver the data based on application level requirements which determine the needed exchange operating mode (e.g. on occurrence or periodic).

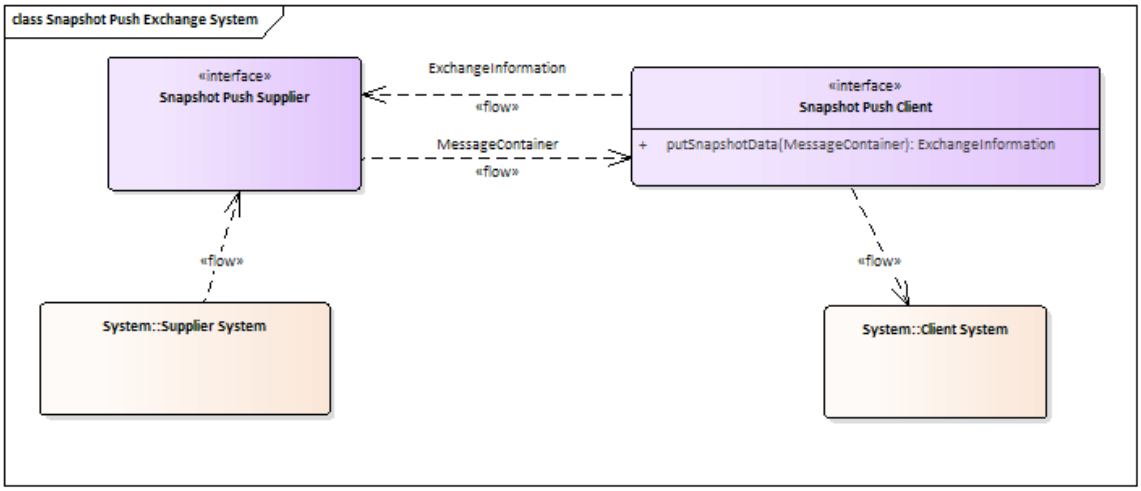

Figure 12: Snapshot Push, Source: [http://docs.datex2.eu]

8.1.2.4 Simple Push

A client provides a mechanism to receive data from action taken at a supplier site, invoking specific resources / methods offered by the client. Therefore, the supplier logically “pushes” messages to the client. The client shall acknowledge what is received by a return exchange information to the supplier. This exchange information return message is available to bring information back from the client to the supplier, such as SessionId, failure, success, snapshot synchronisation request. Return message information is logically described in this PIM, while implementation will be defined at PSM level.

A client provides two mechanisms to the simple push supplier to push data:

- a "push" method is intended to push "available data" which had not yet been delivered to the client, based on some supplier side logic and status,
- a "snapshot push" is intended to push "all currently available data", also called “snapshot” of information, i.e. current information at supplier system or last retrieved information for sampled data. This snapshot push method is used for synchronisation purposes among client and supplier.

In addition to these push data delivery methods the simple push client also provides a "keep alive" method to implement link monitoring capabilities among client and supplier, the keep alive method is used from the supplier to advise the client when no information updates are to be delivered, so the supplier delivers a "keep alive" message to check and enable the client to check that exchange systems and network connection are available, despite the supplier doesn't need to exchange payload content. "Keep Alive” messages are delivered by the supplier to the client, according a time interval which is defined among them.

In a typical FEP+EP framework the supplier “pushes” messages to the client. The client acknowledges the received message by a return information to the supplier. This return information shall be coded as “ExchangeInformation”.

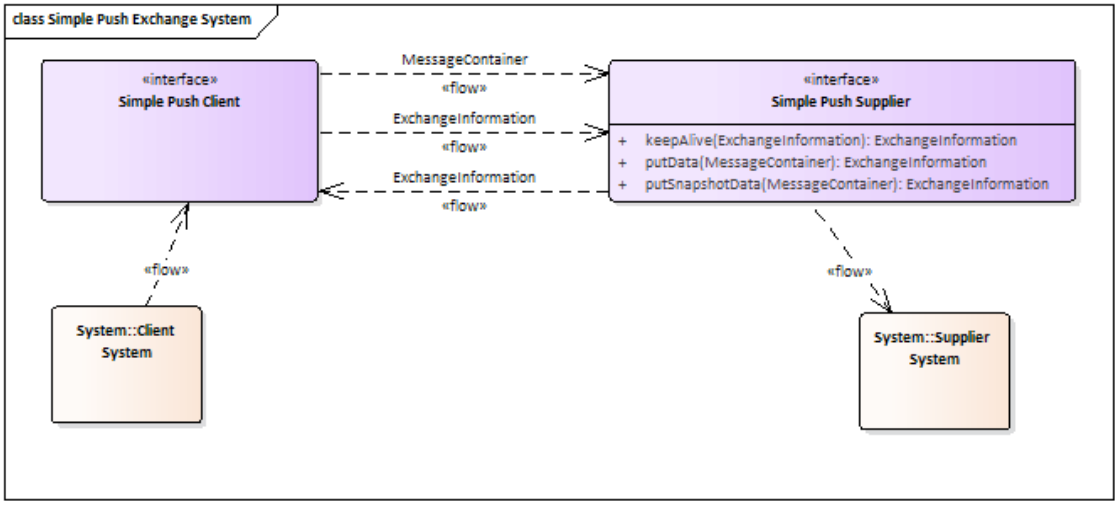

Figure 13: Simple Push, Source: [http://docs.datex2.eu]

The Supplier takes the initiative to push the data under the following conditions:

On Occurrence Push: as soon as an information is updated at the Supplier Systems, this condition triggers the Supplier to send push data to align to the Client to update the Client System as soon as possible after this update.

Periodic Push: at predefined time interval the Suppliers start an exchange based on Client and Supplier agreement (subscription contract)

A Snapshot Synchronisation with all the currently available content snapshot in case a snapshot alignment feature is needed or requested by client.

Response to a Snapshot Synchronisation request: one Snapshot alignment can also be acknowledged to the client for internal system need / maintenance / debug, it may be requested by the Client via any Return Messages, i.e. wrapped in returned Exchange Information.

8.1.2.5 Stateful Push

A client provides a mechanism to receive data from an action taken at the supplier site invoking specific resources / methods offered by the client. Therefore, the supplier logically “pushes” messages to the client. The client shall acknowledge what is received by a return exchange information to the supplier. This exchange information return message is available to bring information back from the client to the supplier, such as SessionId, failure, success, snapshot synchronisation request. Return message information is logically described in this PIM, while implementation will be defined at PSM level.

As in "Simple Push", the "Stateful Push" client provides two mechanism to the "Stateful Push" supplier to push data:

- a "push" method is intended to push "available data" which had not yet been delivered to the client, based on some supplier side logic and status,
- a "snapshot push" is intended to push "all currently available data", also called “snapshot” of information, i.e. current information at supplier system or last retrieved information for sampled data. This "snapshot push" method is used for synchronisation purposes among client and supplier.

In addition to these push data delivery methods the simple push client also provides a "keep alive" method to implement link monitoring capabilities among client and supplier, the keep alive method is used from the supplier to advise the client when no information updates are to be delivered, so the supplier delivers a "keep alive" message to check and enable the client to check that exchange systems and network connection are available, despite the supplier doesn't need to exchange payload content. "Keep Alive" messages are delivered by the supplier to the client, according a time interval which is defined among them.

"Stateful Push" session management methods are available to implement session management features; such methods, namely openSession and closeSession usage which are used to define dynamic exchange information context to enable session management exchange features.

In a typical FEP+EP framework the supplier “pushes” messages to the client. The client shall acknowledge the received message by a return information to the supplier. This return information shall be coded as “ExchangeInformation”.

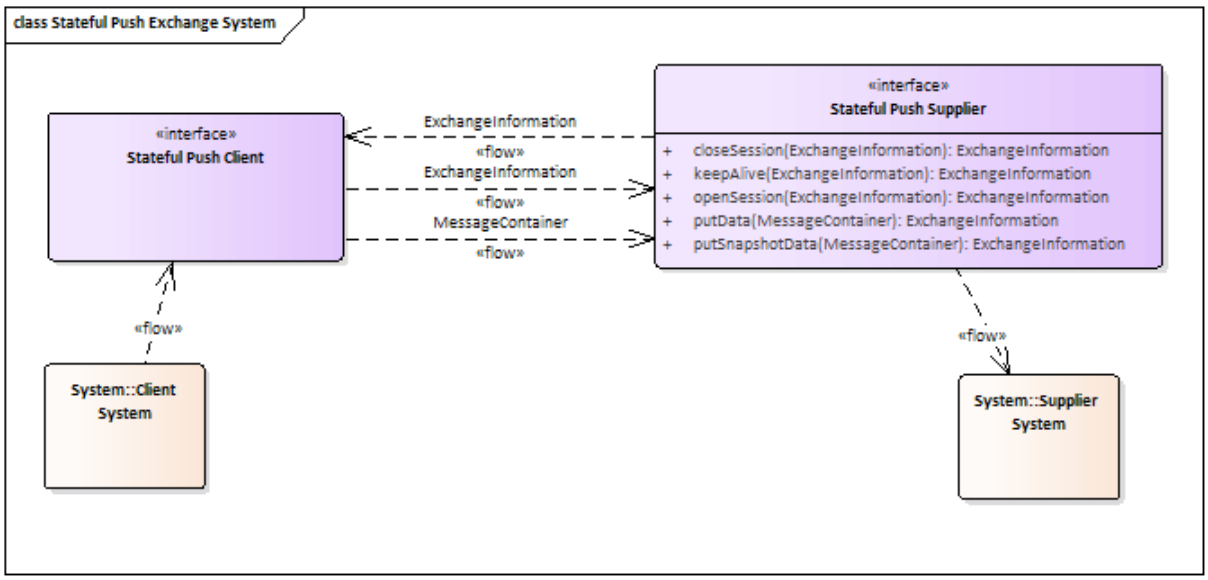

Figure 14: Stateful Push, Source: http://docs.datex2.eu

The Supplier takes the initiative to push the data under the following conditions:

- First Session Initialisation: one Snapshot alignment is needed to convey al currently available data at a first connection of Exchange.
- Session Initialisation: after a First Session had been created once needing a First Session Initialisation, for any time a Session had been closed or broken after some errors, it is necessary to align the Client by:
- A Delta Synchronisation, i.e. a simple payload Push delivering all updated content since last fulfilled Push
- A Snapshot Synchronisation with all the currently available content snapshot in case of snapshot alignment feature is requested by client.
- Snapshot Synchronisation request: one Snapshot alignment can also be acknowledged to the client for internal system need / maintenance / debug, it may be requested via any Return Messages on Exchange data.
- On Occurrence Push: as soon as an information is updated at the Supplier Systems, this condition triggers the Supplier to send push data to align to the Client to update the Client System as soon as possible after this update.

- Periodic Push: at predefined time interval the Suppliers start an exchange based on Client and Supplier agreement (subscription contract)

8.1.2.6 Properties of Push/Pull patterns

The following figure shows the properties of the different Push/Pull patterns.

Features area	Feature	Snapshot Pull	Snapshot Push	Simple Push	Stateful push
Subscription contract	Contract				
	Catalogue				
Session	Session life cycle				√
	Link monitoring			√	√
Information management	Operating modes	Periodic or On Occurrence (i.e. triggered by client conditions)	Periodic or On Occurrence (i.e. triggered by supplier conditions)	Periodic or On Occurrence (i.e. triggered by supplier conditions)	Periodic or On Occurrence (i.e. triggered by supplier conditions)
	Update methods	Snapshot	Snapshot	Snapshot, Single Element Update, All Element Update	Snapshot, Single Element Update, All Element Update
	Life cycle management	based on snapshot: new and updated content delivered, outdated data not delivered	based on snapshot: new and updated content delivered, outdated data not delivered	√	√
Data delivery	Data delivery	√	√	√	√
	Data request				Snapshot realignment
	Large datasets handling			optional	optional
	Synchronisation	√	√	optional	√
Self-Description	Handshake				
Communication	Security	*To be defined at PSM level*			
	Compression				
	Communication				

Figure 15: Properties of the Push/Pull patterns

8.2 Message exchange patterns

Beside the Exchange patterns and Functional Exchange profiles described in Section 8.1.2, there is also a choice between different message exchange patterns.

8.2.1 Request / Response - Client / Server

The request/response pattern describes a situation in a client service architecture, when a lot of clients (or devices) need to connect to a single server. They can request data from the server which is send to them in return. A typical example is a http request, answered by an (internet web) server.

8.2.2 Publish / Subscribe

In this centralised kind of messaging, one device is acting as a broker and manages subscriptions from clients (consumers), which can subscribe to different channels or topics, that are served with data by one or more publishers (producers). The broker does not store data; it simply moves it from publishers to subscribers. When data comes in from a publisher, the broker promptly sends it off to any client subscribed to that data.

By this construct, two interfaces between three parties are involved. Quite typically, these interfaces may be operated in push mode (i.e. publisher as well as broker are pushing the data), but this is not necessarily always the case. As a decoupling of participants and interfaces in terms of time, space and flow is one of the key aspects of publish subscribe, the exchange patterns of the two interfaces may vary. In the German Mobility Data Market Place (MDM) for example, push or pull patterns can be chosen individually and independent between the interfaces *publisher–broker* and *broker–clients* (and also independent between the different client interfaces).

8.2.3 Application layer protocols

8.2.3.1 Overview

In [Dizdarevic et. al, 2019], application layer protocols are analysed in terms of their usability for the Internet of Things (IoT), but this does not prevent them from being useful in terms of NAPs, C-ITS and the DIRIZON context, either.

Despite the popularity and wide-spread usage of HTTP, the currently used protocols in various domains are de-facto fragmented with many different solutions. This is due to the different requirements and areas that need to be covered, combining the functionalities of sensors, actuators and computing power with security, connectivity and a myriad of other features. As a result, there is no common agreement on the reference architecture or adopted standards of communication protocols. Thus, one of the fundamental challenges for system engineers is to choose the appropriate protocol for their specific system requirements.

The following table from [Dizdarevic et. al, 2019] lists some protocols in question together with some basic information and properties. For example, most of them are based on a publish-subscribe pattern, and TLS security is widely spread. Some of the more interesting protocols are presented in the subsequent chapters.

Protocol	Req.-Rep.	Pub.-Sub.	Standard	Transport	QoS	Security
REST HTTP	✓		IETF	TCP	-	TLS/SSL
MQTT		✓	OASIS	TCP	3 levels	TLS/SSL
CoAP	✓	✓	IETF	UDP	Limited	DTLS
AMQP	✓	✓	OASIS	TCP	3 levels	TLS/SSL
DDS		✓	OMG	TCP/UDP	Extensive	TLS/DTLS/DDS sec.
XMPP	✓	✓	IETF	TCP	-	TLS/SSL
HTTP/2.0	✓	✓	IETF	TCP	-	TLS/SSL

Figure 16: Application layer protocols and their features; from [Dizdarevic et. al, 2019]

8.2.3.2 RESTful http

Representational State Transfer (REST) describes a programming paradigm (an architectural approach) for distributed systems, especially for web services. In this sense, a REST API represents an alternative to other interfaces such as SOAP or WSDL. REST itself is neither a protocol nor a standard. However, implementations of the architecture characterized as "RESTful" use standardized procedures such as HTTP/S, URI, JSON or XML.

The term REST is intended to illustrate the transition from the current state to the next state of an application. This state transition is affected by the transfer of the data representing the next state. Originally, REST is an abstraction of the structure and behaviour of the World Wide Web. REST aims to create an architectural style that better represents the requirements of the modern web. REST differs from other architectural styles primarily in the requirement for a uniform interface.

The main purpose of REST is machine-to-machine communication. REST is a simple alternative to similar procedures such as SOAP and WSDL and the related procedure RPC. Unlike many related architectures, REST does not encode method information into the URI, because the URI specifies the location and name of the resource, but not the functionality that the Web service provides for the resource. The advantage of REST is that a large part of the infrastructure required for REST (e.g. HTTP-enabled clients, HTML and XML parsers, security mechanisms) are already known from www applications.

The fact that simple HTTP is used for a web service opens up many more interesting possibilities. For example, because HTTP defines a whole set of caching headers, a REST Web service can specify exactly under what circumstances and for how long a client can cache responses. In combination with unique addressability, the cache control headers also allow responses to be cached via a reverse proxy (such as Varnish or Squid).

Access security in a RESTful web service can be achieved most easily by using normal HTTP authentication. In this case, the client sends an authentication header with each request, in which a user name and password are encoded. The HTTP authentication itself does not require a user session, since the complete authentication data is simply sent along with each request. To ensure that no one can read the whole thing, the entire HTTP communication at transport level can be encrypted using SSL.

8.2.3.3 HTTP/2

Due to limitations in the well-known HTTP/1.1 protocol, a number of improvements have been developed and implemented in its successor HTTP/2, defined in RFC 7540. It provides an optimized transport for HTTP semantics and supports all of the core features of HTTP/1.1 but aims to be more efficient in several ways:

The 1.1 version uses the request/reply pattern, well known from calling internet sites, and is not suitable for push notifications from the server. In 2.0, the so-called server push is introduced, which means the server can send content to clients with no need to wait for their requests. Server push allows a server to speculatively send data to a client that the server anticipates the client will need, trading off some network usage against a potential latency gain. The server does this by synthesizing a request, which it sends as a PUSH_PROMISE frame. The server is then able to send a response to the synthetic request on a separate stream.

In addition, HTTP/2 enables a more efficient use of network resources and a reduced latency by introducing compressed headers, using a very efficient and low memory compression format, as well as allowing multiple concurrent exchanges on the same connection. This has especially advantageous impact upon request sizes in the common case, allowing many requests to be compressed into one packet.

Multiplexing of requests is achieved by having each HTTP request/response exchange associated with its own stream. Streams are largely independent of each other, so a blocked or stalled request or response does not prevent progress on other streams.

Flow control and prioritization ensure that it is possible to efficiently use multiplexed streams. Flow control helps to ensure that only data that can be used by a receiver is transmitted. Prioritization ensures that limited resources can be directed to the most important streams first.

8.2.3.4 MQTT

MQTT (Message Queuing Telemetry Transport) is a fairly well-known publish subscribe message queueing protocol. Version 3.1.1 is standardised in ISO/IEC 20922:2016 and adopted by OASIS. MQTT is extremely lightweight: it takes up almost no space in a device, so that even small devices with very little computing power can use it. MQTT itself doesn't define how the load (the data) is packed or unpacked, that can be done by open client specifications.

MQTT runs on top of the TCP transport protocol, which ensures its reliability. In comparison with other reliable protocols, such as HTTP, and thanks to its lighter header, MQTT comes with much lower power requirements, making it one of the most prominent protocol solutions in constrained environments. However, since MQTT was especially designed for unstable networks, it allows the use of three different service qualities (Quality of Service, QoS) 0, 1 and 2.

One central aspect of MQTT is an event-driven publish/subscribe architecture. There is no end-to-end connection, as for example with HTTP with its request/response architecture, but a central server (broker) to which senders and receivers of data connect equally. Messages are sent (published) or received (subscribed) via so-called topics. A topic is a string that has a URL-like structure and represents a type of subject for the message. The Broker now checks which interested parties in turn have opened a channel to receive this data and forwards the messages to them.

8.2.3.5 AMQP

The Advanced Message Queuing Protocol (AMQP) is an open internet protocol for business messaging, a binary network protocol on wire level that is independent from programming languages. All Functions of Java Message Service (JMS) are integrated. The protocol was initiated by an industrial consortium (JP Morgan, Microsoft, Red Hat, ...). The current version 1.0 is an open OASIS standard (Advancing open standards for the information society) and is also standardised in ISO/IEC 19464:2014.

AMQP has a layered architecture and the specification is organized as a set of parts that reflects that architecture. AMQP also implements a topic based publish subscribe system. It has a range of features that it implements.

AMQP can be used as a guaranteed transport for Web service calls - AMQP does not define the payload, just the transport layer, which means that SOAP, WS-Security, WS-Transactions, WS-MetaData Exchange, and so forth can all be run over AMQP in the same way that they can be used over JMS. However, AMQP provides vendor-neutral interoperability at the lowest levels of the transport link.

In the C-ITS scenario "NordicWay"[2], the interchange uses a publish-subscribe AMQP (v1.0) queuing system for distributing messages between connected actors. In this system, all actors take the role of either a producer or a consumer. A single actor can also be both a producer and a subscriber at the same time.

8.2.3.6 STOMP

The Simple (or Streaming) Text Oriented Messaging Protocol (STOMP) is an Interoperable wire format. It was formerly also known as TTMP and provides easy and widespread messaging interoperability among many languages, platforms and brokers. The simple design is coming from the HTTP school of design and leads to a very simple and easy to implement protocol, at least at client side (the server side is harder to implement). Telnet can be used for interactions with STOMP brokers.

A typical usage scenario of stomp could be the following, like in the German C-ITS Corridor for the interface between an ITS Roadside Station (IRS) and an ITS Central Station (ICS):

The transport layer between is based on TCP, using IP as its network layer. The physical layer is realized by cellular links with different protocols on the data link layer (GPRS, UMTS, LTE) (alternatively, also wired connections could be used for data transmission).

[2] https://www.nordicway.net/

The transport layer is encrypted by using TLS/SSL in the session layer. On top of the session layer, the WebSocket protocol is used to establish a connection between the communication partners. In the given context, this protocol has been chosen due to its compatibility with firewalls. STOMP is used as application level protocol to exchange messages. STOMP has been chosen because it is a simple messaging protocol which has been designed to work with internet connections passing through firewalls. The interface between Message Broker and App is internal, so any messaging protocol (e.g. STOMP, AMQP etc.) can be used to connect to the message broker. The messaging approach is important to realize the bidirectional and asynchronous communication pattern of message flow between the two partners. Messages are encoded in XML and optionally compressed by GZIP.

Information is exchanged via message queues, which are provided by a message broker. Both applications connect to a message broker, subscribe to specific message queues, send messages to message queues and receive messages from previously subscribed message queues.

Before sending and receiving messages to and from a message broker, the application must open a STOMP connection over secure web sockets. The following figure shows the application stack:

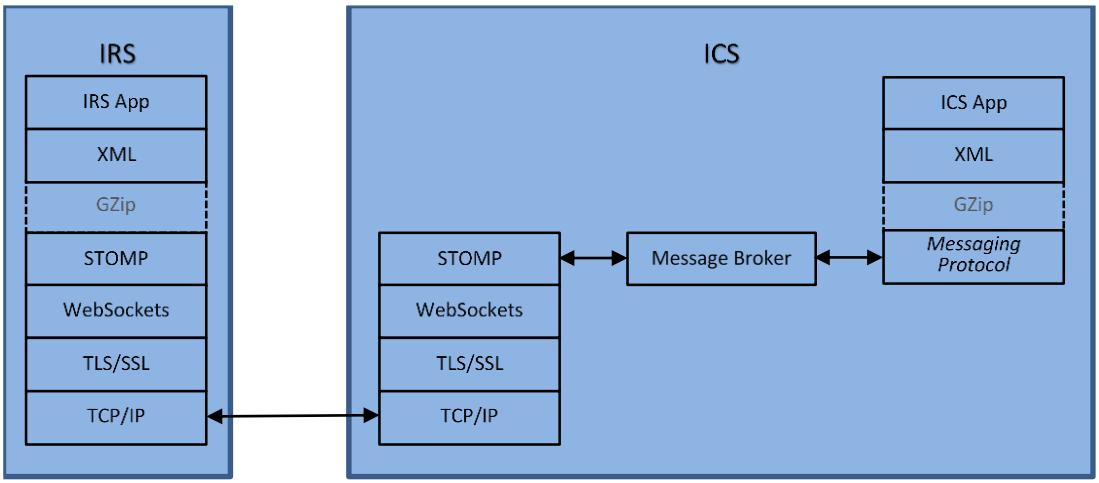

Figure 17: Application stack using STOMP, here in a scenario for the German C-ITS Corridor

8.2.4 API

An API (Application Programming Interface) is a set of definitions and protocols that allow technology products and services to communicate with each other via the internet.

It allows an application to interact with an external service using a simple set of commands. Using an API allows developers to implement specific modularised functionalities for their applications which can speed up the development process or in other words APIs act like building blocks, allowing developers to build applications much faster. They prevent developers from having to “reinvent the wheel,” and spend time creating functionality that already exists.

Today, APIs are provided by various software vendors to make it easier for programmers to access software components. SAP, Amazon and Google, for example, offer APIs for various application areas. Developers can use these interfaces to perform different tasks:

- Forward a programmer's instruction to a software and receive its response
- Inserting content into web services
- Reuse app codes thanks to networking of programs
- Control access by other programmers

In daily use, APIs are used for example for web services. Anyone who books a flight can instruct an appropriate search engine to find all flights and fares to a specific destination and date. As soon as you click on "Search", the website starts communicating with the APIs of the individual airlines to query the prices to the destination. This is done within seconds and the customer quickly has an overview of bookable flights.

Although they serve the end user, APIs are primarily for programmers. The Application Programming Interface is usually provided by the developers of a software so that programmers of other applications can use the interface. The Application Programming Interface defines how information and data is received and returned between modules. Google, for example, publishes the API to allow other programmers to dock their own applications to Google's services. To do this, they use their own standard to which the external software must adhere.

Very popular for communication between applications - especially within the web - is the REST protocol. A REST API uses the same commands that are used for HTTP. The instructions are not complex and therefore make the exchange of information very easy. Additionally, the simple protocol makes it easy for programmers to connect to the API.

Standardisation is therefore important in order to be able to provide the programming interface - no matter which protocol is used for the exchange. In addition, other programmers should also be taught how to use the interface correctly. Therefore, an API is often provided with detailed documentation on syntax and function.

There are basically four different classes of programming interfaces:

- Function-oriented APIs
- File-oriented APIs
- Protocol-oriented APIs
- Object-oriented APIs

The choice of class depends on the application. Function-oriented programming interfaces are relatively complex interfaces. For example, they enable developers to access hardware components. Only functions are ever called. File-oriented APIs enable connection at file level. Data can thus be retrieved and written. The protocol-oriented interface is used for standardised communication between programs, but is independent of operating systems or hardware. The object-oriented APIs can be used flexibly.

When differentiating between APIs, the internal interfaces can also be distinguished from the public ones. Private interfaces are only available within a company for example. They are often used to connect company-owned functionalities so that employees or customers can access them via private networks. Public interfaces are available to everyone and can often be conveniently used by software developers. Google, Amazon, eBay, Facebook, Twitter and PayPal are good examples of public APIs. Many manufacturers (e.g. Google) also actively invite developers to participate in their API development.

APIs have advantages for different groups: Users benefit from the programming interfaces as much as internal or external developers or service providers.

Developers or service providers who equip their programmes with good programming interfaces can expect to see better distribution. Because it makes it easier for other programmers to interact with the software, applications with good APIs are preferred. Other developers or service providers can greatly extend the functional scope of their own software or application by linking it to other applications. In the end, it is mainly the users who benefit from the connection via the interface: they can easily combine different programs or applications with each other and thus enjoy more comfort and potential additional benefit of combined information.