Whitepaper

Technical design and setup of Mobilidata environment V2.0

`

Author: M. Wiggerts, W. Vandenberghe
Version: 2.0
Date: 12-05-2026
Status: Final

Version history

Version	Date	Author	Remarks
0.1	05-19-2022	W. Vandenberghe, M. Wiggerts	Initial version
0.2	06-01-2022	W. Vandenberghe, M. Wiggerts	Details added
0.3	06-03-2022	W. Vandenberghe, M. Wiggerts	Review comments
2.0	12-05-2026	W. Vandenberghe, M. Wiggerts	Reworked version. Includes changes that were made to the Mobilidata system architecture during its development. Also overhauled the component names for improved clarity. And added envisaged to be changes regarding archive and movable physical barriers.

Content

1 Introduction

The architecture of the Mobilidata platform was designed to fulfil the needs and wishes of the Flemish government with regard to improving traffic safety and the efficiency and sustainability of roads through data infrastructure and innovative use cases that make use of that data. To achieve this goal, the ability to exchange data between different partners, suppliers and road authorities in a standardized manner is essential. In the following paragraphs, the design and handling of the information objects and information flows are presented in a framework that can be used by current or potential partners to build and interact with the Mobilidata environment.

Existing technology is used as much as possible to simplify deployment, reduce costs and increase the degree of acceptance. International programs like C-Roads (EU), Talking Traffic (NL), Nordic Way (FI, NO, SE, DK) and the Data Task Force (EU) already paved the way for communication standards, message formats and centralized interchange mechanisms. This Mobilidata Framework used and extends these standards for optimal use in Flanders and possible extensions in the initiating programs.

2 Adding value

For obtaining optimal results in efficiency and sustainability optimization, 27 operational use cases have been defined originally in Mobilidata for which the environment must provide support and ideally exceed the expectations. The architecture is based on existing mobility deployments, but makes use of the flexible setup to support first the use cases and the mechanisms that improve the supplied data by road user feedback and other comparisons/analytics. In this way, the Mobilidata environment is capable of adding effective value to the entire mobility ecosystem by improving the quality of source information and information for end users and by enabling the necessary feedback.

2.1 International standardization

The Mobilidata environment uses the basic standards of international smart mobility initiatives, adding extensions to enhance or update the value of applied services. The standards are derived from the following initiatives:

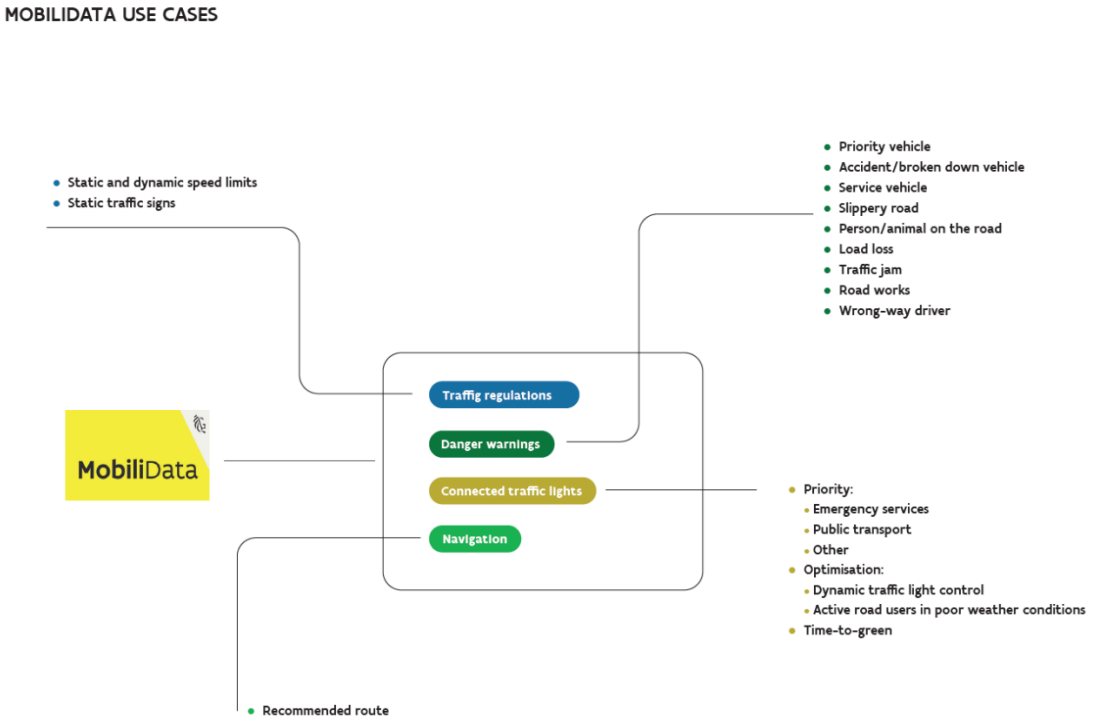
- C-ROADS.
  The C-ROADS Platform is a joint initiative of the European Member States and road operators for testing and implementing C-ITS services with emphasis on cross-border harmonization and interoperability.
- Talking Traffic.
  The Talking Traffic partnership is a collaboration between the Dutch Ministry of Infrastructure and Water Management, 60 regional and local authorities and national and international private companies. Together they work on the large-scale deployment of long-range C-ITS use cases in the Netherlands, including several C-ITS use cases related to traffic lights.
- Data for Road Safety
  Conceptually, the purpose of a neutral server is to receive and distribute safety messages sent by vehicles (e.g. engagement of stability control, airbag deployment). These messages are provided by servers controlled by car manufacturers, displaying ExVe[1] safety messages from vehicles as specified by ISO20078. The first project in which this ISO standard was tested was the Data Task Force. As part of the project, BMW, Ford, Volvo, Mercedes-Benz and Scania shared their vehicle-generated safety related traffic information (SRTI) with each other, with service providers such as HERE, TomTom and NIRA Dynamics, and with road operators from Germany, the Netherlands, Luxemburg, Spain, Finland, Austria, Flanders and the United Kingdom. Given the success of this proof-of-concept delivered by the Data Task Force project, the involved parties decided to continue these activities after the project ended in an initiative called Data For Road Safety.

2.2 Use cases

There are 27 functional use cases defined as part of the original Mobilidata requirements in which the architecture must be compliant in supporting the information flow and excellent performance technology. Each use case adds value to the end user through the specific form of information it provides. Use cases can be used in any combination or separate, without loss of functionality.

The diagram below illustrates these use cases and divides them into distinct categories:

[1] Both the ExVe interface and the Sensoris interface are supported



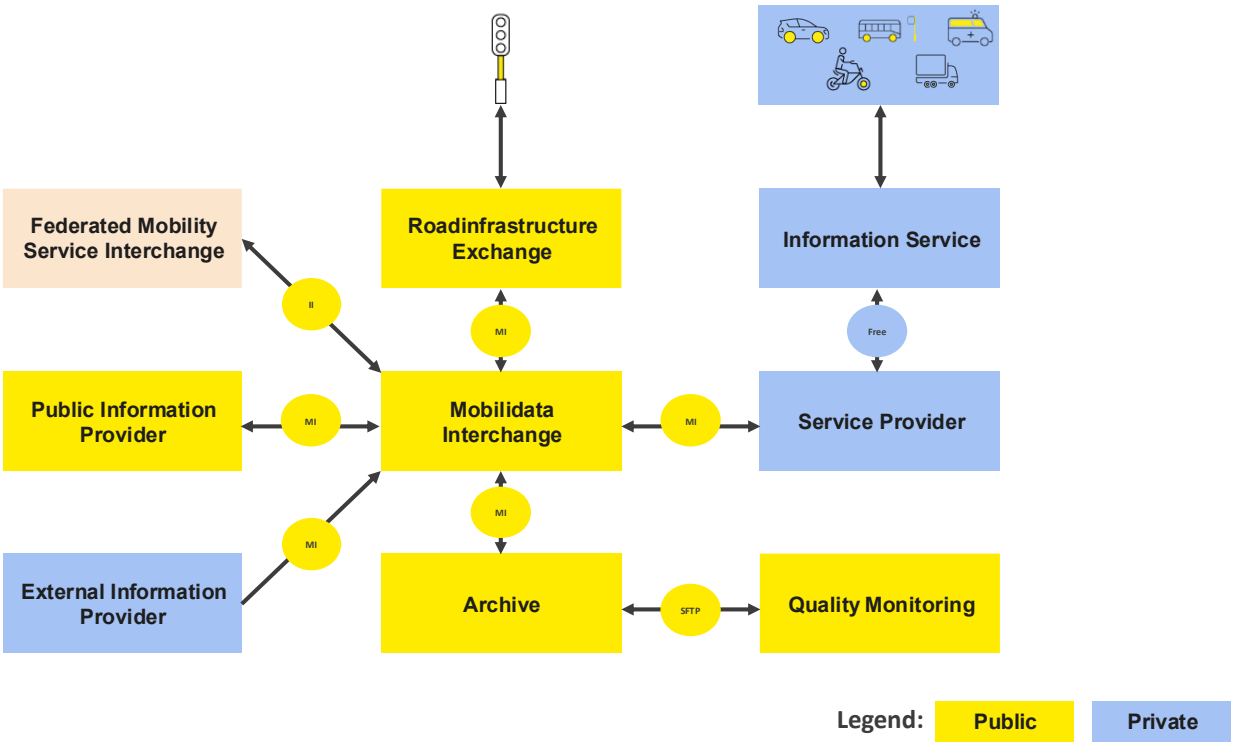
01. Traffic regulations
    Providing static road information, like road signs or other roadside information for in-car notification.
02. Danger warnings
    These use cases are meant to provide users with information about actual traffic or infrastructure conditions in order to improve safety and traffic flow. Note: while only motorists are mentioned, this also extends to cyclists and pedestrians.
03. Connected traffic lights
    Increasing the efficiency of traffic lights is one of main goals of Mobilidata. To achieve this, the architecture and experience first gained in the Netherlands through Talking Traffic is applied to the Flanders context.
04. Navigation
    Providing deviations from preferred routes and information about available parking spaces for specific vehicles.

The use cases in relation to connected traffic lights all focus on making traffic lights smarter by supporting the following situations:

- Improving the flow of emergency vehicles at a traffic light:
  Giving absolute priority (both green light and empty passage) to emergency vehicles that are legally allowed to go through a red light
- Supporting preference requests:
  Giving conditional priority to road users based on vehicle type (e.g. public transport, exceptional goods transport) or grouping similar road users
- Informing road users of the current and upcoming traffic light status (e.g. time-to-green light).
- Improving traffic control:
  Managing traffic more efficiently by providing real-time location data about the different road users near the intersection.

3 Information streams

The information streams in the Mobilidata environment are based on (but not identical to) the standards and protocols used by C-Roads, Talking Traffic, Neutral Server and others. Additional information is provided alongside the original protocols to increase value as needed. This additional information should ideally become part of the standard itself.



The most important link in the information chain is the Mobilidata Interchange. This interchange allows public information providers to interact with external information providers such as neutral servers and road infrastructure (e.g. smart traffic lights) for the benefit of end users. The interchange (following C-Roads) uses two interfaces:

- MI interface: this is an extended but upwards compatible version of the C-Roads Basic Interface (BI), which is in essence a metadata envelope that allows for the exchange of standard ETSI or DatexII messages using the AMQP protocol
- II interface: this improved interface is used to communicate with other mobility environments about available capabilities, to which players in the information chain can automatically adjust

For monitoring and analysis purposes, data is stored in a GDPR-compliant historical archive from which the data is retrieved in SFTP interface format. Retention time varies for different types of content.

General traffic information for public information purposes is derived from a number of local government data sources. The information is converted for compatibility with a standard

transmission method, as described in the previous paragraphs. Examples of public data sources include GIPOD (database with road works data), static information about truck parking, calamity routes, road registers, dynamic lane signals (RSS) and dynamic zone 30.

Road users receive Mobilidata updates from Information Services, which on their turn are supported by Service Providers. These Service Providers communicate with the interchange and are responsible for receiving and creating C-ITS messages (as defined by C-Roads using ETSI and ISO C-ITS message standards), and providing that same information to the Information Services in a potentially more easy to process data format (JSON, XML, …). Priority requests from road users are initiated by the Information Service that shares the locations and potentially desired routes from its users with the Service Provider. The Service Provider then creates the appropriate C-ITS messages and sends them via the Mobilidata Interchange to the Road Infrastructure Exchange and the relevant connected traffic light (iTLC aka iVRI).

Road user feedback is a very important mechanism to improve the quality of road and traffic-related messages. Road users have a real-time opportunity to spot faulty or incomplete information. There are two ways in which end users can share feedback with the system:

- Directly by using the mobility application while driving
- Indirectly by completing a questionnaire at the end of their journey

In both cases, the road user feedback (RUF) is based on the original C-ITS information message (IVI, DENM) and sent via the service provider for storage in the historical archive. The dashboard and analytics feature compares the original messages to the RUF messages in order to spot potential anomalies.

4 Technology

4.1 Concepts

The overall Mobilidata system architecture is based on three main technological concepts.

- Interchange (adopted from C-Roads)
- Intelligent traffic light control installations (iTLC, adopted from Talking Traffic)
- Extended vehicle information (adopted from Data for Road Safety)

These items are explained in the next paragraphs.

4.1.1 Interchange

Following the C-Roads architecture, the concept of an interchange is implemented in the Mobilidata environment. The interchange is primarily meant as a low-latency publish-subscribe service to exchange messages with the peripheral functionality. The message-based system is built on an AMQP bus structure that can exchange most message types and is particularly useful for the small mobility messages used in the Mobilidata environment (ETSI C-ITS messages). The communication is IP-based.

As standard, AMQP uses properties for internal administration purposes. An application can add specific metadata (application properties) as well. Within C-Roads, a standard set of metadata is defined (basic interface or BI) that does not take into account road user feedback streams or specific service providers. For this reason, a new standard was created: the Mobilidata interface (MI). The MI interface is a superset of the BI interface defined by C-Roads.

<table>
<tr><td></td><td></td><td></td><td colspan="3">BI message</td><td></td></tr>
<tr><td>Header</td><td>Delivery annotations</td><td>Message annotations</td><td>Properties</td><td>Application properties</td><td>Application data</td><td>Footer</td></tr>
<tr><td colspan="7">Annotated AMQP Message</td></tr>
</table>

The improved interface is used to detect the remote's interchange capabilities. No additional features have been defined, which means the Mobilidata II interface is identical to the C-Roads II interface.

Access to the AMQP bus is through token-based authorization and whitelisting. A service provider can only read or write in areas for which it has specific rights. In this way, service providers are strictly separated and can only provide the agreed services.

4.1.2 Connected traffic lights

Connected traffic lights are also regularly called Intelligent Traffic Lights (iTLC or iVRI as they are referred to in the Talking Traffic program that coined the term). These are traffic lights that:

- Adapt their control strategy to the actual presence of different modalities and policies of the road authority
- Adapt their control strategy to priority requests from authorized vehicles, such as emergency vehicles
- Send the geographical layout and current and upcoming signal group statuses (including expected timing and priority request confirmations) to the users in close proximity

All iTLCs consist of three (shared) components:

- RIS:
  Responsible for maintaining a local dynamic map of a junction and handling C-ITS messages for a junction. It also manages network-related security tasks, essentially connecting the iVRI to the outside world.
- Traffic Light Controller (TLC):
  Responsible for actuating the lights of the different signal groups (i.e. traffic lights) at an intersection and preventing unsafe situations (e.g. checking traffic light conflicts and intersection clearance times). This means the TLC is similar to a legacy traffic light controller.
- ITSApp:
  Responsible for controlling the traffic flow in an optimal way and determining the best signal phase and timing values to be sent to the Traffic Light Controller. Hence the ITSApp actually puts the extra intelligence in iTLC compared to a legacy traffic light controller.

The central Mobilidata service architecture of the iVRI is built around the Road Infrastructure Exchange. This component is responsible for distributing traffic light information. It is the single aggregation point that couples all deployed iVRIs with the Mobilidata Interchange, handling C-ITS messages to and from road users and traffic lights. A sub-component is the Traffic Light Priority Validator. That component performs basic checks on priority requests coming from emergency and high-priority road users (e.g. buses, cycling groups). The responsibility to grant these requests (taking current road conditions into account) lies with the ITSApp component of the iVRI.

4.1.3 Extended vehicle information

Many modern vehicles are equipped with telematics units. These units are able to send safety related traffic information (SRTI) across the mobile network to data collector-specific car manufacturers. The Data for Road Safety ecosystem (dFRS), an initiative of the auto industry and European governments, is responsible for collecting the anonymized and free data in neutral servers. For the latter, the ExVE and Sensoris protocols are used.

4.2 Security and privacy

4.2.1 Security

Security is a vital concern for the overall Mobilidata system and its parts. As designed today, the Mobilidata system architecture does not use the geo-casting network protocols on top of MAC-layer packet broadcasts, since deployment of short-range communication (ITS-G5, LTE-V2X) does not fall within scope of the program. The Mobilidata system architecture can therefore be seen as a rather classical ICT or IoT ecosystem. It is composed of a rather limited number of well-known services and applications that interact with each other in a connection-based way using the standard IP stack. Based on thorough analysis, it was decided by the Mobilidata program to base the security approach on the following two main security principles:

- **Transport Layer Security (TLS):**
  All connections between components will be secured using Transport Layer Security (TLS). The Certificate Authority of Flanders Government (vlaanderen.be) is used as a root. Hierarchical coupling with more slave systems is possible.

- **Binding Requirements:**
  New components are only allowed to connect to the Mobilidata system architecture deployment once trust in them has been established through the verification of compliance with all binding requirements. These requirements determine which prerequisites should be fulfilled by a component before it can be trusted to participate in the Mobilidata ecosystem.

Note: Verifying this requires thorough testing, both on a component and a system level. Their results must be approved by the Mobilidata governing body, which is part of the Flemish Agency for Roads and Traffic (AWV). No participant of the Mobilidata deployment is allowed to connect to a new component that has not been approved by this governing body.

In this way, trust is established in all components and in all connections. The following security measures are hence taken for the entire deployment:

- Authentication
- Authorization
- Confidentiality
- Integrity

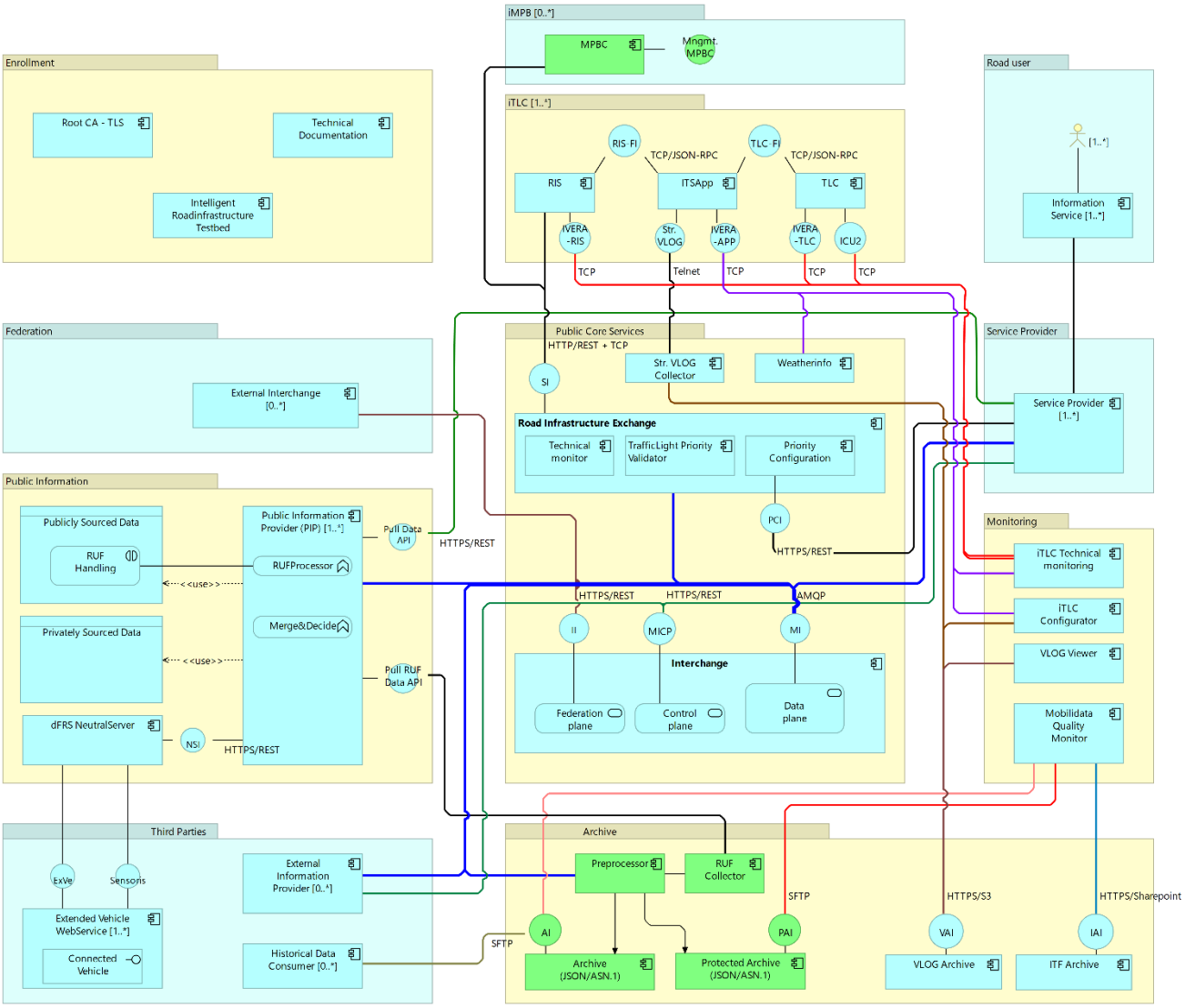
Note: After the TLS connections are established using asymmetric cryptography, symmetric cryptography is used for the TLS data payload. This does not compromise latency or throughput of the information flow, nor does it require excessive computational power at aggregation points in the system architecture. This makes the proposed approach to security cost-efficient. It also only relies on the availability of trusted certificate authorities (CA) for issuing the X.509 certificates that are needed to establish the TLS tunnels. These trusted CAs are already widely available since TLS is used to secure practically all current internet services. This approach has no dependency regarding deployment lead times on the availability of novel public key infrastructure concepts. In fact, all X.509 certificates are acquired from the existing CA service of the Flemish Government.

4.2.2 Privacy

All components deployed within or coupled with Mobilidata must comply with the General Data Protection Regulation (GDPR). This implies that every party deploying components in the Mobilidata ecosystem must sign the appropriate Data Processing Agreements (DPA) with their peers as part of the binding requirements introduced in this chapter. This guarantees that the deployment of Mobilidata does not infringe upon the consent given by end users as regards the processing of personal data. Furthermore, sound access management must be implemented for all components and all cloud and data storage platforms must be physically located in the EU and compliant with the Schrems II Judgement.

5 Solutions

The following diagram provides an overview of the Mobilidata architecture, depicting both the components and their organizations into packages. These packages are described in more detail in other documents. Note that components in one package are not necessarily deployed on the same node. It also shows which ports and interfaces are supported or required by these components.



The packages are described in more detail in the next sections.

5.1 Public Core Services

This package contains the components that constitute the public Mobilidata services from the perspective of third parties. In other words, it is with these components that external parties will connect.
The components are:

- **Interchange**
  This connects to the public service that enables the efficient exchange of information used to create co-operative use cases. The Interchange implements the interchange concept as defined by C-ROADS and is responsible for collecting and distributing traffic information to mobility applications with the low latency required by C-ITS applications. It is responsible for:
  - publishing capabilities through the II interface
  - performing AMQP server functions, including:
    - connection management
    - message management
  - receiving and publishing MI messages:
    There can only be one MI message publisher per information type for one or more use cases.

- **Road Infrastructure Exchange**
  The Road Infrastructure Exchange is responsible for exchanging all data between the iVRIs and the vehicles/users in the direct proximity of an iVRI. Communication between Road Infrastructure Exchange and other Mobilidata components goes through the MI interface. It contains three sub-components:

  - **Technical Monitor**. The purpose of this component is to assess the correct real-time functioning of the Road Infrastructure Exchange from a technical point of view. It also validates the technical functionality of the priority request information stream. This includes checks on latency timing on incoming and outgoing priority messages (SRM and SSM), the number of rejections and other statistics. These checks are also very suitable for detecting abuses of the priority feature based on anomalies in the information stream, traffic science aspects, monitoring and analysis. This assessment is based on the information that is communicated over the MI interface of the Road Infrastructure Exchange. The correct functioning from a traffic engineering perspective is not assessed by this component. This means that it does not assess if the iTLC is reaching optimal throughput, if it could have made a more empty passage for priority vehicles, etc.

  - **TrafficLight Priority Validator**. All priority requests (SRM messages) sent through the Road Infrastructure Exchange to an iTLC (iVRI) are redirected over the TrafficLight Priority Validator for validation. Once the technical and administrative validation has been completed and the request does not conflict the specific priority rules for the iTLC (iVRI) stored in the Priority Configuration, the priority request message is passed on. If the request is not valid, the denial message (SSM) is sent via the Interchange to the original Service Provider.

  - **Priority Configuration**. This components contains the envisaged policy of the road authority regarding the priority use cases for every iTLC. It is used by the TrafficLight Priority Validator to make sure only requests are sent to the connected traffic lights that are in line with the desired road authority policies. It is also used by the Service Providers to make sure they only create priority request messages that are in line with those policies.

- **Streaming VLOG collector**: VLOG is a specific logging format supported by iTLC's. It provides insight in not only the switching cycles, but also the activations of the different sensors installed at the intersection (inductive loops, push buttons, radar, etc.). The Streaming VLOG collector component retrieves this data from the iTLC's, and pushes it to the VLOG Archive.
- **Weatherinfo**: this component provides the iTLC's information on the current weather conditions. This is needed for the use case where active road users are served quicker by the iTLC in case of poor weather conditions.

5.2 Public Information

For the use cases regarding traffic regulations, dangers warnings and navigation, the goal of Mobilidata is to have the public sector, hence the road authority AWV, create a useful information stream that can be presented to road users. The Public Information package contains the components needed for this. It consists of four components.

- **The Public Information Provider (PIP)** component is the primary component of this package. It is intended to supply information needed to realize one or more Mobilidata use cases, information created from raw public and private data (which is turned into information by the **Merge&Decide** subcomponent) and from received RUF (which is processed by the **RUFProcessor** subcomponent). In some cases, the RUFProcessor will also forward this RUF to the corresponding Publicly Sourced Data component so that it can update the source data accordingly. An example of such a feedback loop is a public road database for which RUF indicates that there is a faulty speed limit on a certain road segment).

  To make dynamic information available, the Public Information Provider converts it into MI-supported messages. Some more static information does not need to be published on the MI interface of the Interchange, since that interface is mainly intended for low-latency dynamic information. Other pull instead of push oriented publication mechanisms are therefore allowed for more static information. The preference is to work as standardized as possible and to therefore use a Pull Data API (TN-ITS and DATEX II) for the publication of specific more static information where possible. The PIP adopts the

following publication type strategy:

Overview Mobilidata use cases data publication path

Mobilidata Use Case		
1 – Static speed limits 1 – Dynamic speed limits	14 – iTLC Time-to-green information and speed advice	27 – iTLC Traffic signal optimisation – active road user
2 –Static road signs	15 – iTLC Priority emergency vehicle	28 – iTLC Time-to-green information advice – active road user
3 – Priority vehicle warning	16 – iTLC Prioritising public transport	29 – iTLC Prioritising in adverse weather conditions – active road user
	17 – iTLC Prioritising vehicle convoy	
5 – Accident/vehicle breakdown warning	18 – iTLC Prioritising truck	
6 – Active service vehicle warning	19 – iTLC Traffic Signal optimisation	MAP topic on Interchange: enabled retention
	20 – Recommended routing – emergency routes & locations to avoid 20 – Activated emergency routes	
8 – Slippery road warning	21 – Truck parking information – static data (location, capacity, …)	
9 – Person/animal on the road warning	22 – Park & Ride facility information – static data	
10 – Spilled load warning	23 – Static road signs – active road user	
11 – Traffic jam ahead warning	24 – Priority vehicle warning – active road user	
12 – Road works warning	25 – Road works warning – active road user	
13 – Wrong way driver warning	26 – iTLC Prioritising convoy – active road user	

Interchange publication
Pull data API publication (TN-ITS or DATEX II)

- The **Publicly Sourced Data** component represents a type of public raw data sources. This can be a road database, real-time data on road incidents coming from the traffic control center of the road operator, etc. Note that a public data source can be a source owned and managed by a public authority but can also be a third-party data source provided as open data on behalf of a public authority.

- The **Privately Sourced Data** component represents a type of private raw data sources. This is data that is not publicly available, and obtained (often through purchase from commercial data providers) by the PIP to be able to create an information stream with higher coverage and quality for the Mobilidata use case that it realizes.

- **dFRS NeutralServer**
  Collecting sensor data for Flanders gained from vehicles from the different car manufacturers united in the Data for Road Safety initiative (which they expose in their Extended Vehicle Webservice). The collected data is provided to the PIP's that want to use it to create information and translate that into MI messages to send to the Mobilidata Interchange MI interface.

  For car manufacture data exchange, the standard protocols ExVe and Sensoris are used by the dFRS NeutralServer.

5.3 Service Provider

This package consists of one component with the same name, **Service Provider**. This component can be seen as the back-end oriented component that helps the front-end oriented Information Service with the realization of the Mobilidata use cases. These Service Providers communicate with the interchange and are responsible for receiving and creating C-ITS messages such as CAM, SREM, SSEM, SPaTEM, MAPEM, DENM, IVI, etc. They share the corresponding Mobilidata information they received from the Interchange with the Information Services in a potentially more easy to process data format (JSON, XML, …). The other way around they also create C-ITS messages on behalf of the Information Services and send them to the Interchange. E.g.: priority requests from road users are initiated by the Information Service that shares the locations and potentially desired routes from its users with the Service Provider. The Service Provider then creates the appropriate C-ITS messages and sends them via the Mobilidata Interchange to the Road Infrastructure Exchange and the relevant connected traffic light (iTLC aka iVRI). Road User Feedback (RUF) generated by the road users is also provided by the Information Service to the Service Provider in a proprietary protocol. The Service Provider then creates the corresponding ETSI message to capture that RUF, and sends it to the PIP over the Interchange

5.4 Road user

This package consist of one road user-facing component called the **Information Service**. It receives and displays up-to-date information to the user to realize the different Mobilidata use cases regarding traffic regulations, danger warnings, connected traffic lights and navigation. It also sends timely location updates for the connected traffic lights optimization and priority use cases. And it also collects and sends Road User Feedback (RUF). The Information Service makes use of a Service Provider to connect to the Mobilidata ecosystem, as described above, and summarized as follows:

- Information Services receive and display up-to-date information and create and send timely location updates and RUF.
- Service Providers on one hand create correct C-ITS messages regarding the location updates and RUF received from the Information Service, and send them to the Mobilidata Interchange. On the other hand, they process C-ITS messages received from the Mobilidata Interchange and send the corresponding information to the Information Services.

This functional separation makes it clear that the distinction between Information Service and Service Provider cannot be reduced to a distinction between cloud services and smartphone applications. Depending on the technical design, this boundary between the two can be very different. For example, a client app on a smartphone can create correct C-ITS messages and process them all on the phone. That app should then be seen as both a part of the Service Provider (the component that creates and processes C-ITS messages), and as the entire Information Service (the components that collect the GPS data and present iTLC information to the user). But another client app on the smartphone can, for example, limit itself to forwarding GPS updates to a backend, and expect that back-end to translate this GPS data into correct C-ITS messages (CAM, SRM, etc.) at the right time and then send it further down the chain on behalf of

the app. In that case, the smartphone app is the Information Service, and the backend is the Service Provider.

5.5 Intelligent Traffic Light Controllers (iTLC)

The connection of intelligent traffic lights (iTLC or iVRI) is standardized based on the Talking Traffic program and uses the SI protocol to communicate with the Road Infrastructure Exchange.

The iTLC sub-package consists of the following three components:

- **RIS**: the Roadside ITS Station sends cooperative information messages to ITS applications and a SPAT/MAP service, as well as information on the junction structure (Local Dynamic Map).

- **ITSApp**: the component that controls an intelligent traffic light and contains the more advanced logic to realize the different use cases for one or more traffic lights.

- **TrafficLightController (TLC)**. The component that steers the actual lights of the traffic lights. In normal operation an ITSApp tells the TLC how the switching cycle should look like. But in case connectivity between TLC and ITSApp is lost, the TLC can also control the lights using a built-in backup switching cycle definition. A single TLC can manage multiple physical intersections. The TLC-ID is therefore not the same as the intersection-ID.

5.6 Intelligent Movable Physical Barrier (iMPB)

This package represents the connection of movable physical barriers such as bar gates and automatic telescopic bollards to the Mobilidata ecosystem. This way the iTLC priority use case can also be used to provide authorized services such as emergency services access to the area that is being restricted by the barrier. Although some of these iMPB's are publicly owned (e.g. bollards at pedestrian areas), the majority of them is owned by private organizations to protect their private property from undesired access (factory sites, camping grounds, etc.). By coupling their iMPB to Mobilidata, these owners can make sure that help can arrive as quickly as possible if an incident would occur on their site. In contradiction with the iVRI, the internal architecture is kept simpler and more open. It is only assumed that the iMPB is controlled by some kind of **Movable Physical Barrier Controller (MPBC),** that this MPBC is able to connect to the Road Infrastructure Exchange through the SI interface, and that it can be configured (e.g. access policies) by a **Management MPBC component**.

5.7 Archive

Historical data archive for quality monitoring of the Mobilidata information streams and other functions that realize the different use cases. The archive is also intended to support historical mobility analytics (assessment of mobility policies, among other things) where the data licenses allow this and privacy regulations are complied with. Information collection is done through:

- **Preprocessor.** This components retrieves messages from the MI interface, assesses if it is allowed to archive this message according to GDPR regulations and the PIP data licenses, and if so also determines if the message should be stored in the Archive or in the Protected Archive and forwards it for storage to the appropriate component. Next to MI messages, the Preprocessor also receives RUF messages from the RUF Collector that it processes in a similar way.

- **Archive.** This component is responsible for the long-term storage of published Mobilidata messages that are not privacy-sensitive. The messages are stored in a file-based manner, and contain both the Base64 representation of the C-ITS message as it was published in ASN.1, and the JSON representation of the AMQP Application Properties that were attached to that published message on the MI interface. The files can be retrieved using an SFTP interface. Different retention times will apply, depending on the character of the information.

- **Protected Archive**. This component is responsible for the long-term storage of published Mobilidata messages that are privacy sensitive. For instance early warning messages regarding emergency vehicles or shock absorber trucks. The Protected Archive is identical to the Archive, but has more stringent security measures that only allow access to the data for specific individuals that have been granted access to this data by the Mobilidata / AWV DPO. Different retention times will apply, depending on the character of the information.

- **RUF Collector**. Retrieves RUF messages from the PIP, and forwards them to the Preprocessor for long term storage.

- **VLOG Archive**. Long time storage of the VLOG data produced by the Mobilidata iTLC's. Also exposes its data through a S3 compatible interface. The format of the VLOG messages is not altered, and stored as-is.

- **ITF Archive.** Sharepoint document storage used by the Mobilidata team that coordinates the iTLC deployments in the field. All Intersection Topology Format (ITF) files used by the iTLC's are collected on this location as part of the iTLC deployment process. The ITF file is used by the RIS component to automatically create the derived MAPEM messages. The correctness of those ITF files has proven to be critical for the correct functioning of the iTLC related use cases. Therefore the Mobilidata Quality Monitor uses the ITF archive to perform different kinds of quality control checks on these files.

5.8 Monitoring

The Monitoring package contains all functionalities for gaining insight into produced information message flows for the use cases related to traffic regulations, danger warnings and navigation. It also allows to analyze connected traffic lights behavior. The results can be used with quality assurance purposes to adjust the implementation of the different components in the Mobilidata system architecture. The Monitoring components include:

- **iTLC Technical Monitoring**. The purpose of this component is to assess the correct real-time functioning of the iTLC's deployed in the field. This assessment is based on the information that is retrieved from the management interfaces of the RIS, ITSApp and TLC components of every iVRI. It allows the quick activation of mitigation actions in case an iTLC has technical issues. The correct functioning from a traffic engineering perspective is not assessed by this component. It also does not verify the proper handling of priority requests.

- **iTLC Configurator.** This component can update traffic engineering related parameters in the ITSApp component of the iVRI. It reads VLOG data from the VLOG Archive to allow the user to identify the appropriate parameters to change.

- **VLOG Viewer**. This component allows users at the road authority to visualize the rich log data of the iTLC's stored in the VLOG Archive. This is useful to analyze if a certain iVRI is correctly functioning from a traffic engineering perspective.

- **Mobilidata Quality Monitor**. Tool intended for data scientist that want to analyze the quality of the information streams that Mobilidata is publishing for the different use cases. Does not rely on real-time data on the MI bus, but instead collects the data from the different archives.

5.9 Third Parties

These components are or will be developed by external parties and focus on producing raw data or realizing additional use cases through the Mobilidata platform. The following components are included in this package:

- **Extended Vehicle WebService**: a manufacturer-controlled server that provides ExVe or Sensoris information according to the ISO20078 standard.

- **External Information Provider**: A placeholder for a service that injects data owned by a third party in the Mobilidata ecosystem to be used by others (e.g. weather, event information).

- **Historical Data Consumer**: a placeholder for a service that uses historical information from the Archive component for analytical purposes (e.g. measuring the effects of certain applications on traffic).

5.10 Federation

Through the II interface also defined in C-Roads, it is possible for the Mobilidata Interchange to federate with External Interchanges of other road authorities. As a result, Service Providers retrieving data for the Flemish region from the Mobilidata Interchange will easily be able to also subscribe to other message streams coming from other road authorities in the federation. Or the

data of those other areas will flow through the Mobilidata Interchange to the Service Provider so that it only needs to maintain that one MI connection to the Interchange of Mobilidata. Or the Service Provider will be automatically redirected to the other Interchange(s) in the federation where it can automatically retrieve the desired messages directly.

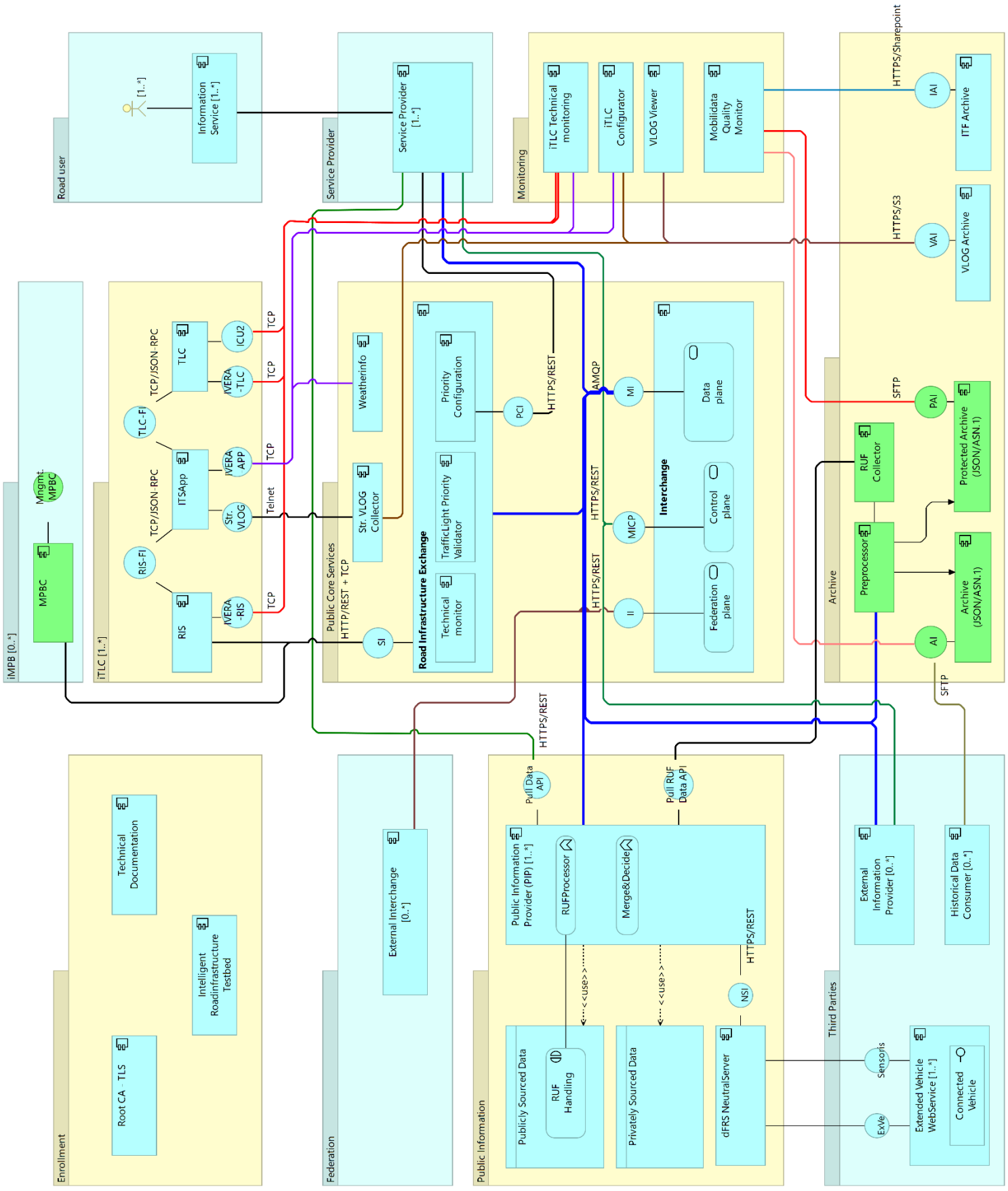
5.11 Enrollment

The three components in the architecture overview are not part of the technical Mobilidata environment but part of the AWV certificate authority/governance environment, ensuring integrity and independency. The components are:

- **Root CA - TLS**: The certificate authority server of the Flemish Government for X.509 certificates.

- **Technical Documentation**: website where all parties interested in joining the Mobilidata ecosystem can find as much documentation as possible. It can be found on https://documentation.mobilidata.be/

- **Intelligent Roadinfrastructure Testbed**: this is an environment that allows testing and certification of iTLC related components in a safe manner. I can provide any developer a temporary lab setup of a fully working end-2-end complete Mobilidata deployment of a real iTLC (located in a lab, not on the road), Road Inrastructure Exchange, Interchange, Service Provider and Information Service. More information can be found on https://dev-ivri-portal.ilabt.imec.be/


Road user
Information Service [1..*]
[1..*]
Service Provider
Service Provider [1..*]
Monitoring
iTLC Technical monitoring
iTLC Configurator
VLOG Viewer
Mobilidata Quality Monitor
HTTPS/Sharepoint
IAI
ITF Archive
HTTPS/S3
VAI
VLOG Archive
iMPB [0..*]
Mngmt. MPBC
MPBC
iTLC [1..*]
TLC-FI
TCP/JSON-RPC
TLC
iCU2
iVERA -TLC
TCP
RIS-FI
ITSApp
iVERA APP
Str. VLOG
Telnet
RIS
iVERA -RIS
Public Core Services
HTTP/REST + TCP
Weatherinfo
Str. VLOG Collector
SI
Road Infrastructure Exchange
Priority Configuration
TrafficLight Priority Validator
Technical monitor
PCI
HTTPS/REST
AMQP
MI
MICP
II
Interchange
Data plane
Control plane
Federation plane
Archive
SFTP
PAI
Protected Archive (JSON/ASN.1)
RUF Collector
Preprocessor
AI
Archive (JSON/ASN.1)
Enrollment
Technical Documentation
Intelligent Roadinfrastructure Testbed
Root CA - TLS
Federation
External Interchange [0..*]
Public Information
Pull Data API
Pull RUF Data API
Public Information Provider (PIP) [1..*]
RUFProcessor
Merge&Decide
<<use>>
Publicly Sourced Data
RUF Handling
Privately Sourced Data
dFRS NeutralServer
NSI
Third Parties
External Information Provider [0..*]
Historical Data Consumer [0..*]
Sensoris
ExVe
Extended Vehicle WebService [1..*]
Connected Vehicle