

THE MASTERPLAN

federative network of platforms concept

Final Version

FEDeRATED MILESTONE 14

29 February 2024

www.federatedplatforms.eu



Co-financed by the Connecting Europe
Facility of the European Union



EU DIGITAL SINGLE MARKET
EU SUSTAINABLE AND SMART MOBILITY
EU DATA SPACES (incl. MOBILITY DATA SPACE)

DIGITAL TRANSPORT AND LOGISTICS FORUM (DTLF)

PLUG & PLAY

FEDERATION

TECHNOLOGY INDEPENDENT SERVICES

SAFE, SECURE, TRUST

FEDeRATED CORE OPERATING FRAMEWORK

DATA QUALITY

OPEN & NEUTRAL

TRUST

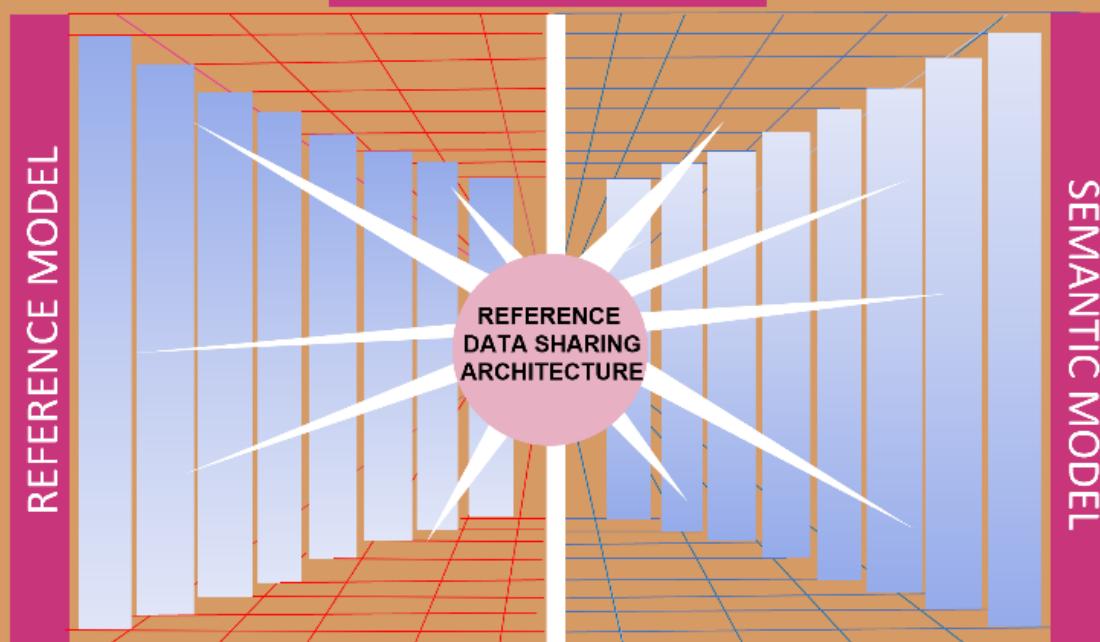
INTEROPERABILITY

DATA SOUVEREIGNTY

LEADING PRINCIPLES

THE PHYSICAL WORLD

REFERENCE MODEL



SEMANTIC MODEL

THE VIRTUAL WORLD

OPERATIONS

OPERATIONAL
FRAMEWORK

IT SOFTWARE

VALIDATED MASTERPLAN - NODE PROTOTYPE

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the FEDeRATED project consortium and can in no way be taken to reflect the views of the European Union.





EXECUTIVE SUMMARY

The FEDeRATED Action was tasked to develop a Master Plan setting out the organisational and functional requirements and the technical specifications – together called the operational framework - to enable the federated network of platforms concept taking shape.

The reason for applying digital technology in transport and logistics is to resolve current bottlenecks in the physical world focussing on real-time data sharing and supporting logistics innovations (like the Physical Internet). The bottlenecks are:

- No common language;
- No level playing field;
- Insufficient interoperability.

With the purpose to apply digital technology for solving these bottlenecks, the DTLF has developed the federative network of platforms concept, stressing the need for data sharing, identifying 4 building blocks - design principles - that require operationalisation:

1. Plug and play;
2. Technology independent services;
3. Federation;
4. Safe, secure and trusted.

Based on these building blocks, FEDeRATED developed a Core Operating Framework (COF). The COF guided the further development of the federative network of platforms concept, identifying the elements (setting the foundations) for federated (real-time) data sharing, being:

1. Ensure data sovereignty;
2. Create trust among all stakeholders;
3. Provide a framework to enable interoperability;
4. Be open and neutral to any participating party;
5. Ensure data quality.

The 4 DTLF building blocks and the Core Operating Framework combined resulted in a Vision document defining the federative network of platform concept to **provide for an infrastructure provision containing a set of agreements and technical applications to enable data in existing IT systems (platforms) of companies and public administrations to become available to authorized users through a publish and subscribe approach.**

Based on the above, **Leading Principles** were established to detail the infrastructure provision to take shape. The federative network of platform concept, branded as federated data sharing, is about data accessibility (pull data) by authorized users to:

- Make data-based logistics feasible for all stakeholders;
- Develop - just like one internet, made up of many different networks and services - one (common) data sharing grid where all data users and holders can qualify – based on a set of capabilities - as a node. The market that this will unlock will be much bigger than any of them could create alone;





- Provide any stakeholder the freedom to safely browse the (data sharing) grid: to explore new business opportunities, conduct data-based business transactions and compliance procedure, under the condition of safeguarding data autonomy;

The federated data sharing design is based on the notion of interoperable Nodes, enabling platforms and organisations to become fully interoperable.

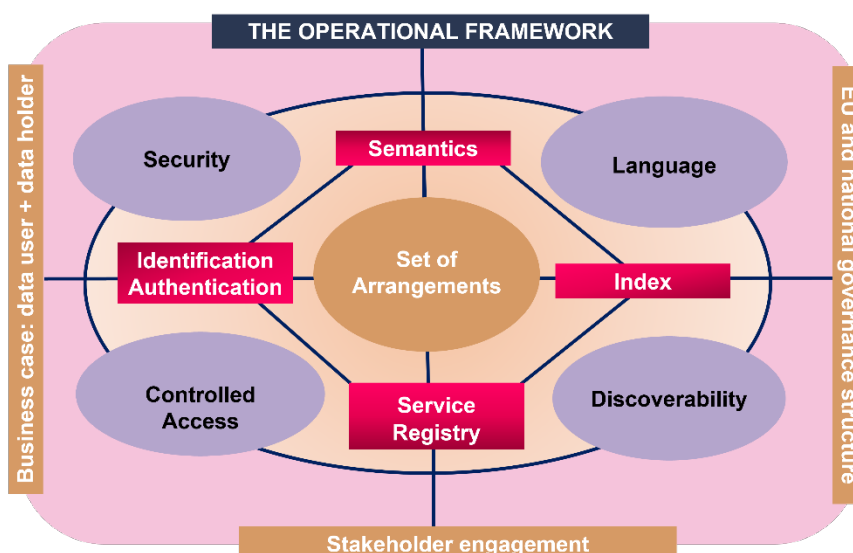
In 2020, the Leading Principles were incorporated in the **Interim Master Plan** - which also covers technical components, a reference model, security provisions and an approach towards semantic interoperability.

From 2020-2023, the Interim Master Plan was validated (tested) in **Living Labs** covering numerous use cases covering all transport modes and a wide variety of stakeholders located all over the EU and some third countries.

Based on the Living Labs experience, **lessons learnt** have been recorded. It can be concluded that many stakeholders are hesitant to transition their often bilateral, and propriety-based data sharing practices towards federated data sharing. The major reasons being:

- The logistics market lacks full understanding of the advantages federated data sharing might bring, especially as many stakeholders have only just begun engaging with digital technology in their operations;
- The federative network of platforms concept is difficult to understand, requiring a rather holistic mindset;
- A multi-stakeholder business case is difficult as there is a constant questioning on the why and how, what is profitable for my business and why opening my IT system for other partners than one does normally do business with;
- There is no legal obligation to share data, especially not beyond the scope of known partners in a propriety data environment.

An **Operational Framework** for federated data sharing has been established based on the lessons learnt. This Operational Framework sets the requirements to realize federated (decentralized) real time (pull) data availability for authorized users for seamless multimodal freight transport and logistics.





From an organisational perspective federated data sharing starts with organisations willing to do business with one another and/or fulfilling compliance procedures accordingly.

A. The organisational requirements are:

1. Stakeholder engagement - identification, interaction, and involvement.
2. Valid business cases based on data exchanges between data users and data holders.
3. An EU and national governance structure, including a set of agreements¹ on:
 - a. the collaboration between the stakeholders.
 - b. installing and maintaining hardware and software.
 - c. a manual on how to hold and use the data, also for providing services and fulfilling compliance procedures.

When organisations start sharing data in a federated way this will be done within the context of the infrastructure provision.

B. The functional requirements of the infrastructure provision refer to the need for:

1. "Common" language – the semantics and interaction order (process choreography) for data processing by heterogeneous systems or platforms.
2. Discoverability of business services – it is about being able to search and find (query) service providers and data that an organisation needs for its tasks. The latter is filled in with 'Linked Data': an organisation receives a link to data as an indication of the data they may access.
3. Security for all participants - to provide trust for all participants.
4. Controlled Access to all participants – enabling any company to give another company or competent authorities access to data that either the company is willing to make available to others or need to provide in accordance with legislation. This can be done through open data or via links that have been shared. In practice, this access will be limited, thus controlled access.

The infrastructure provision can only be developed based on the capabilities of its participants to participate.

C. The technical specifications – capabilities - for any data holder or user to participate are:

1. Apply the semantic web technology and a common semantic model (Semantic adapter).
Semantics - discussed in the context of semantic web, instead of modelling data – can add contextual meaning around data so it can be better understood, searched, and shared within supply chains, full of varied and complex logistic operations and compliance procedures.
2. Apply a Service Registry – enabling organisations to formulate their capabilities, specify the maximum of queries, events, and digital twins they can support, identify the infrastructure they use, and the business service(s) they require or support.
3. Deploy an Index – providing any participating organisation a transparent overview of the event-based data being available to share for conducting business and administrative compliance procedures.

¹ A set of agreements can be structured in various ways like Legal acts, Standards, proprietary Terms of Use, bilateral/multilateral Set of Agreements or legal contracts. Can also be a combination. Based on technology developments, these requirements and specifications will be constantly updated.





4. Utilize an Identification and Authentication (IA) infrastructure – the unique identification and authentication of an organisation and its authority granted by a recognized registration authority.

This Master Plan integrates the Operational Framework, which requires customization and has been validated against the FEDeRATED Living Labs². The Master Plan details the infrastructure provision as well as the capabilities, whereby stakeholder engagement has been given a prominent place. The Master Plan also provides tools on what is required to kick start the federative network of platforms concept.

The Master Plan supports the **four DTLF building blocks** as follows:

1. Plug and play – service customization is the recommended way for realizing plug and play. It results in a ‘profile’. This concept is introduced in section 5.3, underpinning the Service Registry. A profile is part of a Verifiable Credential (section 5.5), is matched during data sharing (section 5.4.2) and configures the index APIs (section 5.4.3).
2. Technology independent services – this is about service development by the Service Registry (section 5.3) for business activities (section 5.2.4). Examples of required services are given in section 5.3.2.
3. Federation – this is the core of this Master Plan. All relevant aspects are described to create a ‘federative network of platforms’.
4. Safe, secure, and trusted – this is about Identity and Authentication (section 5.5), access control (section 5.3.1), authorization (section 5.4.1), and governance, which is given as a recommendation (section 9.2).

The Master Plan facilitates **paperless transport**, like eCMR and AWB, and eFTI. Semantics (section 5.2) is based on best practices and standards. The Service Registry supports the specification of an eFTI data set (section 5.3.1) and the data sharing pattern (section 5.4.2) of the Index functionality supports sharing events with links to data sets, e.g. eFTI. The Index APIs (section 5.4.3) can be configured by the Service Registry for paperless transport.

Support of existing (or newly developed) **standards** is via the semantic adapter (section 5.6). It requires alignment of these standards with the FEDeRATED semantic model (section 5.2.1) to identify those elements that need to be supported by standards for data transformation. By expressing standards in the FEDeRATED semantic model, services are created (Technology Independent Services) that can be implemented as profile by an organization (Plug and Play).

Moreover, the Master Plan provides guidance in expressing standards, data sets for paperless transport (like eCMR/eFTI), and visibility events in the semantic model (section 5.3.3).

A **FEDeRATED Node prototype** has been developed.³ The Node prototype provides generic open-APIs for the Index, the **Index APIs**. These Index APIs are configurable with a first version of the Service Registry. These configurations, based on the semantic model, can be made for any use

² While executing a federated data sharing use case, a two-way street, or rather integrated, approach is necessary. IT capabilities should be demonstrated as well as a governance structure - a set of agreements on what is to be pursued as a business case, like services or legal compliance, between the parties involved.

³ Installation and configuration instructions are available on the FEDeRATED Github page: <https://github.com/Federated-BDI/Docker-BDI-Node>





case.⁴ The Index APIs also enable continuous improvements of the Node to meet latest data sharing requirements⁵ and makes the infrastructure provision fully programmable for arbitrary data sharing services. To achieve this, the capabilities need to be based on a pull approach.

The Node prototype and other FEDeRATED provisions are Open Source. In total they can be applied implementing the eFTI Regulation towards a future proof data sharing approach.

In the final year of the project, various LivingLabs used the FEDeRATED Node prototype enabling several LLs to connect with one another in a common pilot via the Index APIs, applying the FEDeRATED semantic model and a specimen of a Service Registry – semantic treehouse.

This Master Plan describes an **implementation path**, enabling customization integrating the required various capabilities and provided tools into their business cases, and provides an assessment framework to validate federated data sharing initiatives.

An EU cohesive strategy is required to structurally enhance the EU operational brainpower for federated data sharing. Thereto some **recommendations** are provided:

1. Adoption of this Master Plan by the DTLF as a basis for putting an operational framework for a federated network of platforms in place.
2. Development of a governance policy by DTLF balancing different aspects for optimal adoption, namely:
 - a. Governance organisation and the potential future role of the DTLF.
 - b. Standardization of the semantic model (upper ontology) that is the core for capabilities, and the Index APIs.
 - c. Open-Source project for ongoing development and alignment of the FEDeRATED prototypes with data space solutions.
3. To set up an adoption program focussing on first movers and EC regulatory bodies, for instance via EDIC for the European Mobility Data Space (EMDS).
4. Development of a cohesive research and innovation program via DTLF for continuous improvement of the infrastructure provision with supply and logistics innovations.
5. Development of an EU Regulatory Framework for data sharing in supply and logistics, optimally applying existing EU Legal Acts.

Independent of these recommendations, enterprises can use the Master Plan for interfacing with customers and service providers. Innovative software and service providers can develop innovative services and solutions. All based on hiding complexity via (a variant of) the configurable Index APIs.

⁴ Configurations can support Technology Independent Services and/or profiles. The latter is the plug and play building block of the DTLF. With these configurable Index APIs, organisations can already start implementing a Node.

⁵ The GAIA-X initiative has developed the API Gateway concept, which shields the complexity of many APIs at source systems (e.g. from data holders) and offers 1 set of APIs. This is similar to what the Index API, proposed in this Masterplan. However, there are two differences: 1) In the API Index one set of APIs is generic and configurable, while in their approach different applications give different APIs. 2) FEDeRATED offer semantics: which sets it apart (also on the GUI). The configuration of generic (Index) APIs from semantics makes it possible only 1 API needs to be added to the index to work with the Data Space Connectors, e.g. publishing data sets. This is a POST Data API. In addition, the Service Registry must publish a structure of that dataset (which is already possible) and the implementation of this API must inform data users via a pub/sub mechanism that there is new data.





TABLE OF CONTENT

EXECUTIVE SUMMARY.....	2
INTRODUCTION.....	10
Scope of the FEDeRATED Master Plan	10
How to use the Master Plan	10
How to read the Master Plan.....	10
Supporting documents.....	11
The steps being taken towards developing this Master Plan	12
1 CONTEXT	13
1.1 The virtualization of transport.....	13
1.2 The EU policy development.....	13
1.3 Digital Transformation in the EU supply chain	14
1.4 The stakeholders.....	17
2 UPDATING THE INTERIM MASTER PLAN.....	18
2.1 The major lessons learnt.....	18
2.2 Adjustments based on the Lessons learnt.....	19
3 THE LEADING PRINCIPLES.....	20
3.1 Introduction.....	20
3.2 The principles.....	20
3.3 Compliance with existing rules.....	27
4 THE INFRASTRUCTURE PROVISION	28
4.1 The objective of an infrastructure provision	28
4.2 The concept of the infrastructure provision.....	28
4.3 Services of the infrastructure provision.....	29
4.3.1 Services for enterprises.....	29
4.3.2 Services for authorities towards supply chains	29
4.4 Functional requirements.....	30
5 STAKEHOLDER CAPABILITIES	31
5.1 Capabilities	31
5.1.1 The capabilities	31
5.1.2 Relations between the capabilities	31
5.1.3 Baseline standards for capabilities and their interfaces.....	32
5.2 Semantics	33





5.2.1	Baseline structure of the semantic model.....	33
5.2.2	Baseline standards for semantics	34
5.2.3	Best practices.....	34
5.2.4	Logistics business activities.....	35
5.3	Service registry	37
5.3.1	Functionality.....	37
5.3.2	Services.....	38
5.3.3	Data structures of services	39
5.4	Index functionality.....	42
5.4.1	Functionality.....	42
5.4.2	Data sharing pattern.....	43
5.4.3	Index APIs.....	44
5.5	Identity and Authentication (IA).....	45
5.6	The semantic adapter.....	46
5.6.1	Functionality.....	46
5.6.2	Interfacing with other standards.....	47
5.7	Identifications.....	47
5.8	Assessing the LivingLab (technical) capabilities	48
6	IMPLEMENTATION CONSIDERATIONS	53
6.1.1	Data versus document-oriented approach.....	53
6.1.2	Data at source.....	53
6.1.3	Data sharing mechanisms	53
6.2	Implementation variants of the Index.....	53
6.3	openAPIs with IT applications.....	55
6.3.1	Service APIs	55
6.3.2	Profile APIs.....	56
6.3.3	Query API	56
6.3.4	Infrastructure Support Service (ISS) APIs	56
6.3.5	Information Service (IS) APIs.....	56
7	ORGANISATIONAL ISSUES.....	58
7.1	Roles and responsibilities.....	58
7.2	Distributed Service Development and - Customization.....	60
7.3	Adoption.....	61





7.4	Migration path	62
7.4.1	Migration strategy.....	63
7.4.2	Community migration – capability development.....	63
7.4.3	End-user migration.....	64
7.4.4	General observations	65
7.4.5	Considerations for a pilot / Living Lab.....	66
8	NON-FUNCTIONAL REQUIREMENTS	68
8.1	Non-functional requirements for end-users.....	68
8.2	Non-functional requirements to the network	69
9	RECOMMENDATIONS.....	70
9.1	Adoption of this Master Plan by DTLF.....	70
9.2	Governance policy developed by DTLF.....	71
9.3	Adoption by first movers	72
9.4	Research and innovation.....	72
9.5	EU regulatory framework.....	73
ANNEX 1 THREE TYPES OF DATA SHARING.....		75
ANNEX 2 DIGITAL COMPETENCE.....		78
ANNEX 3 NODE INSTALLATION.....		80
.....		81





INTRODUCTION

Scope of the FEDeRATED Master Plan

The DTLF has developed the federative network of platforms concept. Its' goal is to enable seamless data sharing for B2G, G2B, G2G and B2B. The FEDeRATED Action was tasked to deliver a validated Master Plan to set the EU federative network of platform concept in operational motion.

This Master Plan aims to present the functional, technical and organisational requirements to be implemented with respect to the federative network of platforms concept. The major question this Master Plan tries to answer is: ***How to build a future proof data sharing infrastructure provision for freight transport and logistics in the EU?*** The answer to this question is based on shared knowledge, consultation, coordination, human resource management, validation through pilot projects and living labs and openness towards different appreciations on how to effectively build this infrastructure provision. Within this process, an Interim Master Plan was developed in 2020 and applied by 23 Living Labs, running numerous use cases, generating knowledge that was fed into the current Master Plan.

This Master Plan is the result of validation of the Interim Master Plan against various Living Labs being developed and executed within the context of the FEDeRATED Action and the DTLF framework (EU Digital Transport and Logistics Forum). The validation process resulted in development of an Operational Framework which contains specifics on the organisational and functional requirements and technical specifications for federated data sharing. A specific Reference Architecture document was also developed, available as addendum..

How to use the Master Plan

This Master Plan can be used:

- to interact and commit many stakeholders to engage in federated data sharing practices;
- for policy people to base its data driven logistics policy on, for legislative as well as re-search and implementation guidance purposes;
- for software developers and research institutions to use the links to OpenSource software for further action.

How to read the Master Plan

The Master Plan contains the following chapters:

1. The context.
2. Updating the Interim Master Plan.
3. The leading principles.
4. The infrastructure provision.
5. Stakeholder capabilities.
6. Implementation.
7. Organisational issues.
8. Non-functional requirements.





9. Recommendations.

Three annexes are included. As addendum, you can access a(click on) a [Reference Architecture](#) document.

Supporting documents

The following documents, which provide additional information, are available on the FEDeRATED website (www.federatedplatforms.eu) for further consultation, also supporting this Master Plan:

- [Vision](#), (2019) including the Core Operating Framework
- [Interim Master Plan](#), (2020) and Annexes
- LivingLabs (since 2019), including:
 1. [Scoping](#)
 2. [Human touch \(interviews\)](#)
 3. [Testing framework](#)
 4. [Common Living Lab](#)
 5. [Assessment Framework](#) (2023 - LivingLabs validation criteria)
 6. [The Soul of the Machine](#) - an account of 5 years developing FEDeRATED Living Labs
- [Semantic interoperability](#), since 2020, including:
 1. [Ontology Engineering](#)
 2. [Semantic Model](#)
 3. [FEDeRATED Semantic Model - Development Portal](#)
- Technical interoperability, since 2019:
 1. [Technical Interoperability](#)
 2. [Reference Architecture](#)
 3. [Elements of Building](#) brochure
 4. [Multimodal Visibility Service](#)
 5. FEDeRATED Node Prototype development, (since 2020) including:
 1. [Node prototype and installation, incl codes](#).
The latest version of the node prototype and updated documentation can be found at: <https://github.com/Federated-BDI/FEDeRATED-BDI>
Updated Docker installation instructions are available at: <https://github.com/Federated-BDI/Docker-BDI-Node>
 2. [Service Registry](#) (semantic treehouse) see also [presentation](#)
 3. [Multimodal Visibility Infrastructure - Hackathon 25-26 October 2024](#)
 4. [Multimodal Visibility Service](#)
- Legal interoperability, since 2021:
 - [Legal Interoperability](#)
 - [An informal sketch assisting the development of a possible EU Communication and proposal for a Regulation on enhancing supply chain visibility](#) – (NON-PAPER, not committing the FEDeRATED partners)

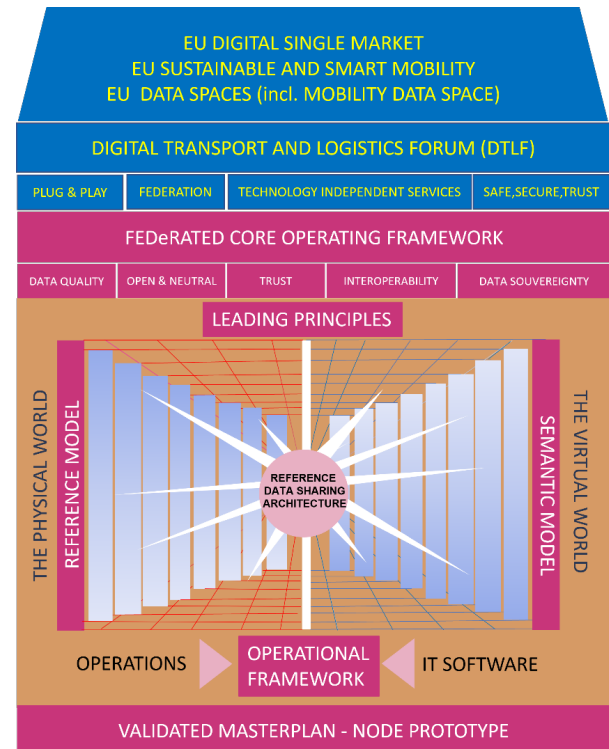




The steps being taken towards developing this Master Plan

The illustration hereunder provides an overview of the steps taken by the FEDeRATED project to develop this Master Plan.

Based on the combined EU transport and data policy, the DTLF Building blocks were developed. The FEDeRATED Core Operation Framework served to define Leading Principles. These leading principles were connecting to real life Living Lab use cases, that were to be structured into digital twins (engineered on a reference model), preferably applying a (or the FEDeRATED) Semantic model. This semantic model serves to align various unimodal transport standards to allow for smooth data transmission for multi modal transport cross border operations. Based on the experience gained, the Leading Principles were translated into operational guidance – the Operational Framework. This Operational Framework constitutes the basis of this Validated Master Plan and a prototype on how federated data sharing can be achieved in due time. To advance, the Master Plan and prototype need further assessment and experimenting in the real world, whereby a governance - possibly framed within as an EU Rule of Law, could serve as a safety belt for stakeholders to find the courage to seek collaborative innovation.



1 CONTEXT

1.1 The virtualization of transport

The importance of digital technology in our society and economies is growing. Over the last two decades, data sharing has become increasingly important. Public transport policy strategies have indicated the need to synergize the data requirements requested in the public and private domain. Legislation was developed in direct response to these strategies. Instant economics, the call for real time data exchange between all stakeholders in the supply chain enabling multiple objectives, not in the least visibility, is becoming a reality.

The need and use of seamless transport and logistics operations, including its potential to substantially contribute to sustainability goals, i.e. recently the EC Green Deal, have been stressed in various policy documents. The policy development towards the greening of transport and the development of a suitable infrastructure to make this happen go together.

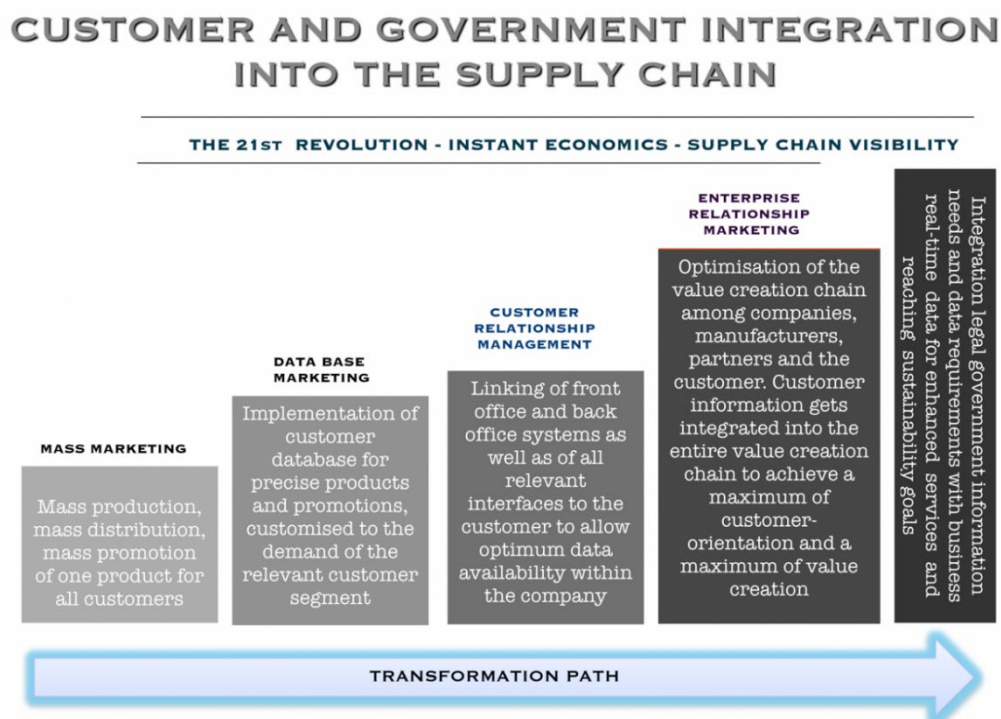


Figure 1 The digitization process of the supply chain – from mass marketing to supply chain visibility

1.2 The EU policy development

Some major EU freight transport and logistics policy developments in relation to digital technology are:

- The EU and national policy and business practices aim to deliver seamless multimodal freight transport operations.



- The European Union pursues a sustainable and smart transport agenda, also in connection with developing an EU Digital Single Market. For that purpose, the European Commission initiated various policy initiatives, such as the EU Digital Transport and Logistics Forum (DTLF⁶), an expert group, and the EU Data Strategy⁷.
- The EU DTLF has developed two interconnected policy perspectives: subgroup 1 on electronic transport documents, which led to the Regulation on electronic Freight Transport Information (2020/1056) and Subgroup 2, on Corridor Management Information (subgroup 2). Subgroup 2 aims to create an open, neutral and trusted data sharing infrastructure that can be applied by all logistics stakeholders with the so-called 'federated network of platforms' approach. The DTLF approach is supported in the EU Data strategy, that has proposed the concept of data spaces.
- Data spaces are decentralized infrastructures, where diverse actors can share and use data in a secure, reliable, and trustworthy manner, following governance, organisational, regulatory, and technical mechanisms. They will interact various data ecosystems in a demand-driven process⁸.
- For logistics, the DTLF and Data Space approach should preferably converge in an EU Mobility Data Space (EMDS), which should also cover passenger transport.

A digital infrastructure can solve current bottlenecks in the physical world, also by creating a digital twin. In the world of digital twins and data space, the things we talk about today like documents, cargo, routes, bookings etc. will be details. The constructed digital twins will take this to a whole new level with new business models, opportunities, and challenges. By then, a printed cargo manifest will look as cute as your grandfather's pocket watch. Digital twins and data spaces are the next frontier in logistics and transport. (see website – [Digital twin in freight transport and logistics \(federatedplatforms.eu\)](https://digitaltwinplatforms.eu))

1.3 Digital Transformation in the EU supply chain

The FEDeRATED Vision aims to develop a data sharing infrastructure provision that enables current bottlenecks in the physical world to be resolved through data sharing and support logistics innovations (like the Physical Internet). This digital transformation requires the use and integration of digital technologies into existing (and new) business processes as well as the four layers of the European Interoperability Framework (EIF), namely:

- **Technical interoperability**, covering applications and infrastructures linking systems and services. Including Interface specifications, data integration, exchange and interconnection services, and secure communication protocols.

⁶ The DTLF is established in 2015 and acts as an expert group consisting of EU Member States and Industrial Stakeholder organisations representatives. raised and chaired by EC DG Move. The DTLF identified 4 building blocks for federated network of platforms: plug and play, independent technology services, federation and safe, secure and trust.

⁷ The EU Data strategy related and led to several EU legal initiatives, such as the General Data Protection Regulation ePrivacy Regulation, Digital Operational Resilience Act, Data Governance Act, Digital Market Act, Digital Service Act, NIS2 Directive, Data Act, and Artificial Intelligence Act. New proposals are under preparation.

⁸ Source: EC Joint Research Centre (JRC). The data spaces principles are: Data sovereignty: Keep ownership and autonomy over data ; Security: Prioritize data security via encryption and ensure confidentiality ; Control: Revoke access at any time and retain control ; Interoperability: Consistent formatting and nomenclature enabling seamless integration ; Adaptability: By design, versatile and accommodating to various tech, use cases and industries





- **Semantic interoperability**, ensuring that the precise format and meaning of exchanged data and information is preserved and understood throughout.
- **Organisational interoperability**, documenting and integrating or aligning business processes and relevant information exchanged.
- **Legal interoperability**, ensuring that organisations operating under different legal frameworks, policies and strategies can work together.

The reason for applying digital technology in transport and logistics is to enable current bottlenecks in the physical world to be resolved focussing on data sharing and supporting logistics innovations (like the Physical Internet). Focussing on data sharing, DTLF has identified 4 design principles - building blocks - for developing a federated network of platform concept:

- **Plug and play** – each user should be able to register and connect to a platform of choice and select the services it needs.
- **Technology independent infrastructure services** - the services of the platform should be designed technology independent, thus enabling different providers to offer a solution that best fits their end-users and to support different technologies for realizing the services.
- **Federation** – the commodity will establish harmonized connectivity and interoperability of different solutions (platforms). It will consist of platforms of different service providers, whereas these platforms can also operate in an enterprise domain, thus creating so-called peer-to-peer solutions.
- **Trusted, safe and secure** – the commodity and its (integration with) end-users should be trusted, data sharing should be safe, secure and based on minimal central governance.

Based on these principles, FEDeRATED developed a Core Operating Framework⁹ guiding the further development of a federated network of platforms approach, constituting the following key principles:

1. **Ensure data sovereignty** – Data that is exchanged is made available by the data owner through a pull/push mechanism. The data then consumed is based on a push/pull mechanism. A data owner grants access to the data to the authorized recipient.
2. **Create trust among all stakeholders** - Any infrastructure provision¹⁰ facilitating data exchange should contain various mechanisms, services and solutions that contribute to trust in using the infrastructure. Not only should users be identified, but also particular active attacks to the complete infrastructure should be prevented (user requirements with respect to data sharing). Data privacy should also be respected.
3. **Provide a framework to enable interoperability** - to enable interoperability amongst all stakeholders, providing a level playing field, each user of the federated network of platforms should be able to do business digitally without making any additional data sharing agreements. There should be a mechanism during registration at which each organisation will be able to formulate its data sharing policies, expressed in their business services, timetables, voyage schemes, distribution patterns, and what you have. These mechanisms should be supported with results of the semantic interoperability layer (see before).

⁹ See FEDeRATED Vision Milestone 1

¹⁰ The FEDeRATED Core Operating Framework (COF) is also based on the need for establishing an infrastructure provision, see chapter 4





4. **Be open and neutral to any participating party.** The infrastructure provision for data sharing in supply and logistics should be open for anyone to use, be easily accessible for any parties, where each party can make the choice to implement the existing infrastructure provision themselves or connect to a platform that implements these agreements.
5. **Ensure data quality** - various dimensions, i.e., completeness, correctness, and consistency. Data quality also needs to be considered from different views. Data quality is required to meet all goals in supply chain synchronization, innovation, and other opportunities. Data correctness might be enforced based on more technical representations that can be implemented by IT systems. Enforcing data correctness will increase data quality but might decrease the data volume that is shared and made available to, for instance, authorities.

The 4 DTLF building blocks and the FEDeRATED Core Operating Framework combined resulted in identifying the need for establishing the foundations for an EU data sharing infrastructure provision. This was done through developing Leading Principles (see chapter 4).

The four DTLF design principles - Building Blocks - of the federative network of platforms

1. Plug and play - Features: Processes and data structures to support the registration of a user and the 'connection' of its organizations' IT back-office systems to integrate one or more selected Technology Independent Services. A public administration will indicate its data requirements for B2A data sharing with business. The 'connection' of IT back-office systems can be done by creating a user's organisation specific ontology. This will be based on or should be compatible with the ontology of the Technology Independent Services. This organisation's ontology would then be mapped to the IT back-office semantics, potentially by applying machine learning.

2. Technology independent infrastructure services. Features:

- Semantic model – an ontology supporting various standards of choice, modelling data to be shared between any two stakeholders in logistics, covering both B2B and B2A.
- Process – the sequenced interactions between any two stakeholders.
- Data – the minimal data set for each of the interactions identified in the processes. There may be variants to these data sets like mode specificity, commodity type specificity (e.g. reefer cargo, dangerous cargo), etc.
- Technical representation of the interactions. An example of this is Application Programming Interfaces supported with software code operating on a blockchain backbone.

3. Federation. Features: Various platforms and stakeholders' solutions will be integrated via common data sharing protocols based on API (application programming interface) and semantic data standards. An example of this could be a Blockchain backbone whereby each participant could implement a Big Chain DB node and become part of a cluster, or implement its own cluster, interconnect with other clusters by an InterLedger Protocol. To set up such an infrastructure the requirements of the various stakeholders of a Living lab should be assembled.

4. Trusted, safe and secure. Features: Developing Rules of engagement and behavioural rules; Requirements in terms of Identity and Authentication on an international scale will be collected; registration and access rights; data governance and monitoring; data quality -provenance, and – integrity; roaming aspects related to a designated point of entry; governance and certification of the technical infrastructure. Relations with (open) standards will be identified and potential for development of open standards.





1.4 The stakeholders

Implementing digital technology in freight transport and logistics covers various dimensions, thus stakeholder interests. To mention the most common:

1. Public authorities, policy as well as law enforcements agencies, inspections, Port administrations and Customs.
2. Supply and Logistic chain operators – terminal operators, transporters (seagoing maritime, rail, road hauliers, inland navigation, aviation), forwarders, shippers, sellers, consignors and buyers, private port operators.
3. IT companies (software and hardware).
4. Data sharing platforms e.g., Port Community Systems (PCSs) and supply chain visibility platforms.
5. Scientists and researchers.
6. Consultants.
7. Standardisation organisations (e.g. ISO, CEN, UN CEFACT, W3C, GS1).





2 UPDATING THE INTERIM MASTER PLAN

Mainly through Leading Principles and some technology concepts¹¹, the Interim Master Plan constitutes the requirements for data sharing in logistics, based on the need for data at source, decentralisation, open, neutral and safety. It challenged numerous LLs to answering the following questions:

- How to get the data in?
- What data are we dealing with?
- What data can be made available?
- How to safeguard the data (integrity, quality, authorisation)?
- Who can use the data?
- How to find the useful data?
- What can be done with the data?
- How to connect data to users?

The LivingLabs - developed and executed between 2019-2023 - covered various business cases, both in the private and public domain.

2.1 *The major lessons learnt.*

- The Leading Principles provide insufficient guidance for many stakeholders developing a federated based data sharing mechanism. Guidance should be offered.
- The federative network of platform concept is based on the power of pull – data availability – enabled by a neutral infrastructure provision. Based on this provision, services can be developed by ownership or storage. For platform service providers this is a very difficult concept to grasp, also appearing as countering their current business cases.¹²
- The concept of data at source resonates well with policy people. Within business processes it is not always easy how to technically apply, especially in connection to IT legacy systems.
- For many operators it is difficult to commit to data sharing, as trust is often lacking.
- In many business cases, stakeholders lack sufficient digital readiness – digitalization (paperless transport – getting from Analogue to Data) versus digitized (knowing how to apply digital technology).¹³
- The Leading Principles most difficult to achieve for many LLs related to making data available in M2M readable formats, data specifications and presenting various data requirements into one data set, making data searchable, and applying publish and subscribe mechanisms.
- P2P data sharing is feasible for most. Using a platform is the next step. Federated data sharing is a rather alien concept to many.

¹¹ See Milestone 2, Interim Masterplan

¹² Most business cases relate to P2P or using a Platform. Federated data sharing appears very abstract and alienating. See Annex 1 for three types of data sharing.

¹³ See Annex 2 Competences





- The concept of federated data sharing resonates, especially as it enables supply chain visibility. The condition to achieve this objective is to provide tangibility on the steps to take and technical tools to assist the stakeholders involved getting started.
- Without substantial public sector involvement or legal obligation stakeholders do not feel committed to structurally engage in federated data sharing.
- Stakeholders are confronted with a fragmented and confusing non-level playing field due to non-harmonized EU legal acts and policy incentives on logistics and supply chain, corporate social responsibility and data, leading to a proliferation of tools, services and research activities.

In short. There is hesitation getting into an operational level. A Master Plan, including some tools to get started, is required to provide guidance.

2.2 Adjustments based on the Lessons learnt

Based on the lessons learnt, the Interim Master Plan was adjusted to this Master Plan. One of the major lessons learnt was that developing and executing a federated data sharing use case requires a two-way street, or rather integrated, approach. The development of the technical setting and stakeholder engagement should be balanced. Based on the Living Labs validation more emphasis was given in this Master Plan to:

- **Stakeholder engagement.** Many Living Labs contributed a lot of time engaging a great variety of stakeholders. The experiences gained are covered in this Master Plan, especially chapters 7.3 and 7.4.4. textbox
- **Operational framework:** The operational framework was developed to make the Leading Principles more tangible, easier to comprehend.¹⁴ The operational framework provides the first stepping stones, which require customization (which is partly described in this Master Plan) in its implementation, possibly accommodated through an overarching EU federated network of platforms framework strategy (chapter 9).
- **Assessment framework.** The assessment framework serves to validate the technical setting, more concretely to test the capabilities developed and executed by the specific Living Labs. The assessment framework is elaborated in chapter 6.8. Its application on the FEDeRATED Living Labs is elaborated in Milestone 12 (Final testing Pilots/Living Labs)
- **Node development (technical tools):** The federated data sharing design is based on the notion of interoperable Nodes, enabling platforms and organisations to enjoy full interconnectivity. The Node is based on complying with the federated capabilities. A prototype of such a Node¹⁵ has been developed.¹⁶

¹⁴ Unlike physical infrastructure development, whereby you first must build the provision (road, rail etc) before people start to start to use it, a data sharing infrastructure provision can only evolve if there is enough logistics operators and public authorities sharing data in a federated way. Therefore, one must know what is required.

¹⁵ For the Installation and configuration: <https://github.com/Federated-BDI/Docker-BDI-Node>

¹⁶ See chapter 5.8. In practice, the LLs only started to experiment with the concept of the Node in the final year of the FEDeRATED project. Many LLs were rather working with gateways. The Node prototype challenged several LLs to connect with another in a common pilot applying the *FEDeRATED semantic model* and a Service Registry specimen – semantic treehouse.





3 THE LEADING PRINCIPLES

3.1 Introduction

The Leading Principles (LPs) serve as a guide to formulate the system boundaries, the services, and the functionality for the federative network of platforms concept. The LPs address the interfaces between individual organisations, which should be implemented by many organisations that what to share data through a federated approach. This also requires several considerations, such as the encoding for sharing data and/or the sharing of links, including the linked data approach. The LPs aim to provide tangibility answering the following questions:

- How to retrieve / receive the data (connectivity, linked data)
- What data are we dealing with (semantics)
- How to safeguard the data (integrity, quality, authorisation)
- Who can use the data (authorization)
- What data can be made available (access control)
- What can be done with the data (business process collaboration and compliance)
- How to connect data to users (identification and authentication)

3.2 The principles

The following table defines the LPs in relation to the Core Operating Framework elements, the DTLF

LEGENDA - The following columns are given:

- Principle – a brief name for the principle
- No. – a number for reference to the principle
- A sjhort description of the principle
- The building block of the DTLF Subgroup 2, consisting of 4 teams, to which the principle is linked. s:
 - 1 – Plug and play;
 - 2 – Technology independent services;
 - 3 – Federation of platforms;
 - 4 – Trusted, safe, and secure
- The key requirement(s) of the Core Operating Framework that are fulfilled by a principle. The key requirements are encoded as follows:
 - TR- Create **trust** among platforms and participants;
 - DS - Ensure **data sovereignty**;
 - IN - Provide a framework to enable **interoperability**;
 - ON - Be **open and neutral** to any participating party;
 - DQ - **Data quality**.
- The role to which a principle is applicable. These roles are identified in annex to this document. They are:
 - A – Authority;
 - E – Enterprise;
 - C - Customer;
 - SP – Service Provider;
 - DH – Data Holder;
 - DU – Data User.





design principles (also called building blocks), and the applicable roles. The Interim Master Plan contained 37 LSs. This table contains 36 LPs deleting the original LP13.

FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
Level Playing Field	1	All supply chain operators and public authorities involved in freight transport and logistics must be able to participate.	4	ON	E/A
Electronic/digital format	2	The information is to be encoded digitally, using a revisable structured format.	1 2 3	IN	DH/DU
		Principle 2 refers to technical interoperability. The information is to be encoded digitally, using a revisable structured format, which can be used directly for storage, and processing by computers, such a structured format for digitally encoded messages that can be transformed into for instance PDF. ¹⁷			
Compliance with existing rules	3	Data sharing must be compliant to existing legislation (e.g. GDPR) and privately agreed rules.	4	IN	E/A
		Principle 3 refers to legal interoperability			
Business service	4	Each participant must formulate the business service(s) it provides (service provider) or requires (customer).	1	IN	C/SP
		Principle 4 addresses organisational interoperability for enterprises			
Business relations	5	Trust between enterprises is primarily driven by their real work relationships.	4	TR IN	E
		E.g. an enterprise can trust a (known) service provider, but not necessarily another one with whom that enterprise did not do business			
Supply and logistics chains	6	The business relations between participants are shown according to their outsourcing hierarchy from the perspective of for instance a shipper and/or consignee based on services implemented by any two collaborating organisations.	2 3	IN	E
Data	7	The matching of the implementation of	1	IN	E

¹⁷ XML, EDIFACT, JSON(-LD), and RDF(s) are supported. Mail attached files, i.e. PDF, Excel, Access, and JPEG, are not supported





FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
requirements of enterprises		services and negotiation between a customer and service provider specify the data that they will share.			
	Principle 7 contributes to semantic interoperability and access control.				
Data requirements established by an authority	8	Data requirements set by an authority are related to the legislative basis afforded to that authority.	1	EN	A/E
	Principle 8 refers to legal interoperability and organisational interoperability for authorities				
Data processing	9	Any organisation can specify its internal processing.	1	TR ON	A/E
	E.g. outsourcing strategy (enterprises) or governance of cargo flows by risk assessment (authorities like customs).				
Fit for purpose	10	Public authorities that access enterprise data require a legal basis to refer to.	4	TR	A
	Principle 10 refers to legal- and organisational interoperability				
Publication of data requirements	11	Public authorities publish their data requirements in a machine-readable form.	1	TR IN	A
	Principle 11 iterates that public authorities publish these data requirements to enable rapid and consistent implementation of these requirements by enterprises, thus reducing errors and supporting rapid changes.				
Business Service Discovery	12	Business services of all enterprises are discoverable according to harmonized search criteria	1	IN ON	E
Authorities providing data (authority services)	13	Public authorities can share their data with enterprises for policy reasons within a legal framework	1	IN	A
	Principle 13 refers to legal interoperability and organisational interoperability for authorities				
Push/pull	14	A legally allowed data sharing mechanism has two choices: <ul style="list-style-type: none"> a push, data to be duplicated by enterprises to authorities; 	3	IN	A/E





FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
		<ul style="list-style-type: none"> a pull, data being made accessible to authorities. 			
		<p>Principle 14 is part of technical interoperability. In case a regulation does not prescribe a mechanism, the pull mechanism is preferred to prevent unnecessary data duplications and thus errors. A reporting data set is only virtual: it is not stored separately but extracted from all other data sets based on a data pull by an authority.</p> <p>The EMSWe (European Maritime Single Window environment) data set consists of additional data sets like passengers and waste, which is for further development. However, the EMSWe data set will be made available in a similar manner</p>			
Publish/subscribe	15	An organisation must have the ability to subscribe to any relevant new data in accordance with fit for purpose (public authority) or a commercial relationship (enterprise).	3	IN	A/E
		Principle 15 is part of technical interoperability. A data provider issues a unique link to the relevant data and will distribute data when it becomes available.			
Combining data requirements	16	Whenever a public authority is responsible for governance of more than one regulation, the data requirements of those regulations will be combined into one data set as much as possible.	1	IN	A
		Principle 16 refers to legal interoperability and organisational interoperability for authorities			
Identification of organisations	17	Each organisation must identify itself uniquely. This unique identification is preferably based on open standards and provided according to agreed attestations with transparent validation processes of these attestations (e.g. Chamber of Commerce Registration, AEO certificate).	1	TR	A/E
Identification of users	18	Identification and authentication of employees (or delegated persons) is the responsibility of individual organisations. Sharing these identifications outside an organisation is optional and decided by each organisation.	1	TR	A/E
User capabilities	19	The capabilities. i.e. the authorized actions that may be performed, of an identified user are governed by each organisation	1	IN	A/E





FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
		Principle 17, 18, and 19 refer to minimal requirements where each organisation is responsible for having an internal Identity and Access Management system (19 and 20) linked to authorization for users to apply an organisational identification (18) for data sharing with other organisations.			
Data sensitivity	20	Sensitive data should not be accessible or changed by unauthorized users or organisations.	4	TR	E
		Principle 20 implies access to data that is stored or shared via some solution/platform. is applicable to for instance commercial sensitive data. It also relates to non-repudiation (principle 35).			
Metadata of data sharing	21	Any metadata specifying which data is accessed or shared between any two enterprises is not accessible by unauthorised users or organisations.	4	TR	A/E
		Principle 21 addresses that business patterns can be derived from data shared between any two enterprises and should be hidden from third – non authorized - parties. It implies that metadata of data sharing between public authorities and enterprises is open data.			
Identification of systems	22	IT systems of an organisation that support the roles data holder and – user for any type of data, are uniquely identifiable e.g. by their end-point.	1	TR	
Data sharing policy	23	A common policy or agreement specifies the use and reuse of data as well as the way it is stored or removed.	4	DS	A/E
Data sovereignty	24	A data owner determines the data it will share and retains full rights and controls over this data. This can be based on its customization of services.	4	DS	DH
Data at source	25	Single sharing of links, multiple (controlled) access to data	1 2 3	IN	DH
		Principle 25 indicates that data should be stored at the source to prevent any duplication and potential errors, unless prescribed by a regulation or agreed upon by two organisations that share the data. To have data at the source, these organisations only share links to that data.			
Data sets	26	The data sets of which links can be shared is	2	IN	A/E





FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
Baseline standards		given by the services.			
	Principle 26 addresses semantic interoperability.				
	27	Use of baseline standard(s) that provide all common terminology, data formats, code values, etc. that can be re-used for implementation of the FEDeRATED models.	2 3	IN	DH / DU
Data timestamps	Principle 27 on baseline standards address for instance code values like ISO country codes, ISO standards for date/time formats and terminology with formats like specified in the UN CEFAC Core Component List				
	28	Links to data are shared with events that also provide data of the real-world state. These events have a timestamp of sharing and in case of the real-world state a timestamp when this state became actual.	2 3	IN	E
	Principle 28 identifies the need for difference between these timestamps to be small in the context of process synchronization				
Unique identifier(s) of data (sets)	29	Unique identifiers are used to create and share links of relevant data sets between any two enterprises.	3	IN	DH / DU
	Principle 29 identifies that unique identifiers might differ from identifiers used in the real-world, e.g. a container has a unique container number and can have a unique link for data sharing.				
Data sharing solution	30	Organisations select a solution of choice for data sharing with others (platform, peer-to-peer).	3	ON	A/E
Federation	31	Organisations can share or access data with others that use different platforms or solutions.	3	ON	A/E
	Principle 31 refers to the creation of a federated network of platforms as required by DTLF Subgroup 2.				
Data quality	32	Data is validated by a data holder and a – user against data sharing specifications.		DQ	DH / DU
	Principle 33 identifies that a data holder is only able to share data according to its specifications. These specifications can address completeness, correctness, and sequencing.				
Data Exchange	33	Accuracy and consistency of data over its	4	DS DQ	DH DU





FEDeRATED LEADING PRINCIPLES					
Principle	No.	Description	DTLF Building Blocks	Core Operating Framework	Role
integrity		entire lifecycle is required			
		Principle 34 identifies that the fundamental elements of trust in data are to ensure data audits and non-repudiation hitch. Data delivery must also be guaranteed to ensure trustworthy data exchange			
Historical data	34	Historical data sets are stored for optimizing business processes (public authorities and enterprises), based on legal requirements (e.g. archiving),			A/E
		Principle 34 iterates that data can also be used to support Research & Development and statistics.			
Non-repudiation	35	Organisations must be able to proof that data is shared or received as such (its integrity is assured). This is supported by a (shared) immutable log and audit trail of the data they have shared.	4	TR	A/E
Monitoring	36	Each organisation can trace with whom and at what time particular data has been accessed/shared with any other organisation. This is about accessibility of its logs and audit trail for internal purposes.	4	TR	A/E

The Leading Principles coverage of the DTLF building blocks is illustrated hereunder

No	DTLF Building Blocks	Applicable Leading Principles
1	Plug and play Each user should be able to register and connect to a platform of choice and select the services it needs.	2. Electronic/digital format 4. Business service 7. Data requirements of enterprises 8. Data requirements established by authorities 9. Data processing 11. Publication of data requirements 12. Business service discovery 13. Authorities providing data 16. Combining data requirements 17. Identification of organisations 18. Identification of users 19. User capabilities 22. Identification of systems 25. Data at source





No	DTLF Building Blocks	Applicable Leading Principles
2	Technology independent services the services of the platform should be designed technology independent, thus enabling different providers to offer a solution that best fits their end-users and to support different technologies for realizing the services.	2. Electronic/digital format 6. Supply chain 25. Data at source 26. Data sets 27. Baseline standards 28. Data timestamp
3	Federation of platforms To establish harmonized connectivity and interoperability of different solutions (platforms). It will consist of platforms of different service providers, whereas these platforms can also operate in an enterprise domain, thus creating so-called peer-to-peer solutions.	2. Electronic/digital format 6. Supply chain 14. Push/pull 15. Publish/subscribe 25. Data at source 27. Baseline standards 28. Data timestamp 29. Unique identifier(s) of data (sets) 30. Data sharing solution 31. Federation
4	Trusted, safe, and secure the commodity and its (integration with) end-users should be trusted, data sharing should be safe, secure and based on minimal central governance.	1. Level playing field 3. Compliance with existing rules 5. Business relations 10. Fit for purpose 20. Data sensitivity 21. Metadata of data sharing 23. Data sharing policies 24. Data sovereignty 33. Data exchange Integrity 35. Non reputation 36. Monitoring

3.3 Compliance with existing rules

The following aspects must be implemented by service development:

1. Personal data. EU Member States will ensure compliance with GDPR. The application of restrictions in the scope of the obligations and rights to secure specific national interests may vary between Member States.
2. Confidentiality and commercial data. The common perspective of the commercial data that must be kept confidential has to be identified. Mechanisms are required with respect to providing access to the data reported through the FEDeRATED infrastructure. The reported data is for authority use.
3. Any constraints on data sharing formulated by private or public agreements (e.g. the Hague-Visby rules). There are private and/or public agreed rules for data sharing that are constraints. These rules relate for instance to liability and responsibility. They imply that organisations do not have access to data to prevent for instance additional insurance fees (liability) and access to cargo content by unauthorized persons (theft).





4 THE INFRASTRUCTURE PROVISION

The leading principles were further developed into an operational framework for implementing the concept of a data sharing infrastructure provision. The infrastructure provision can be defined as **a set of agreements and technical applications to enable data in existing IT systems (platforms) of companies and public administrations to become available to authorized users through a publish and subscribe approach.**

4.1 *The objective of an infrastructure provision*

The infrastructure provision relates to all data sharing operations within the supply chain. It aims are to:

- Facilitate operators and public authorities to electronically receive or obtain information in respect of the legal obligations or the business process regarding cargo and transport movements in or connected to the EU.
- Allow electronic data sharing between a data holder and - user of the information; and,
- Identify and authorise different data holders and - users, and to safeguard data sovereignty.
- Facilitate data sharing between business and the various national competent authorities, either with consent of a data provider or within legal boundaries.
- Enable business and public authorities to access high quality data within a trusted environment.
- Empower all parties within the logistic chain to interconnect with one another to do business without discrimination.

The infrastructure provision fosters:

1. Smooth interaction between and among the different logistic chain operators and public administrations involved.
2. Enterprises to optimize their supply chains to achieve seamless goods flows.
3. Dynamic planning to enable various ways of collaboration and optimize capacity utilization.
4. Recognizing existing (partial) systems.
5. Streamlining multimodal transport.
6. Decreasing or removing costs derived from lack of interoperability.
7. Business process collaboration of organisations i.e., data accessibility for planning and optimization purposes and collaboration for compliant execution of physical activities.

4.2 *The concept of the infrastructure provision*

The applicability of the infrastructure provision is defined by its governance, which refers to a set of agreements, which can also have a legal status. The main concepts of the infrastructure provision are:

- Decoupling of implementation by one organisation from implementation by another for the same service.
- Runtime (re-)configuration.

These two concepts enable onboarding: each organisation can join and configure the provision





independent of another. A service implementation is part of the organisational identity, which can be tested and certified, and is the basis for supervision of legal agreements.

To ensure that these organisations are still able to share data - i.e., their service implementation can be matched - services are related to business activities like transport and transshipment performed by those organisations and published according to their business services.

These concepts also enable rapid deployment of new and all types of different services and communities to develop and deploy innovative services with the same infrastructure provision they apply for other services, resulting in cost reduction.

4.3 Services of the infrastructure provision

In supply chains, organisations share data to support and optimize their business processes compliant with regulations. Therefore, business process collaboration of organisations is considered and supported by the infrastructure provision. It addresses data accessibility for planning and optimization purposes and collaboration for compliant execution of physical activities. These are formulated as the (Technology Independent) Services of the FEDeRATED infrastructure provision.

4.3.1 Services for enterprises

The services the infrastructure provision can provide for enterprises are:

- Publish, search, and find business services, available capacity, timetables, etc. Business services must cover at least: transport, transshipment, and warehousing. Stuffing and stripping, cleansing, etc. are considered as additional and port (or hub) related services can be (obligatory) services like piloting and tugging (port).
- Booking and ordering.
- Sharing of predictions and changes of performing physical activities to synchronize these activities (supply chain visibility).
- Compliance with reporting requirements.
- Data accessibility for compliance and process optimization:
 - Access to applicable regulations and reporting formalities;
 - Access to any legal constraints for performing certain activities (e.g. time windows for city distribution in city centres);
 - Access to any third-party and/or authority data (like infrastructure availability) that is required for planning – and operational purposes (resilience).

4.3.2 Services for authorities towards supply chains

The services the infrastructure provision can provide for public authorities are:

- Border control for freight or passengers, with any means of transport ((deep sea/short sea) vessel, airplane, truck, barge, train).
- Safety and security including health inspection, infrastructure management, and customs.
- Data on movement of goods governed by regulations such as waste, hazardous goods.
- The ability to inspect any cargo and transport means at a requested or agreed location customs, (border) police, etc.
- Process control of transport means concerning safety, and security by the responsible authority(-ies).
- The process for monitoring traffic flows (safety) and accessing data of freight/passengers;





- Publication of any data to improve compliance of logistics processes with given legal constraints.

4.4 Functional requirements

The **functional requirements** of the infrastructure provision refer to the need for:

1. “Common” language – the semantics and interaction order (process choreography) for data processing by heterogeneous systems or platforms.
2. Discoverability of data – it is about being able to search and find (query) service providers and data that an organisation needs for its tasks. The latter is filled in with 'Linked Data': an organisation receives a link to data as an indication of the data they may access.
3. Security for all participants - to provide trust for all participants.
4. Controlled Access to all participants – enabling any company to give another company or competent authorities access to data that the company is willing to make.

These requirements are translated into the capabilities of the parties participating in the infrastructure provision.

Technically, the infrastructure provision should provide for:

- an Endpoint - unique identification (“address”) on a [platform](#) or [connector](#) enabling an [end-user](#) to share data with any other end-user having an endpoint.
- The unique identification of an end-user that can be authenticated (verified).

There to, the infrastructure provision should enable connection to be established through an:

- Adapter - implementing the Index functionality and a [connector](#) of an ICT system of a [data sharing steward](#)
- Connector – providing an [endpoint](#) for safe, reliable, and secure peer-to-peer data sharing services
- Gateway – implementing the Index functionality and a [connector](#) and providing a local interface tailored to requirements of a [data sharing steward](#)
- Node - implementing the Index functionality and a [connector](#) and providing Index APIs a [data sharing steward](#)



5 STAKEHOLDER CAPABILITIES

The infrastructure provision is based on applying the Leading Principles. Not all Leading Principles are applicable for all use cases, which means that (potentially) not all functionality of the key elements is fully exploited. However, to fully support all possible use cases, all functionality is described in this section.

5.1 Capabilities

5.1.1 The capabilities

To participate in and benefit from an infrastructure provision, its participants should be capable to comply with some technical specifications – capabilities – which are:

1. Semantics
2. Service Registry
3. Index
4. Identification and Authentication (IA – security perspective)

In addition to these capabilities, this section introduces a semantic adapter. Although it is not listed as a separate capability, a semantic adapter is required to adapt existing IT systems or (defacto) standards to semantics. One could call a semantic adapter a tool.

5.1.2 Relations between the capabilities

Semantics is at the core of the solution. It is fully implemented by the Index functionality, can be applied in the Service Registry for service development and service customization, and is used for discoverability and matching of data sharing capabilities of organisations based on their customization (their 'profile'). Authorisation and access control relate to service development and a profile, based on sharing (links to) data.

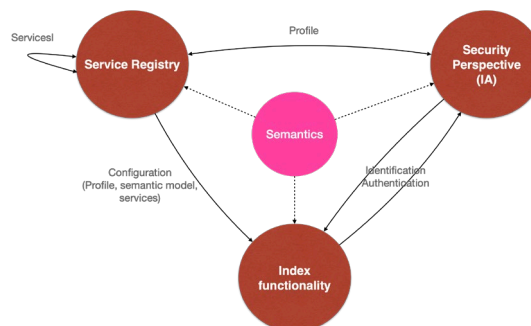


Figure 2 Relations between the various capabilities

In this chapter, the maximum and minimum functionality of the Service Registry, Index and Semantic Adapter are listed. Minimal functionality focusses on the need to fit into existing processes and IT systems that support part of the other functionality e.g., implementing framework contracts and/or (unstructured) person-to-person communication.

5.1.3 Baseline standards for capabilities and their interfaces

The semantic web standards of the World Wide Web Consortium (W3C) are the baseline standards for the multimodal ontology and interfaces between the capabilities of the infrastructure provision. They are applied as follows:

Interface	Description	Capabilities	Baseline standard
Ontology	Ontologies and their constraints	Service Registry – Service Registry Service Registry – Index	OWL (Ontology Web Language) SHACL (SHApE Constraint Language) SKOS (Simple Knowledge Organisation System) – for code lists only.
Service (process)	Specification of event sequencing	Service Registry – Service Registry Service Registry – Index	No standard available yet
Service (data)	Specification of event structures	Service Registry – Service Registry Service Registry – Index	SHACL
Profile	Customization of a service by an end-user	Service Registry – IA (Registration Authority) Service Registry – Index	SHACL
Business service	Discoverability of an end-user for the business services it can provide	Service Registry – Service Registry	SHACL
Data transformation	Configuration of the semantic adapter for data transformation	Service Registry – semantic adapter	RML (RDF Mapping Language)
Events and data	Sharing of events with links to data and accessing the data for those links	Index – Index	RDF (Resource Description Framework)
Queries	(complex) Queries for data retrieval	Index – Index	SPARQL (SPARQL Protocol and RDF Query Language)
Information services	Data made available by a data holder	Index – Index	Metadata standard (e.g. DCAT and/or Dublin Core) SHACL (data) ODRL (Open Document Rights Language, access rights).
Verifiable Credentials	Identity of an end-user that can be authenticated (verified) by another end-user	Registration Authority – Index Index – Index	Open standards (under development)

Interface	Description	Capabilities	Baseline standard
Authen-tication	A means to get author-ized access to data that can be verified (an alter-native for VCs)	Index – Index	OAuth2
Local interface	The integration of an IT backend system with an Index	IT backend – Index	OAS (openAPI Specification) Any others (JSON, XML, CSV or other syntaxes used for file ex-change)

There is a wide range of tooling, triple stores, and graph databases supporting RDF and OWL/SHACL.

For implementation of an SSI/VC based infrastructure open standards must be applied, preferably those relevant to eIDAS2.0, since that is expected to be implemented for business-to-government data sharing. The Architectural Reference Framework (ARF2.0) of eIDAS2.0 still needs to be extended with functionality required by supply and logistics (this is called the EMDS – European Mobility Data Space, see before).

5.2 Semantics

The essence of semantics is to specify machine-readable data to enable stakeholders in multimodal supply chains to exchange information digitally (data sharing in paperless transport). This relates to business transactions as well as compliance with regulations.

5.2.1 Baseline structure of the semantic model

Machine readable specifications of data are by applying semantic web standards like Ontology Web Language (OWL), Resource Description Framework (RDF), and SHACL Constraint Language (SHACL). Since all communities will have different (implementation guides of) standards with different structures, the multimodal ontology provides an alignment framework consisting of ‘Digital Twin’ and ‘event’:

- Digital Twin is a taxonomy of real-world objects (container, truck, barge, goods, livestock, etc.). The taxonomy is constructed by specialization, i.e. creating subtypes for a supertype, like a truck is a subtype of a transport means.
- Event is the association between at least two Digital Twins in time and space (past, present, and future, where future is ‘expected’, ‘planned/estimated’, and ‘required’ and present is ‘actual’). ‘Event’ reflects the state of the physical world (‘where are my goods’, ‘container track’, etc.) controlled by data sharing (‘my ETA is ...’, ‘this container must be loaded on that vessel’, etc.).

Any constraints between subtypes of Digital Twins are formulated on ‘event’ level and specified in SHACL. One of the basic constraints is ‘cargo’, like a container that can be cargo for a trailer and a trailer that can be cargo for a ferry. This makes the semantic model readable, flexible, and extensible to any new services. Any value constraints on data like those of weights or the format for representing a date and time are formulated by SHACL. Code lists are modelled separately.

The semantic model is modularized to increase its maintainability and re-use of existing ontologies.

Specific transport mode infrastructures, e.g. road or rail infrastructure, could be represented as ‘Digital Twin’. Within the FEDeRATED semantic model, it was chosen not to follow this route, but rather design infrastructure as a separate module in alignment with existing infrastructure ontologies developed and maintained by others.

Figure 3 visualizes the result of decomposition, including ‘legal entity’ and relevant financial and compliance concepts.

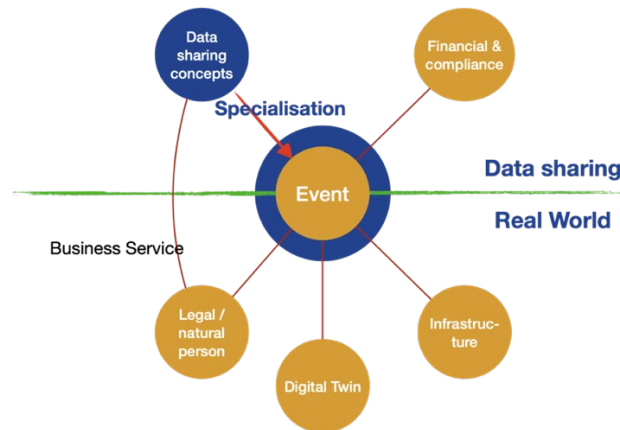


Figure 3 the multimodal ontology with details of business data sharing concepts

Figure 3 also introduces data sharing concepts as a separate model. This is about the interactions of a ‘service’ and their sequencing for business activities. An interaction or a business document is for instance represented by a subtype of event associating Digital Twins, locations, and organisations for a business activity. The data sharing concepts are also an ontology. The ‘Multimodal supply chain visibility’ document provides an example of these interactions for a service.

5.2.2 Baseline standards for semantics

The following baseline standards are identified for constructing the multimodal ontology:

- The United Nations Trade Data Elements Directory (UNTDDED) is a baseline vocabulary;
- The UN CEFAC Core Components Library provides a set of (composite) data types with formats;
- UN ECE Recommendations for all types of code values like packaging.
- ISO standards like the ones for country codes and date/time formats
- International adopted encoding schemes like those for container size and type, vessel types, etc.

Standards like UN CEFAC MMT (Multi Modal Transport model), WCO Data Model, GS1, EU Customs Data Model (EU-CDM), IATA ONE Record, Sea Traffic Management (STM), RIS (River Information Services), Port Collaborative Decision Making (PortCDM), and many others are built upon these baseline standards. Others like TAF TSI (rail) and Datex II (road traffic management) do not share these baseline standards (or only a very small subset).

Any data formats and their constraints are the basis for encoding schemes for data sharing and validation of this data.

5.2.3 Best practices

UN CEFAC and other standardization bodies have best practices that are adopted by the multimodal ontology and services, like:

- Measure unit specifiers – each measure must have a unit specifier of the SI system.
- Date/time format – although much software can automatically process a date/time format, it must be mentioned during data sharing. ISO date/time formats are applicable.
- Time zone – a date/time is linked to a time zone that must be mentioned. Time zones start at GMT (Greenwich Mean Time).
- Currencies – each currency must be mentioned, including an exchange rate with its date when a common currency is applied.
- Geo-coding – international coordinate system for encoding a location. Geo-coding can be attached to other location code values like the UN Location Codes and port numbering schemes for a port. Since there are different ways for geo-coding, the applicable way must be mentioned during data sharing.

Whereas the multimodal ontology covers all potential values, selection of these values must be done at service development level. This selection is also required for all code values like those of location codes. This reduces the number of options for service customization, thus contributing to interoperability.

5.2.4 Logistics business activities

In logistics, the following business activities are distinguished:

- *Logistics (core) activities*: e.g. transport, transshipment/cross-docking, (temporary) storage;
- *Value added activities*: e.g. (re-)packing/stuffing, unpacking/stripping, ironing (of textile), consignment grouping, vendor managed inventory;
- *Supporting physical activities*: e.g. vessel waste management, container cleaning.

These activities have various properties that are represented by events associating (in time) Digital Twins with infrastructure capabilities. For instance, a transport activity is about cargo (goods, containers, bulk, etc.) to be moved from one location to another, based on a customer's goal (expected times), a service provider's planning (planned or estimated times), and actual performance of the activity.

The core of these physical activities is convergence and divergence (Figure 4). Goods can be (re)packed (convergent activity), stuffed into containers, and loaded on transport means (all convergent operations) and unloaded, stripped, and unpacked (all divergent activities). These activities are supported by the semantic model via the event association.

Execution of these activities leads to all types of events, like load, unload, stuff, strip, arrive, and depart.

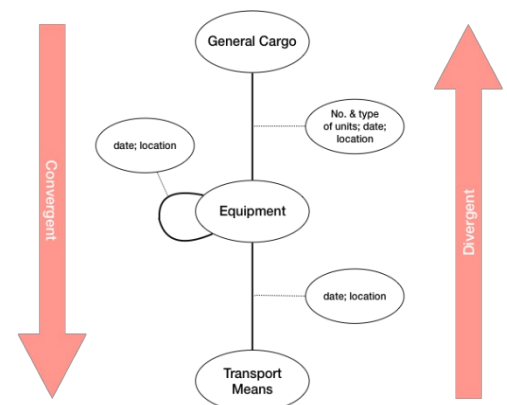


Figure 4 Particular operations reflected by their data perspective

Besides physical activities, many information processing are performed, utilizing data shared for physical activities. Examples of these activities are:



- *Handling of administrative procedures*: e.g. production of transport accompanying documents (certificate of origin, Bill of Lading, (e)CMR);
- *Handling of formal procedures*: e.g. financial (VAT), (food or product) safety, security, customs declaration;
- *Financial services*: e.g. insurance and logistics financing, billing and payment;
- *Infrastructure services*: services required for optimization of safe and secure capacity utilization of infrastructures, e.g. corridor management services, path allocation services, sea traffic management services, piloting services, and tugging services ;
- *Information services*: data required for optimization of logistics flows like traffic information services and forecasts, weather conditions and forecast, water depths, and forecast.

Separating data sharing concepts from real world concepts in different modules makes the semantic model applicable for supporting all types of services and use cases. Where these services or use cases may have their own terminology, these terms are (mostly) represented by the multimodal ontology.

The multimodal ontology can be viewed from different perspectives, based on evaluating the event association between data sharing concepts, Digital Twins, infrastructure, and person. Examples are:

- **Shipment data set** – any data set (i.e. links) shared between a customer and service provider providing details of cargo to be transported from one location to another at the same time. A shipment data set refers to a transport order and its planning.
- **Electronic documents** – links to data that is normally contained by a particular document relevant to a shipment, e.g. a business document like a CMR or a document issued by an authority like a Certificate of Origin. This data set may include links to other data sets like cargo and transport means.
- **Itinerary** – a data set of a transport means calling several locations ('place of call') in a time period or direction. An itinerary has links to cargo data, transport means, and locations like ports; it may have a unique identification stored by the event link between a transport means and locations.
- **Route data set** – any physical route of a transport means between two locations of an itinerary. A route links to a physical infrastructure, for instance by means of physical coordinates or identification of a road.
- **Reporting data sets** – reporting data sets like eFTI and EMSWe are shared as a set of links to one or more of the other data sets, e.g. a link to the cargo loaded at a node and (to be) discharged at another node and the crew of a means of transport.
- **Train data set** – an association between a locomotive as a means of transport and wagons that are a specialization of 'equipment'. The association has a unique identification during a particular path or composition of wagons, the train number.

One can also consider including logistics nodes or hubs as specific data sets, where enterprises provide transshipment services, e.g. a stevedore providing transshipment services at a terminal. Other types of nodes might contain storage facilities (e.g. warehouse or distribution centre).

Genuinely, each community (or data ecosystem or 'data space', like a port community, industry associations, infrastructure managers, and regulators) can develop their own ontology for their own services or re-use services developed by others. Service development may result in identifying missing concepts and data properties in the multimodal ontology. The latter can result in a new ontology.



Semantic web standards deal with the existence of multiple ontologies, in the following two ways:

1. Specifying data semantics with two ontologies. This is about combining two ontologies (virtually) into one, whilst still referring to both during data sharing. It is the union of two (or more) ontologies and allows stakeholders to share the data they require to share. This is called ontology alignment. Shared concepts and data properties appear only once in two aligned ontologies¹⁸. Alignment rules are given in the Reference Architecture
2. Sharing data with different ontologies. This is about federation, where two communities use a different ontology for the same functionality. It is about identifying and relating the common concepts and data properties in both ontologies, i.e. their intersection. This is called ontology matching, which is the basis for the semantic adapter.

Quality assurance procedures are part of governance; these procedures assure optimal use of the multimodal ontology for service development and alignment. These procedures should also manage potential extensions of the multimodal ontology, i.e. adding concepts and properties that are common to multiple communities to the multimodal ontology. They require logistics – and modelling expertise, since some terms can be derived from the multimodal ontology, whereas others have specified them explicitly. An example is ‘itinerary’ (also called journey, track, voyage, flight, or trip) which is represented by a sequence of events linking a Digital Twin to a location.

Figure 5 visualizes that multiple ontologies of different communities can be aligned. Note that alignment is on all modules of the multimodal ontology, including the data sharing concepts.

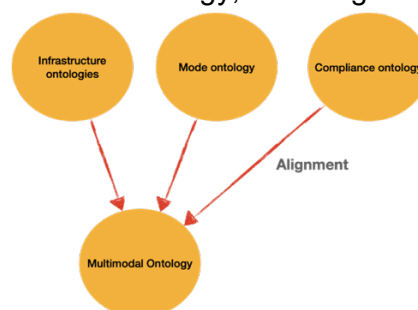


Figure 5 The multimodal ontology: alignment of existing initiatives

5.3 Service registry

A Service Registry of an organization supports its **discoverability** of its **business services** and its **data sharing** capabilities based on **services**. Each organization thus has its own Service Registry; a community uses a Service Registry to develop its services.

5.3.1 Functionality

The Service Registry supports service customization by any individual organisation:

- to specify its data requirements of its business activities for services;
- to define and publish the business services it wants to provide; and
- to formulate and publish any queries with their conditions.

¹⁸ The multimodal ontology is a so-called upper ontology. Any specialisation of this upper ontology with community specific terminology leads to a so-called lower ontology that is aligned with the upper ontology. This improves maintenance of the upper – and lower ontologies.



The latter function can be used by regulators and supervising bodies to formulate their data requirements for a regulation and by organisations that intend to provide data access.

The Service Registry supports communities in Service Development. These services contain minimal data requirements and optional ones. The data requirements as specified by a service define **access control**: the data that is available upon request. Access control has a relation with authorization, which is presented as part of the Index functionality, and Identity and Authentication.

Service customization is the support of the minimal data requirements and selection of applicable optional ones of a service by an individual organisation. It results in a '**profile**' of an organisation for a service. This profile specifies access control of the service implementation by that organisation.

According to the basic concept of the infrastructure provision, any two profiles for the same service can be matched since they support at least the minimal functionality of that service.

A profile does not only consist of service customization, but also selects its implementation specifics like openAPIs (Application Programming Interfaces) and connectivity protocol(s).

Each Service Registry contains (or has access to) the complete multimodal ontology, including those that are aligned with that ontology, and has a discovery function for re-use of business activities and their choreographies.

The functionality of the Service Registry must be as follows:

- The **minimal** functionality combines service development and - customization in generating and publishing an openAPI with an endpoint for each interaction of that service, like a transport order, a business document, or a visibility event, including a connectivity protocol like CEF eDelivery over TLS (Transport Link Security).
- The **maximum** functionality is a separation of service development and - customization where at design time the complete multimodal (and its aligned) ontology(-ies) is (are) applied as input for service customization. Data sharing is implemented with semantic technology, only a (semantic) endpoint is specified.

Since there are (expected to be) many implementations of Service Registry, they interface with each other. The following rules are applicable:

- A Service Registry is discoverable by using for instance DNS (Domain Name Service) identifying a community or an individual organisation.
- Services developed by a community are discoverable by querying the data sharing ontology.
- Business services are discoverable by matching a customer goal with business services, where the goal is formulated by data requirements of its business activity.
- Applicable regulations are discoverable by matching business transaction data with those specifying the applicability of a regulation. An example is the matching to a safety regulation for dangerous goods transport in an area for a modality.

The endpoints of Service Registries must be trusted. They are subject to Identification and Authentication.

5.3.2 Services

Services provide agreed functionality for business process collaboration and compliance for





business activities. The infrastructure provision must come with services like the following (a multi-modal visibility service is specified separately):

Services	Definition
Agility service	The structured set of interactions supporting cancellation of an order due to unexpected conditions like delays, losses, or theft of cargo and/or vehicles and potentially triggering re-planning of a (leg of a) logistics chain.
Booking service	The structured set of interactions for negotiating of and concluding a (framework) contract encompassing an agreement of prices and conditions for performing one (or more) business activity(-ies) by a service provider meeting customer goals. A framework contract is an agreement for multiple orders in a period.
Ordering service	The structured set of interactions for actual execution and detailed planning of a business activity according to prices and conditions resulting from booking service.
Quotation and marketplace services	The structured set of interactions to discover (logistics) business services meeting customer goals. This service needs to implement a high precision and recall, all logistics services, timetables, and spare capacity meeting customer demands have to be found.
Resilience service	The structured set of interactions assessing risks in completion of supply – or logistics chains or individual transport legs based on Information Services. Resilience services implement supply chain resilience.
Visibility service	The structured set of interactions providing details of the execution of a business activity and its planning by a service provider according to an agreed transport plan.

The base assumption behind these services is the reservation and use of ‘resources’ of a service provider by a customer. Transport means, containers, etc. are examples of those resources represented by Digital Twins. Internal equipment like cranes and personnel are other resources. Quotation and marketplace services support discovering these resources, booking services are about their reservation, and ordering services about their use, where visibility services show how they are used.

These services are specified in the context of a business activity, e.g. transport, transship, and stuff/strip.

These B2B services must be supported by others like financial service (insurance and payment). These must be provided by financial institutions.

Not all these services are always required for all business activities and all customer – service provider relations. In some cases, business services are a commodity: there is no negotiation about prices and conditions, those provided by the service provider are applicable.

Support of administrative business activities may require the specification of a single interaction for a service, e.g. an electronic document data set like the eCMR. Such an electronic document can also be considered as part of the other services of transport activities and be specified in the scope of for instance a visibility service.

5.3.3 Data structures of services

Access to data is shared by events with links to that data. These events have a data structure specified by the multimodal ontology referring to the data that is accessible. As a service consists of



several events, a service has a 'state' as the accumulation of events that are shared. Additional structures that are common for logistics, can also be specified, where these structures can be implemented by queries.

5.3.3.1 Event data structure

Events with links to data are used to implement a data pull mechanism. Basically, only links are shared and no data. However, a data user receiving those links must have some ways to selecting links for accessing data of a data holder. This is given by the logistics context, like location codes, container numbers, vessel identifications, flight numbers, and license plates of trucks.

Service developers can construct two types of events, namely 'transaction events' and 'visibility events'. Transaction events will have visibility events and refer to a transaction data set. The following figure shows the main concepts of the multimodal ontology for transaction events for transport.

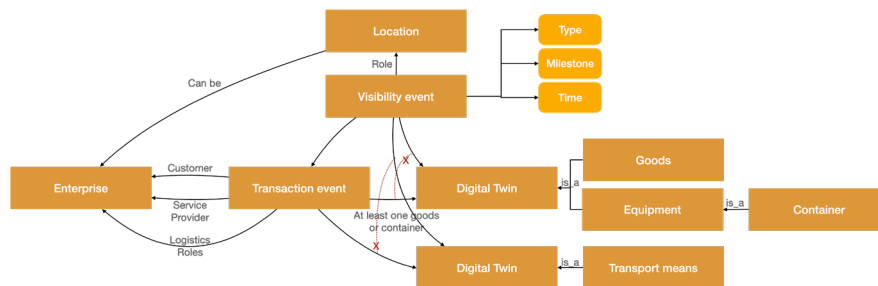


Figure 6 Main concepts of transaction events.

A transaction event is mostly represented as 'header' in a standard or business document. It can also have details on delivery conditions and prices.

Figure 6 shows that a visibility event refers to a transaction event. It also shows that a transport means is either contained by a transaction - or a visibility event. The same is applicable to the 'cargo' which is represented in this example as container equipment and goods. This allows mentioning all details of transport means and cargo at transaction level and include visibility events with links to locations and details of time.

Roles of locations and logistics roles are represented by associations.

A transaction event for transport requires at least two visibility events, namely where and when transport starts and ends. Additional events can be given to distinguish for instance a place of delivery from a port of discharge. These additional visibility events can also be used by a service provider to inform a customer on the legs of a logistics chain.

A transaction event for transshipment requires two transport means with their visibility events for a transshipment location. One of these transport means is arriving for unloading, the other for loading and departure. In this case, the association between a visibility – and transaction event does not exist.

Transaction events for stuffing and stripping (or (re-)packing) are similar to those of transshipment but are between two Digital Twins that represent 'cargo'.

In case of data sharing, it is sufficient to share only the identification of a transaction event (its UUID) and a meaningful reference for users (like a consignment – or shipment reference number). Based on the UUID, all other data can be retrieved. However, it is useful to also share identifications and meaningful references to other concepts (like container numbers) to optimize logistics planning and

data sharing and have additional querying capabilities.

Visibility events are contained by transaction events. The following figure 7 shows the visibility structure for starting and ending (milestone) physical relations like ‘load’, ‘unload’, ‘arrive’, and ‘depart’.

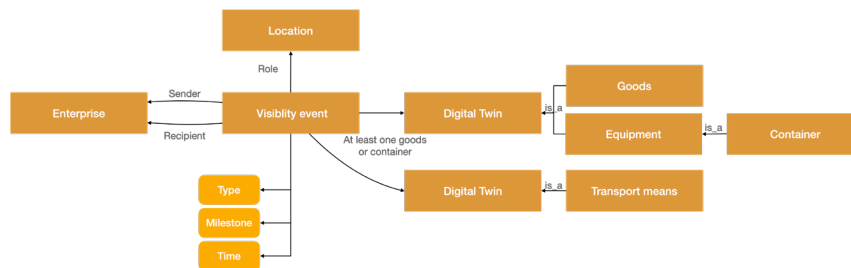


Figure 7 Main concepts of visibility events.

To the event data structure, similar rules for business activities as for transaction events are given. For instance, transshipment requires a transport means for arrival and another for departure, which are, however, mostly represented by two separate events. Stuffing and stripping events don't require a transport means.

In addition to these events, others like ‘border crossing’ can be given, where a visibility event refers to a transport means and a location of border crossing.

5.3.3.2 Data accumulation for services

Transaction – and visibility events are accumulated to retrieve the progress of services and physical activities. This is called the ‘state’ of a service as specified by the data sharing module of the multimodal ontology. Those Service Developers that intend to develop services of two or more events must specify ‘state’.

The next figure shows the concepts contained by state structure. It visualizes how visibility events that represent the physical relations between real-world objects relate to transaction events by sharing sender/recipient - with customer/service provider information as specified by a service.

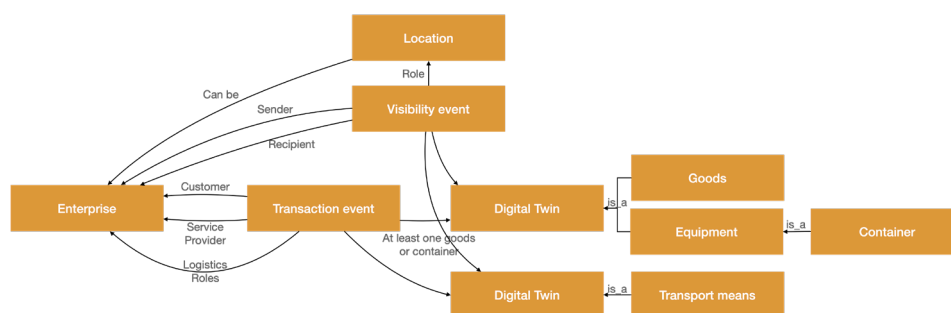


Figure 8 State – accumulation of transaction – and visibility events.

5.3.3.3 Additional data structures

Many other structures can be defined by the multimodal ontology like an itinerary or container track. Figure 9 shows the basic structure of an itinerary where a transport means passes at least one location (‘place of call’). Such an itinerary may have a unique identification like a flight – or voyage number. This is part of ‘visibility event’ as external reference.

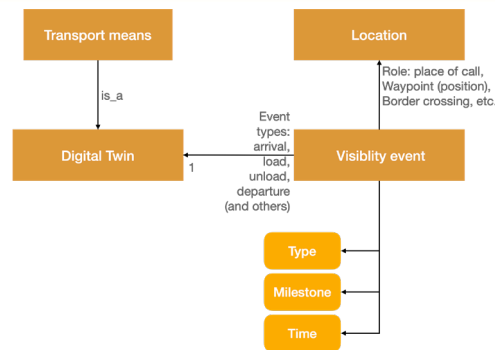


Figure 9 An example for an additional structure: itinerary.

An itinerary is mostly published as a means for service discovery, not necessarily listing the transport means itself. A container track is constructed in the same way, but most probably is implemented as a query. A shipment – or consignment track is constructed by listing all visibility events related to a single transaction event.

5.4 Index functionality

An index of an organisation contains all events (with links to data) sent as data holder with other organisations and received as data user from data holders for a service. An index shares and stores events between a data holder and -user, validates these events and their sequencing, and supports a data user to formulate queries based on links received via events and share these with a data holder. Data and events are shared with RDF between two implementations of the Index functionality.

5.4.1 Functionality

The functionality of an index:

- The **minimal** functionality is to share (visibility) events with no link to additional data. This is only about progress validating the quality of event data.
- The **maximum** functionality is to support:
 - data quality validation,
 - event logic (validating the sequence of events of the service),
 - enable access for replying to data user queries (authorization), and
 - query federation (data provenance).

Event distribution is a simple version of event logic and supports functionality like publish/subscribe. Events with links to data are shared in a commercial – or legal relationship between any two stakeholders. Some events, like an order event, can have links to different data like parties involved including their role (shipper, carrier, forwarder) whereas others represent visibility of the execution of a business activity (e.g. an ETA event that links to an order event).

Each organisation has its own (private) index that stores all events (with links to data) sent as data holder to data users and received as data user from data holders. An index supports a data user to retrieve additional data via the links it has received. The data that is retrieved by a data user for those links is specified by the service (access control, see Service Registry). A data holder provides the data to a data user by validating the link was shared (**authorization**) or a compliance requirement. The data is either stored by a data holder itself or another organisation with whom events with links are shared (**data provenance**). In the latter case, a query is federated to that other organisation

(**query federation**). This mechanism is also applicable for processing complex queries formulated in SPARQL, like retrieval of a container track by a customs officer.

An index supports **event distribution** (sharing an event with the proper data holder(s)) based on input of a data holder initiating a commercial relation, the existing of a commercial relation (previous events are stored by an Index), or for legal compliance. Event distribution can be implemented by a data user subscribing to its relevant events or a data holder configuring a subscription for publishing events to authorities for compliance.

Data quality validation is about correctness and completeness of event data and query (results) according to a service implementation. **Event logic** validates event sequencing according to the service specification. Event logic not necessarily results in an error, meaning that an event will not be shared, but can raise a flag (like the ETA at a location is too late for a next transport leg).

The implementation variants of an Index are described in a separate section of this Master Plan. The optimal implementation of the Index functionality for the infrastructure provision is based on full support of the multimodal (and aligned) ontology(-ies) for implemented services and support of semantic standards for data sharing between any two implementations of the Index functionality.

Index functionality must implement connectivity protocols for safe and secure data sharing, which is separately presented in the Master Plan. The connectivity protocol implemented by an organisation is given in its profile.

5.4.2 Data sharing pattern

The basic data sharing pattern is given by a sequence diagram (figure 10).

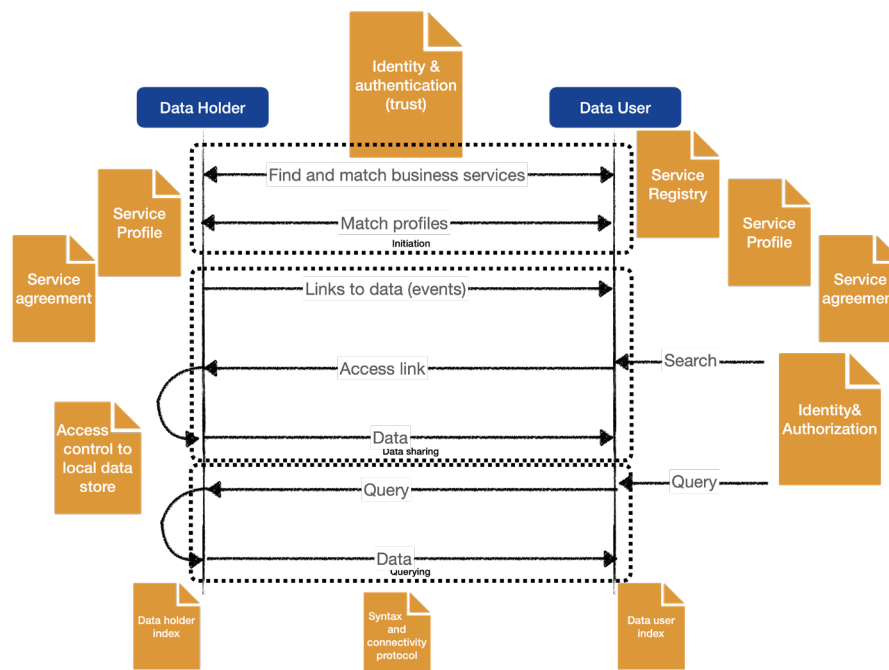


Figure 10 Data sharing pattern.

In figure 10, a customer can act as data holder initiating a service by sharing finding matching a goal with a business service of a data user. When a service provider has been found, profiles of both data user and – holder must be matched resulting in a service agreement covering the data that can be shared. This is the initiation phase that leads to data sharing.



Eventually customers and service providers can share events with links to additional data, like order - and visibility events. Whenever a customer or service provider receives such a link, it can access the additional data via that link.

Whenever events with links to data have been received, complex queries considering various links of those events like 'give me the container track for container x' or 'give me the amount of cargo transhipped at a terminal for a particular recipient in the last month'. These queries are either predefined and published (design time queries), like those for regulations, or can be formulated by a data user at runtime.

These more complex queries can be posed by for instance authorities for their risk assessment and shippers to answer questions of consignees.

The figure shows in comments the various capabilities that are touched upon like the Service Registry with its business services and a service profile. Internally, an organisation must have its Identity and Authorisation implemented to allow only for authorised access of links. Identity and Authentication of a data holder and – user is based on its VC.

5.4.3 Index APIs

This is an implementation of the local interface between the Index capability and an internal IT system of an end-user with openAPIs. These openAPIs are configurable for data transformation, data validation, and event logic by the Service Registry. These configurations can be provided by Service Developers (i.e. services) or end-users for Service Customization (i.e. profiles).

The Index APIs consist of three sets either provided by an Index or required for the integration of an Index with an IT backed system:

Index APIs	Description	Index APIs	Required backend APIs
Event sharing	A set of openAPIs to share events and access data of links shared by these events.	POST Event GET Event GET Data POST State	POST Event GET Data
Service APIs	A set of openAPIs supporting the implementation of a service by an Index (i.e. event logic)	GET State POST State GET Exception	POST Exception POST Complete
Monitoring APIs	A set of openAPIs for monitoring the configurations and behavior of an Index	Examples: GET States GET Services GET Profiles	

The **event sharing** APIs are APIs like POST Event and GET Event for publishing and retrieving events by a data holder and a GET Data for retrieving data from a node by a data user.

An IT backend system must support a POST Event API to receive events from the Index functionality and a GET Data API to retrieve data of a link. The GET Data API required by an IT backend system





can only consider data of links that are shared by posting events. Internal IT backend systems must support this.

The POST State API is the initial state required for event sharing. It is a means of subscription for event distribution. A customer can share this state with its service provider by calling the POST State API, thus subscribing to events. An enterprise can also configure this state as a subscription of a supervising body to events. The data structure of this initial state is given in chapter 6.3.3.2, since a customer (or supervising body) must have a subscription to Digital Twins and events for its order.

Event sharing APIs can be extended by webhook APIs signalling for instance that a new event is available.

The **event logic** APIs are GET States, GET – and POST State, and APIs for exceptions. For accessing proper states of event logic, the GET States provides an overview of the states that are configured. POST State has two variants, namely, to change the state in one's own implementation and to synchronize it with a peer end-user for a service instance. The POST State for synchronization is a type of subscription. This might be required for synchronisation of transportation legs, e.g. by informing the service provider of a next leg of earlier or later arrival.

Exceptions are signalled by event logic like an arrival is too late. These exceptions are provided by a node or gateway to an IT backend system. That system must support a POST Exception. An implementation of the Index functionality can also have a GET Exception API to retrieve exceptions. This can also be part of the monitoring APIs.

An optional API is the signalling of service completion. An IT backend system must implement this API (POST Complete) that can be called by the Index functionality. It can be used to trigger internal business processes like invoicing or payment of a service.

The **monitoring** APIs are the monitoring of the data sharing – and event APIs, the configurations, and accessing the log and audit trail. The GET States API is for instance an API for retrieving states; another is the GET Services to retrieve the list of services that are implemented and GET Profiles to retrieve the profiles of services. The monitor APIs to access the log and audit trail has variants, for instance to monitor data shared in a period, with a customer or service provider, combinations, or any other subset of the log and audit trail. Monitoring APIs of a log and audit trail provide information for payment of business – or (paid) Information services.

5.5 Identity and Authentication (IA)

IA is about creating trust for data sharing between organisations. It is about sharing business data (e.g., order data), services, or profiles. IA relates to authorization of users, i.e. employees of a participant, and capabilities (Service Registry and Index) that provide (access to) data.

IA is built upon two pillars:

- **Organisational** trust – each organisation using the infrastructure provision must implement measures that assure trust, for instance cyber security measures and an Identity and Access Management (IAM) registry. Rules for creating this type of trust will be formulated by a legal framework. This covers trust in processes, employees, etc.
- **Inter-organisational** trust – each organisation must share an Identity with another organisation that can be verified by that other organisation when sharing events, queries, and/or query results.





Organisations thus must not (necessarily) know authorized users of other organisations; they trust that authorization is properly implemented by others (organisational trust). Authorization and access control in an inter-organisational context are already specified separately for services.

Each implementation of the Index functionality and Service Registry for service development must have an Identity that can be authenticated (verified). A Service Registry with business services not necessarily requires an Identity, since the Identity is authenticated at Index level based on service customization. Identity and authentication is based on a completely distributed solution of Verifiable Credentials which is provided and governed by:

- a regulator (providing/establishing a legal data sharing framework e.g. EC),
- a trusted issuer of verifiable credentials registering an organisation, and
- a certification body for organisational trust (separation of concerns).

Supervision of a legal data sharing framework is based on a VC of a holder provided by a trusted issuer. By including claims in a VC like 'profile', authentication is not only based on compliance to the data sharing framework but also on service implementation by an organisation. An organisation can have multiple VCs, e.g. one VC per profile, and thus can gradually increase its service implementation.

Note that a profile for service development differs from a service profile. Where the first contains metadata of the community developing services, the service profile refers to those services by listing implementation constraints.

The implementation of such a distributed solution is still under development. The existing standards, and solutions (like OAuth2.1) can still be applied to create inter-organisational trust (applicable to data of a Service Registry and an Index). This intermediate level requires one or multiple Identity Brokers acting as intermediate Registration Authorities.

5.6 The semantic adapter

5.6.1 Functionality

Each organisation with its own internal IT systems or a platform apply their own data structure and technology. Organisations and platforms may also have implemented existing (open or de facto) standards. The semantic adapter transforms between internal data or standards and semantic data based on matching (see before). The multimodal ontology is always used as an intermediate structure for matching between internal data structure of different organisations and between different standards used by two organisations.

The functionality of a semantic adapter:

- The **minimal** functionality is the support of a JSON file structure that reflects the service data semantics. It is up to an organisation to interface with the intermediate JSON file structure. This minimal functionality may not yet support a link for querying, since that requires additional mapping functionality.
- The **maximal** functionality consists of an ontology matching tool or algorithm for matching different structures to the service data semantics. This allows for transformation between any two data sets via the service specification based on the multimodal ontology.





5.6.2 Interfacing with other standards

Existing data sharing implementations utilize other standards like those of UN CEFAC, GS1, and many others. These standards can be based on a data model, like the UN CEFAC MMT or the Information Model of DCSA (Digital Container Shipping Association).

The multimodal ontology can be used for data transformation between any two of these standards and between these standards and the infrastructure provision. This is called 'matching' resulting in data transformation by the (advanced) semantic adapter. The following steps must be taken:

- Business function matching - each standards has a function in the context of business process collaboration. That function must be matched with an identical function of a service developed with the multimodal ontology. In case of an eDocument like an eCMR or eBL, the mapping is to a specific state of a service.
In case a service is not yet developed with the multimodal ontology and is required to be implemented by those that are users of the infrastructure provision, that service must be developed.
- Data semantic matching – matching of the concepts and data properties of a standard with the ones specified by the business function of a service. There may be one-to-one matches where data of a standard is directly transformed into semantic data; there can also be more complex matches where input data is split into two or more elements or where a data set is specified by a constraint in the ontology.
- Standard specific matches – this is about handling specifics of a standard like the 'qualifier' concept of EDI (Electronic Data Interchange).

Matching may start by generating an ontology from a standard by its structure and using this ontology for matching purposes.

5.7 Identifications

Identifications are important in supply and logistics. It is about tracking of what is called a consignment or shipment, but also tracking of all types of Digital Twins. Many Digital Twins have identifications that are either standardized and can be assigned by individual stakeholders (like container numbers) or are issued by an authority after registration (like license plate of trucks). These identifications are used in the real-world.

There have been various efforts for standardization of unique consignment identifications throughout a supply chain to prevent that each stakeholder includes its own identifier to goods (pallets, packages, etc.). Since physical activities are convergent and divergent (see before), identifiers will change. Goods are repacked, split over containers, etc. Therefore, every instance of a concept of the multimodal ontology has its unique identifier that is shared bilaterally. It is the Universal Unique Identifier (UUID), a software generated identifier. Each organisation can generate their relevant UUIDs. This means that events, Digital Twins like trucks, containers, goods, etc., infrastructure elements, and persons will have a UUID for data sharing purposes.¹⁹

¹⁹ See: [DIGITAL TWIN IN FREIGHT TRANSPORT AND LOGISTICS \(federatedplatforms.eu\)](https://federatedplatforms.eu)



Each UUID is accompanied with a real-world identifier if that exists. This real-world identifier is used to relate data sharing to the real-world environment and enabling monitoring by sensors (IoT), like Automated Number Plate Recognition (ANPR) or other types of sensors based on Vehicle Identification Numbers (VIN) for cars on roads. These real-world identifiers can also be consignment – or shipment identifiers, GTIN (Global Trade Identification Number of GS1), or any other numbering scheme.

5.8 Assessing the LivingLab (technical) capabilities

The following table lists the 4 Capabilities (technical specifications), their detailing per component, and the descriptions and explanations thereof. A scoring is developed for validating the capabilities of any Living Lab (LL) – the Assessment Framework (see Milestone 12, Annex 1).

CAPABILITIES	
1. SEMANTICS	
Technical component	Description
1.1 Semantics - specification	<p>Specification of the data that can be shared by all stakeholders. The specification may take various forms:</p> <ul style="list-style-type: none"> • A model per interaction • A consignment/shipment based model • A model for all data that can be shared. <p>Such a model can also have various forms, e.g. an ontology, a class diagram, or a hierarchical structure (similar to XML structures)</p>
1.2 Interaction pattern	<p>The structured sequence of interactions. There are different options:</p> <ul style="list-style-type: none"> • There is only a single interaction (e.g. a data representation of a business document) • Sequencing is represented by sequence diagrams for the use case (chain) • Sequence diagrams for any two stakeholders • Support of (part of the) normal operation, for instance booking, ordering, and/or visibility <p>Interaction patterns can also be specific to a particular business activity like transport of containers by rail. Interaction patterns are the technology independent services, e.g. a booking -, ordering -, and visibility service. These interaction services can be implemented differently, e.g. with multiple openAPIs and as triples (RDF), see later questions.</p>
1.3 Modeling alignment or -mapping	<p>In case a LL has developed its own model, the model can be aligned or mapped to the FEDeRATED semantic model:</p> <ul style="list-style-type: none"> • Alignment – identifying overlapping concepts and data between two models • Mapping – construct an overlap of a LL model with the FEDeRATED model <p>Alignment is achieved via a representation of a LL model as ontology, most probably as a manual exercise. Mapping can be supported by technical components like a mapping tool and a semantic adapter, see next questions.</p>

CAPABILITIES	
1.4 Access policy specification	Specification of access policies. Access policies are required in case of a data pull. As such they are specified by the individual interactions taking the relevant parts of the semantic model that is applied by a LL. In case of data push, no specific access policy is required; a message supporting data push contains for instance all data that is duplicated. The syntax and technology (messaging, (open/webhook) APIs (Application Programming Interfaces) with JSON(-LD) (Java Script Object Notation – Linked Data), semantic web protocols (SPARQL (Standard Protocol and RDF Query Language), RDF (Resource Description Framework))) used for sharing data.
2. SERVICE REGISTRY	
Technical component	Description
2.1 Modelling toolset	The technical component(s) applied for designing semantics and interaction patterns. These can be any type of modelling tool. Special attention needs to be given to capabilities for import/export of models by open standards.
2.2. Organisational profile	The capability to specify and publish the organisational profile of a user participating in a Living Lab (LL). An organisational profile must refer to a LL model and/or the interactions that are applicable for the LL. The latter could be formulated by for instance APIs or standards applied for data carriers. The capabilities must be accessible for rapid on-boarding and upscaling of a use case to new users.
2.3 Toolset to construct and publish an organisational profile	The technical component(s) for a user to configure and publish its organisational profile. These tools should refer to capabilities like import/export of models and must support open standards. An openAPI environment like Swagger can be an example of publishing openAPIs with their endpoints.
2.4 Syntax	The syntax applied for sharing data. Options are: XML, EDI(fact), JSON(-LD), RDF, or a proprietary format.
2.5 Technology	The technological paradigm to share data messaging, (open/webhook) APIs, etc. In case APIs are applied, the toolset to publish an organisational profile will be probably an environment like Swagger.
2.6 Data carrier / standard	Use of an (open/defacto) standard for sharing data. This can be any standard (GS1, UN CEFACT, other) and/or a specific implementation guide of a standard (e.g. UN CEFACT eCMR, DCSA eB/L, etc.).
2.7 Data transformation (semantic adapter)	A technical component that transforms data between an external syntax/data carrier to another, where the latter is mostly an internal format. The semantic adapter is a specific implementation where RDF is used as external format and needs to be integrated with existing standards, technology, or databases. This can be via so-called RDF plugins, RML (RDF Mapping Language) tools, etc.



CAPABILITIES	
2.8 Data mapping tools	A technical component to configure data transformation. Data transformation can be supported by mapping tools. Examples are those provided by integration brokers/enterprise service busses; others are so-called RML mappers. Large Language Models (LLM) can also be considered, although they are still in an experimental phase.
3. INDEX	
Technical component	Description
3.1 Event storage	A users' view of events that are received from or send to other users. Event storage is required in case events have links to additional (upstream) data. It supports data provenance and authorization. Event storage can be part of a log and audit trail for non-repudiation.
3.2 Data validation	The capability to validate incoming or outgoing data against the agreed semantics. Validation of data sets against agreed standards implemented by for instance SHACL, XML, or JSON(-LD) structures applied at business level internal
3.3 Event distribution	Rules for sharing events with another user. Event distribution can be implemented in different ways, for instance based on a legal obligation (mandatory) or a commercial relation (dynamic configuration). A user may apply publish/subscribe, where the subscription is configured by the one that publishes the events.
3.4 Event logic	Validation of agreed interaction sequencing. Validation is only applicable in case multiple interactions and their sequencing is defined
3.5 Authorisation	The right to access data and use functionality This is about data provenance: links to data are passed between stakeholders and need to be accessible downstream. Delegation might be a mechanism for avoiding query federation, but is considered to be static.
3.6 Query federation	Access to data by a data user via an intermediary acting as data holder to the data user. This is about data provenance: links to data are passed between stakeholders and need to be accessible downstream. Delegation might be a mechanism for avoiding query federation, but is considered to be static.
3.7 Graphical User Interface (GUI)	A technical component for presentation of data presentation to a human. A (temporary) GUI might be provided in case full integration with existing IT systems is not yet feasible. The GUI will include data validation functionality (see Linked Event Protocol).
3.8 Connectivity protocol	The technical capability for reliable, safe, and secure data sharing with a (defacto) standard. Current list of connectivity protocols: FENIX connector protocol, IDSA connector protocol, EDS (Eclipse Data Space) protocol, Message queueing protocols (like AMQP), blockchain protocols (like Baseline, Hyperledger Fabric, Ethereum), and AS4 implemented by CEF eDelivery. Note: not all data sharing implementations



CAPABILITIES	
	require a separate connectivity protocol since they may use an openAPIs wit https/TLS.
3.9 Connectivity component	The technical component (and its vendor or open source/freeware) implementation of a single or multiple (layered) protocols. Please be aware that even if the protocols are identical, their implementation by a component is not necessarily interoperable with an implementation of another component.
3.10 Non-repudiation	The immutable proof that data is shared. An implementation is by a log and an audit trail. It contains all data that is shared according to the presentation protocol (events, messages, queries, etc.). Although there may not be a specific connectivity protocol, there may still be a log and audit trail.
3.11 Internal connectivity	The connectivity between various stakeholders should be supported by an individual user In case an external agreed protocol is implemented, this might not be supported by existing systems and solutions. For instance, APIs using https may have to be mapped to the eDelivery or IDS protocol.
3.12 System security protocol	The safe and secure sharing of data with PKI certificates, utilizing standard protocols (e.g. https, TLS).
4. IDENTIFICATION AND AUTHENTICATION	
Technical component	Description
4.1 Identity and Authentication (IA)	Unique identification and authentication of users (organisations). Use of open standards like OAUTH2.1, Verifiable Credentials (VCs) and Decentralized Identities (DIDs), JWT (JSON Web Tokens), or others.
4.2 Authorisation (other than link)	The right to access data and use functionality. This relates to access policies (see before) and is supported by index functionality like event storage and - distribution. In case an event storage and - distribution are not implemented by a technical component, authorization must be defined separately.
4.3 Distributed versus centralized implementation	A single IA mechanism for a use case or utilizing IAM (Identity and Access Management) systems of users via an Identity Broker There are different approaches that can be followed. VCs/DIDs are distributed; FENIX proposes limited centralized governance (issuing identities); iSHARE has an Identity Broker for identifying satellites (IAM registries of for instance a platform); a Corda based implementation has a central component for issuing identities.

Each Living Lab can be scored on a scale from 'low', 'medium', or 'high' support of the required functionality. Not applicable is also feasible, where a Living Lab did not develop a part of the technical specifications. A table has been developed for the non-functional requirements, see chapter 8.

The common Living Lab, which was established in 2023 for interoperability amongst the various Living Labs and based on the FEDeRATED node solution is the most advanced. Various Living Labs

have integrated this node and experimented with event-based data sharing²⁰.

The resulted support of the required capabilities (technical specifications) through the Living labs is illustrated in Figure 11.

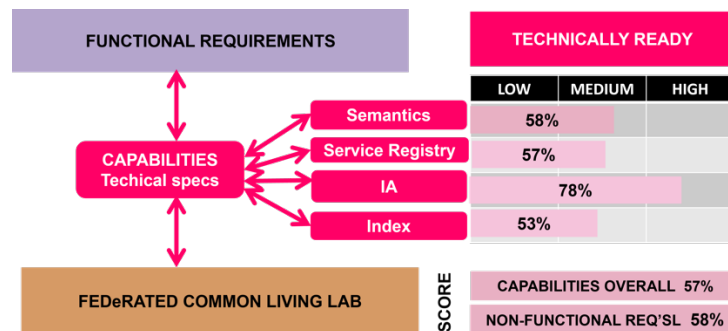


Figure 11 Technical specification support by the (common) Living Labs.

Overall, 57% of the required capabilities (technical specifications) are realized by the Living Labs. Based on a common Living Labs, the participating FEDeRATED end-user scored 58% compliance with the non-functional requirements.

Assessment of the FEDeRATED Living Labs teaches us that basically those Living Labs are the most advanced in adopting the Operational Framework capabilities in case they:

- Are driven by public authorities executing a dedicated national policy approach, including programmes and a set of agreements between stakeholders.
- Can establish a set of agreements, including standards and semantics, for a tangible and dedicated number of stakeholders.
- Have developed a mature and internally harmonized business approach based on a flexible technical setting for dealing with data sharing issues with a dedication to expand their business ventures to third parties.

²⁰ The node installation is elaborated in Annex 3

6 IMPLEMENTATION CONSIDERATIONS

This chapter elaborates the interfaces between the functionalities of the capabilities (chapter 5), with a focus on data sharing and interoperability, and proposes different approaches to their implementation. As such, standards also play an important role.

6.1.1 Data versus document-oriented approach

Data of physical objects - i.e., objects that can be observed in the real-world like containers and trucks, and their operations - is the core of the Logistics APIs. Various views on this data of physical objects can be created e.g., a transport contract like and eCMR, B/L (Bill of Lading) or eAWB (Air-WayBill), a transport order and a load list.

6.1.2 Data at source

Data is stored only once and as much as possible at the source where it was created, implying that only identifications of objects are shared, e.g. UUIDs to data or real-world identifications like container numbers. Sharing only identifications limits the amount of data shared and prevents data duplication and thus errors. It contributes to data quality (see the Vision).

6.1.3 Data sharing mechanisms

Based on the concept of data stored at the source and links being shared, the following mechanisms are applied for sharing those data:

- One-to-one sharing – a link to one or more data sets is shared by a data holder to one user.
- Publish & subscribe – a link published by a data holder and data is automatically distributed to all data users that have a subscription. Subscriptions are based on commercial relations and can be registered by customers; subscription can also be registered by data holders thus enabling automatic publication of data to authorities for compliance to regulations.
- Push-pull transformation – a data holder is not always able to share links or has systems that provide access to data when a data user pulls it. In this case, a data holder can upload (push) the data to a facility that generates a link to an intended user who may access (pull) the data by evaluating the link.
- Pull-push transformation – a data user is not always able to receive links and pull data. In this case, a data user has a facility that automatically pulls data based on links received and forwards the combined data set to the data user.

6.2 Implementation variants of the Index

The 4 variants for implementation of the Index functionality are:

- Node – all functionality is implemented by a node.
- Gateway – closer integration of the index functionality with an internal IT system.
- Adapter – the index functionality is implemented by the IT systems of an organisation.
- Platform – functionality is implemented by platform provider for multiple organisations.

A node and a gateway support openAPIs to internal IT systems. Since a node or gateway can be developed as standardised products according to the [Reference Architecture](#), these will have to be tested only once. One may also consider having them tested for various profile variants to assure



that they will always operate for an organisation.

Whenever an organisation decides to implement a node or gateway, its openAPIs with that node and gateway must support the services implemented by its profile. This allows the processing of any query in the context of that service implementation. An adapter is assumed to support these queries.

Any queries that include data of two or more services must be specified at development, enabling an organisation with a node or gateway implementation to support these queries. The latter is only required if that organisation implements those services; otherwise, part of the query can be federated to another data holder via the node or gateway (federated querying).

6.2.1.1 Node

This variant is especially useful during piloting, for SMEs without any IT functionality, and other organisations that are not able to support the functionality in their internal IT systems. A node implements the Index APIs. For piloting and to suit SMEs, the node variant must also have a GUI.

This implementation variant requires additional functionality, namely:

- Semantic adapter – transformation of internal (JSON) data into RDF, where the JSON structure reflects a service profile.
- Service registry – an additional module to generate (configurations of) the semantic adapter.
- JSON enrichment – inclusion of UUIDs in outgoing event flows and matching these UUIDs to internal IDs of data.

Since querying existing IT systems with SPARQL may be (too) complex, data could temporarily be stored by a node in a triple store or graph database. This may also be done for handling federated queries: data of a data holder is temporarily stored by a data user and can be made available to another data user upon request.

Such a data duplication must be avoided since business operation is handled by employees with their existing IT systems.

6.2.1.2 Gateway

A gateway is an extension and an alternation of a node. There are two variants of a gateway, namely the variant where event logic is implemented by internal IT systems or by the gateway.

The extension of a gateway is its support of (open)APIs of internal IT systems and their transformation to the Index APIs (or any Service -/Profile APIs). This requires a more complex semantic adapter and a matching module for mapping internal data structures to the ontologies of a service profile. It also requires handling internal identifications and UUIDs applied for data sharing.

It can also require additional functionality for instance filtering data retrieved from an openAPI or combining data retrieved by two or more openAPIs. This additional functionality must be developed for individual organisations; it may become part of a gateway solution in the future.

6.2.1.3 Adapter

All functionality is implemented as an adapter by the internal IT system(s) of an organisation. It is up to the software developer, i.e. the Commercial Off The Shelf (COTS) software – or service provider or the IT developer of a proprietary system to implement the functionality.



6.2.1.4 Platform

A platform provides its services to multiple users and can federated with other platforms or nodes on behalf of all or part of its users. Platforms are governed by a community of end-users or operate commercially. Semantic concepts for platform services may differ from the data sharing ontology, but services that are federated must be based on the data sharing ontology. A platform must have:

- A profile and Verified Credential (VC) for each federated service. This VC and profile is used for those users of the platform that implement that profile.
- An implementation of the index functionality by any of the three other implementation options, and
- A business service registry with business services of those platform users that support a particular profile for discoverability of these users.

Platform providers must define roaming agreements with other platforms and distributed implementations by end-users (node, gateway, or adapter).

6.3 openAPIs with IT applications

When using a node or gateway variant, OpenAPIs are one of the ways to implement the interface between the infrastructure provision and internal IT backend systems. Index APIs are already mentioned in chapter 5.4.3. Non the less, end-user or node/gateway provider may want to support other openAPIs. Of course, IT systems can have their own openAPIs. To do so, these open APIs must be mapped to the openAPIs of the infrastructure provision, resulting in (data) transformations.

OpenAPIs of the infrastructure are generated and must be configured by the Service Registry. Index APIs (5.4.3.), Service APIs (6.3.1.) supporting a service, and Profile APIs (6.3.2.) with service customization are distinguished.

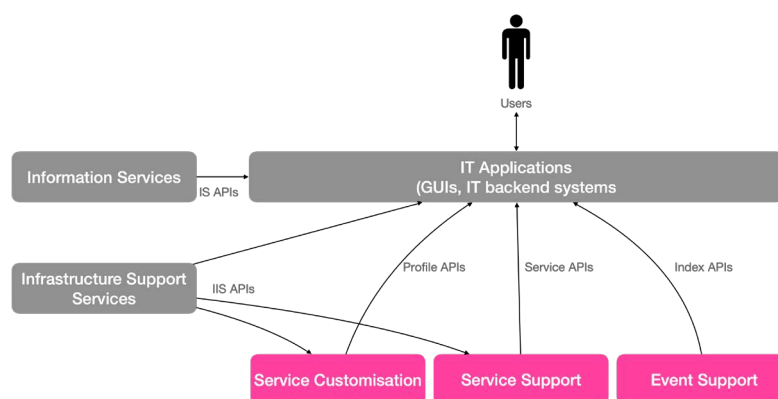


Figure 12 The various types of openAPIs.

An openAPI also contains code for data validation. Implementation of any of these three sets of openAPIs is based on the ability to configure those openAPIs with SHACL and RML from the Service Registry.

Figure 12 shows additional APIs for Information - and Infrastructure Support Services. The functionality for providing these APIs is out of the FEDeRATED scope.

6.3.1 Service APIs

Service APIs are openAPIs supporting a service. Service APIs are provided by Service Developers. They are configurable for a service profile of an end-user for its data transformation, data validation,



and event logic. The Service APIs encapsulate the Profile APIs, implying that the Index APIs also encapsulate the Profile APIs.

The Service APIs consist of data sharing APIs, event logic APIs, and monitoring APIs. The latter sets are identical to those of the Index APIs. In addition to the event logic APIs, there is a GET Service_states to retrieve the applicable service states.

The baseline of the Service APIs for data sharing in terms of GET and POST operations is identical to those of the Index APIs, but they reflect the event type they support. To support sharing ETA events this will give for instance a POST and GET ETA event supported by a node and gateway of a data holder and a POST ETA event with that of a data user. Furthermore, the data retrieval can be specific to that type of data that requires to be shared, for instance GET eFTI to retrieve the eFTI data set.

Implementing Service APIs results in (potentially) many openAPIs that must be tested and implemented by a node/gateway and IT backend system(s) of an end-user. An end-user may also require a single set of Service APIs that support various services with overlapping functionality.

6.3.2 Profile APIs

Profile APIs are openAPIs that support the implementation of a service for an end-user, based on its profile. The set of openAPIs is identical to those of the Service APIs, but only support a profile of a service.

6.3.3 Query API

The query API supports queries of data of multiple services. These are queries like 'container track' or 'trip'. These queries are posed via a SPARQL endpoint of a node or gateway. A node or gateway can also pose this query to an IT backend system, which thus must support this query.

Since openAPI implementation by IT backend systems takes time (and costs), it is recommended that a community specifies and publishes several queries at runtime, based on the multimodal ontology.

6.3.4 Infrastructure Support Service (ISS) APIs

ISS APIs are computational services that can be embedded in the other services. These services are provided by third parties. There are two types of services, namely those to support:

- Data sharing. An example is a data transformation API. Data sharing ISS APIs are based on metadata, e.g. the business function and the input-/output semantics and syntax required for data transformation.
- Logistics operation Examples are an ETA calculation – and a chain composition API. A route planning API is also an example of a logistics ISS API, that can also be used for roads and person mobility. These ISS APIs must relate to logistics concepts and properties of the multimodal ontology to make them widely applicable. It is however up to a provider of this type of service to specify it.

6.3.5 Information Service (IS) APIs

IS services provide access to data to improve decision making and validation of operation. These are for instance:

- openAPIs to access traffic information, to share capacity, etc, or





- IS APIs for publishing accidents that might be accessed for validating delays that cause late delivery.

It is up to a data user to identify the applicability of these IS APIs. The data holder has to specify and publish the IS APIs with the applicable conditions. For interoperability, these IS APIs must use the multimodal ontology. Their specification may result in specialisations (lower ontologies).



7 ORGANISATIONAL ISSUES

This chapter describes some rules for an infrastructure provision to operate as being open, neutral, trustworthy, available to all supply and logistics stakeholders, and supporting Service Development and Customization by many stakeholders.

7.1 Roles and responsibilities

The template hereunder provides the roles and responsibilities for the functioning of the infrastructure provision.

Role or responsibility	Definition	Description
Certification	Validating an implementation against agreements by a set of (mandatory) tests.	Certification consists of several tests that must be supported by an end-user. These tests are known. They are based on the specifications and their implementation by an end-user (i.e. its service profile). Certification can be implemented by a Certification Service
Certification Authority	A role providing a certification service to end-users using a reference implementation	Certification authorities must have a reference implementation of all functionality.
Data sharing agreement	The rules and procedures for creating and operating the infrastructure provision and registration of end-users to that provision.	These refer to governance. The rules and procedures cover the infrastructure provision itself, service development and – customization, certification, registration, and use of the infrastructure provision by end-users.
Data sharing legislation	The process and collaboration for developing data sharing agreements .	The collaboration and the legislator specify the scope and application of the data sharing agreements, and thus the governance.
Data sharing steward	The role that is responsible for data sharing on behalf of an end-user .	This role can be part of an end-user but can also be supported by a platform provider. A data (sharing) steward might be supported by a data custodian that is responsible for running the soft- and hardware integrity. The operation of a data custodian could be outsourced to a cloud service provider.
End-user	Any organisation (public or private) operating in supply and logistics, e.g. LSPs, RUs, IMs, carriers, shippers, Food Safety Authority, customs authority.	This refers to organisations that operate the ICT systems, either from a business – or authority perspective.



Role or responsibility	Definition	Description
Identity Provider	A role assigned by a legislator for issuing identities to end-users identities based on their certification.	Computer systems cannot “see” who they are interacting with and therefore Identity Provider roles are needed to certify that a user really is who they say they are by a digital identity. The role is trusted since it is assigned by a legislator. Synonym: issuer.
Legislator	The role responsible for (data sharing) legislation .	This normally covers development, publication, implementation, and maintenance of data sharing legislation.
Registration	The process of onboarding an end-user with the infrastructure provision.	This process results in providing an Identity to an end-user after its certification. Registration of end-users can also be done by a platform provider, where the platform provider receives an Identity. Registration can be implemented by a Registration Service.
Registration Authority	A role assigned by a legislator for providing registration services to end-users with the infrastructure provision.	A registration role can be combined with the role of Identity Provider. The organisation with this role is trusted since it is assigned by a legislator.
Service customization	The process of selecting only those optional elements of a service that are required by an end-user.	Service customization results in a profile which implementation can be certified.
Service customizer	The role responsible for service customization according to the data sharing agreements .	This role can be taken by the organisation having the data (sharing) steward role. A Service Customizer may generate Profile APIs or configure the Service – or Index APIs for a service profile.
Service development	The process of developing, publishing, and maintaining ‘services’ with the data sharing module of the multimodal ontology.	The services are for business process collaboration.
Service developer	The role responsible for organizing service development according to the data sharing agreement .	A private community, legislator or individual organisation can take the role of service developer. Service development is compliant with the data sharing agreements of the infrastructure provision. A Service Developer may generate Service APIs for each of its services or provide



Role or responsibility	Definition	Description
		configurations for the Index APIs.
Verification	The process of authenticating an identity of a holder and trust in the Identity Provider.	The data sharing steward is the holder of an identity.
Verifier	The function of a data sharing steward performing verification.	The data sharing steward role can be taken by end-users themselves or platforms on behalf of end-users.

7.2 Distributed Service Development and - Customization

It is up to the supply chain communities developing their semantics model (ontologies). It will result in services with similar functionality, services that are based on another model represented by another technology, implementation guides of domain standards, etc.

Service development is use case driven. Two or more organisations may want to share data digitally, either using existing services or requiring new ones. Normally, use case analysis starts by drafting sequence diagrams, visualizing data sequencing amongst stakeholders. Several data sequences in such a diagram can be mapped to or combined into a (new) service. Thus, sequence diagrams are a means to identify required services. Tooling may assist organisations in this process.

Services with similar functionality are not necessarily overlapping. There can be visibility services for a modality and a cargo type. For instance, visibility services for container transport by sea differ from those of livestock transport by road, although the pattern for sharing events is identical. Also, some ports may have services like tugging and piloting that are not required by other ports.

The Master Plan supports various solutions for dealing with the differences between services, based on the need to reduce complexity for end-users of an infrastructure provision. The focus is on:

- Service re-use – services are discoverable and can be re-used by Service Developers to create new services by specialization (applying them for a modality) or extension (make them applicable to another modality or cargo type).
- Service harmonisation – based on discoverability resulting in identifying services with overlapping functionality, Service Developers may also decide to align their services and create specializations. Service harmonisation is based on the ontology alignment methodology.
- Service discoverability - also required for service customization. An end-user thus must know how these services have been developed. An end-user may decide to customize each applicable service or a combination of (specialized) services. For instance, an end-user provides transport service for multiple modalities and cargo types. Service discoverability may result in a service for each modality and cargo type. There are two cases:
 - the services are harmonised and/or created via re-use. This enables an end-user to create one profile for these combined services or a profile per modality and cargo type. The latter results in many profiles, each with its VC.
 - the services are not harmonised or created via re-use. An end-user must have a profile per service.



Creating a single profile for multiple services supports the Once-Only Principle: the same data is accessible for multiple purposes.

Trust in Service Developers is created by their registration with a trusted Registration Authority as part of the infrastructure provision.

7.3 Adoption

Large-scale adoption of the infrastructure provision and its capabilities takes time and therefore requires a long-term strategy. It is about technology adoption and digitization of business process collaboration. Large-scale adoption depends on stakeholder engagement,²¹ both from a technology (IT service providers) and business perspective (logistic operators and public authorities):

- From a technology perspective, it is about involving developers in creating the various capabilities of the infrastructure provision.
- From a business perspective, is about enabling end-users the capabilities to benefit from the infrastructure provision.²²

Large-scale adoption of the infrastructure provision relates to:

- Use case initiatives between more than two enterprises towards service development and, for instance, a multimodal supply chain visibility service, and technology support, like configurable Index APIs implemented by a prototype.
- Data requirements set by supervising bodies, which makes services obligatory, or which could be voluntary, leading to business advantages (e.g. the eFTI Regulation is a voluntary regulation for enterprises, but obligatory when they digitize their data sharing).
- Stakeholder engagement, sometimes called collaborative innovation, aimed at adoption and diffusion aimed at engaging so-called first movers implementing the infrastructure provision. First movers will start by piloting technology, gradually implementing this technology in their business processes, IT, and organisation. As opinion leaders, they can convince organisations to adopt the solution, first of all what are called 'followers'. It also requires convincing data sharing stories, i.e. appealing business cases.
- Development of Killer apps, i.e. new services that are not yet implemented by organisations. These services may support innovative business models like required for the Physical Internet and new technology like Large Language Models (LLM). The latter requires data from various data holders to provide new services to organisations.
- Horizontal data sharing agreements to support collaboration amongst stakeholders. The adoption will depend on the scale of the community pursuing these data sharing agreements, whereby engagement an independent public body like the EC is essential²³.

²¹ The major operators involved are Shippers, Transporters, Forwarders/agents, Terminal operators, Retailers, and Public authorities. In addition, there can be many third parties involved, such IT Services providers (platforms), software companies, standardization bodies, ports, bankers, insurers, etc.

²² Adoption also relates to the re-use of (adopted) horizontal standards underpinning the infrastructure provision, and services available to end-users. Two major questions to be answered are: - what is the business functionality of the infrastructure provision? - Does the technical solution fit into the IT landscape of an end-user.

²³ An EU Regulatory Framework persuading supply chain stakeholder to engage with federated data sharing can create





- Technology adoption for creating capabilities with a high TRL, Technology Readiness Level, and supporting capabilities, i.e.:
 - Support of so-called horizontal standards: those that are independent of any domain. OAS (Open API Specification), IDSA (International Data Space Association) protocols, and eSens eDelivery that is part of the Connecting Europe Facility (CEF) are examples of these horizontal standards. This is about technology adoption and implementation, in accordance with the IT landscape of end-users.
 - Standardisation of semantics, creating an open standard for the multimodal ontology or its capabilities, in such a way that it is applicable to multiple domains, not only freight, but also passengers, trade, and industry. It is about support of new regulations like those for Digital Product Passports. The main concepts of the multimodal ontology (event, Digital Twin, infrastructure, person, and data sharing module) can be standardized by an independent standardization body. This is the upper ontology for data sharing that can be specialized to multiple domains and supporting a large variety of existing domain standards. It results in a horizontal standard for multiple domains, thus reducing data sharing costs.
 - Standardisation of the infrastructure provision interfaces with IT backend systems for end-users that implement a node or gateway with openAPIs (chapter 6.3). Especially, the Index APIs (chapter 6.4.3) are candidates for standardization since they support all types of services and their customization. They are a stable interface for end-user enabling upgrading or changing technology of an Index implementation.
 - Availability of solutions, being COTS (like a gateway provided by an IT solution provider) or proprietary (like a platform with its own adapter).
 - Open-source development and maintenance of tools and applications

7.4 Migration path

Gradual development and implementation of capabilities and services enabling any organisation to act as Node enables the smooth transition towards a federated infrastructure provision. Initially, no capabilities (or their prototypes) may be available for organisations, let alone services (or maybe services are available in proprietary formats). Whenever services are available in proprietary formats, these can be transformed into formats required by the infrastructure provision (easily).

A community (or project) can develop (prototypes of) capabilities and develop or transform services for end-users. Since there might be multiple communities working in parallel, quality assurance between these communities must be established to prevent creation of community-based dataspace.

Thus, a distinction is made in migration of a community and an individual organisation.

an EU market for developing (innovative) solutions for SMEs (see chapter 1). Such a Regulatory Framework should incorporate current and future EU legal Acts with regard to the digitization of the supply chain.



7.4.1 Migration strategy

Adoption requires a long-term strategy according to the various aspects given in chapter 7.3. It also requires a migration strategy incorporating the following considerations:

- Start small, grow big – this is about the scale of adoption. Start with a small community of opinion leaders with the intention to scale to a larger one. The small community must have the ability to validate all capabilities for an appealing business case.
- Add value – this is about the business case of not only end-users, but also that of Service Developers and technology providers. Where the first is about a logistics business case, the latter is about implementing the Service Registry.
- New services – start with services that are not yet implemented by the community (and add value). A visibility service is an example; capacity sharing services could be another example. A visibility service may not yet require a 'profile'. Gradually, 'profiles' can be introduced by replacing existing data sharing standards with services.
- From experiment to application – this is about validating the capabilities of the infrastructure provision in their business context. It can imply to start with a node and migrate to a gateway or decide to develop an own adapter. It can also imply to partly implement the Service Registry functionality for service development and – customization.
- Hide complexity – provide a common set of interfaces of the infrastructure provision to end-users. It enables ad hoc technology selection with the ability to migrate to horizontal standards.
- Best practices – re-use of what others have developed and learned. This is about service re-use and its customization to users in a community (creating profiles).

7.4.2 Community migration – capability development

Figure 12 shows the migration phases for a community. It is about development and validation of capabilities by end-users for use cases.

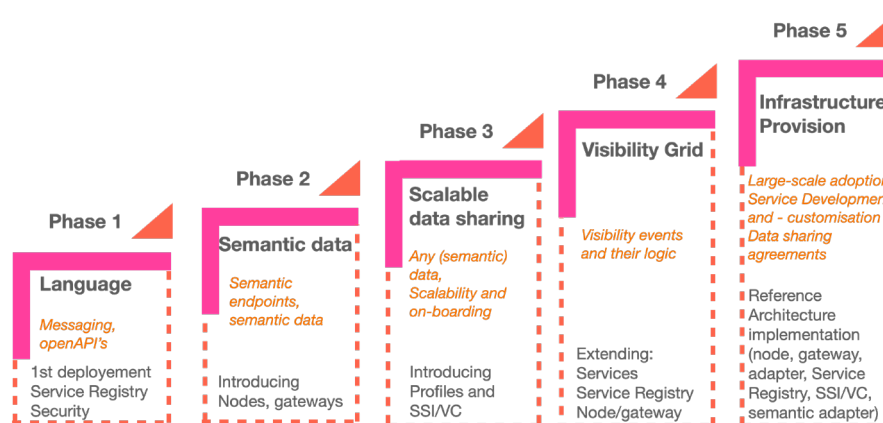


Figure 13 Migration path for a community

7.4.2.1 Phase 1 - Language

In this first phase, the semantic model for generating openAPIs for services required by a community is applied, covering existing services and possibly new services. A service can be about sharing the data set of a business document or cover multimodal supply chain visibility. It is advised to start small in this phase, thus applying existing Identification and Authentication means and reducing complexity of the great many APIs that must be integrated. The openAPIs produced by the Service



Registry are based on considerations given in section 6.3.

7.4.2.2 Phase 2 – Semantic data

The second phase is about introducing semantic technology implemented by a node or gateway hiding complexity and the Index APIs supporting the functionality developed in the first phase. These Index APIs are implemented at the interface of an end-user with the infrastructure provision, i.e. a node (section 7.2). This reduces complexity by limiting the number of APIs that must be implemented.

The first implementation of node (or gateway) can be based on ad hoc selection of capabilities and new versions can be constructed to support horizontal standards. Updates of this software always have at least the Index APIs (or a relevant subset), which means that updates don't have implications for an end-user.

7.4.2.3 Phase 3 – scalable data sharing

The third phase covers scaling, including the implementation of an SSI/VC based Identity and Authentication infrastructure, and implementation of the Index APIs for data pull mechanism with semantic technology. Accommodating policies based on data sharing agreements and its legislation provide for a sound governance framework.

7.4.2.4 Phase 4 – Visibility grid

The fourth phase is about implementing new services like a multimodal visibility service. It is about re-use and harmonization of overlapping services and applying all concepts of the data sharing ontology resulting in event logic for a node and gateway implementation. A multimodal supply chain visibility is an example of such a new service, shown in the figure. Nodes and gateways can still have the interfaces (openAPIs) with IT systems of end-users as in the third phase, extended with openAPIs for event logic.

7.4.2.5 Phase 5 – Infrastructure Provision

In the fifth phase, all capabilities of the infrastructure provision and sufficient services to support organisations in data sharing should be made available. Each end-user can decide to implement the Index functionality by a standard node or gateway or develop their own adapter.

7.4.3 End-user migration

The objective is the migration of an end-user, an individual organisation, to fully implement their capabilities. It requires technology support of these capabilities (developed in a community, see migration of a community) and availability of services.

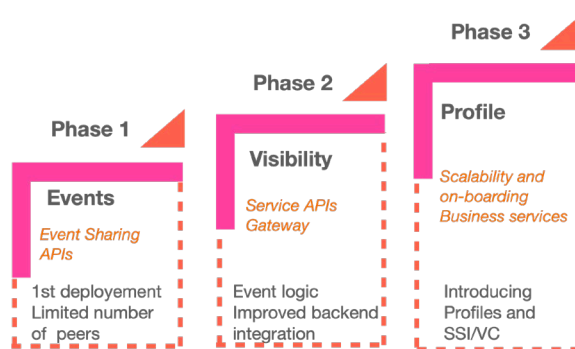


Figure 14 Migration path for an individual organisation





7.4.3.1 Phase 1 – Events

This first phase covers the sharing of events; - the implementation of the event sharing functionality of the Index API (section 6.4.3), preferably with a node implementation with a GUI (section (6.2.1.1.)). In a pilot, a node with a GUI can be used without further integration with IT backend systems. The Index API hides complexity of semantics, it is fully configured for events of a service. Links to additional data can be shared and access to that data is via the Index APIs.

7.4.3.2 Phase 2 – Visibility

The second phase is about implementing the logic of a service and extending the functionality of the Index API. It can also be on integration with IT backend systems via a gateway solution that provides a mapping of internal APIs and Index APIs.

End-users may already have IT facilities for visibility like events with their APIs and a web interface provided to their customers. These APIs can be matched to events of a visibility service. Event logic will most probably be implemented in IT backend systems and also needs to be matched with that of a visibility service.

7.4.3.3 Phase 3 – Profile

Where the previous phases are experimenting and implementing functionality with a limited number of peers, the third phase is about becoming a full end-user of the infrastructure provision. It is about the support of 'profile' with Verifiable Credentials (VC). As service providers, enterprises publish their business services. Authorities publish their data requirements in the context of regulations. This third phase requires complete functionality of the Service Registry for development and discoverability of service specifications of Service Developers.

Since Phases 1 and 2 fully implement sharing of events with links to data and event logic, the third phase can support services complementary to visibility like booking and ordering.

7.4.4 General observations

There are some common statements to be made with respect to migration, namely:

- Don't wait. Communities can always start by adopting semantics for generating openAPIs. This is the first phase for a community. Organisations can start with the first phase with the Index API supported by the prototype node²⁴ and Service Registry.
- Continue after Phase 1 to the next Phases, even after introduction of SSI/VC in Phase 3 for communities. Phase 1 is only applicable for a small community. A large community as all logistics enterprises in the EC cannot manage the implementation of 'a forest of' many openAPIs, even in most of them are functional identical.
- Sticking to phase 1 for a community is only applicable with a limited number of platforms. This reduces the 'API forest'.
- Supervising bodies need at least a Phase 3 implementation (organisational migration). They must supervise a many logistics enterprise, including SMEs. Thus, managing 'an API forest' (Phase 1 for a community) comes with too high costs.

²⁴ See: [Node prototype and installation, incl codes](#) . The latest version of the node prototype and updated documentation can be found at: <https://github.com/Federated-BDI/FEDeRATED-BDI>
Updated Docker installation instructions are available at: <https://github.com/Federated-BDI/Docker-BDI-Node>





- End-users require service re-use and harmonisation. This is fully supported by at least Phase 3 and Phase 5 for all services.
- Especially (a community of) first movers i.e., the opinion leaders, will develop capabilities for the first four phases collaborating for data sharing agreement legislation. Followers and laggards will adopt these capabilities according to the migration phases of an individual end-user.
- Platform – and COTS software providers can be amongst the first movers or communities for developing capabilities. Especially platform providers can figure out the impact on their business model, starting in phase 2.
- Platform – and COTS software providers are most likely to develop adapters to their system. This provides optimal support of non-functional requirements.
- As end-users, SMEs require standard (COTS) solutions or platforms with standard applications. These provide large-scale adoption.
- Service developers and -customizers require a testing environment for testing the technical implementation.
- Service developers also require first movers for new services; these are most probably the end-users that require these new services.

7.4.5 Considerations for a pilot / Living Lab

Moving towards a migration path, communities can be organized as pilots or Living Labs. The various issues to be explored in a Living Lab, including one or more use cases or pilot relate to Scope, Stakeholder Engagement, Technical Setting, Testing and Impacts. ²⁵

²⁵ For this purpose FEDeRATED developed a Living Lab project book, containing the various items: [LL Project Book \(federatedplatforms.eu\)](https://federatedplatforms.eu)





STAKEHOLDER ENGAGEMENT (based on the experience gained in the FEDeRATED Living Labs)

Data sharing is a collaborative effort: interaction and involvement are paramount¹. Generally, sharing data is between different entities within one organisation – internal collaboration – or between various organisations (companies and public authorities). The goals can be manifold: (new) business services, legal compliance, process innovation, effective law enforcement, Return on Investment, ESG goals (CO₂/NO_x emission reduction, less congestion) faster lead times, less administrative burdens, more safety and improved emergency response.

Data sharing is about trust (often data sensitivity) dealing with different dimensions:

- Technical - 'Is my data accessible to authorized organisations only?'
- Liability – 'What is done with my data?'
- Business - 'Do I get paid? or "Has the service/product been delivered?'

The most important steps to take executing a data sharing project are:

1. The identification of the partners, based on a business case (can also be legal compliance, facilitation, etc.). This should lead to a common understanding between the stakeholders of the problems to be resolved, including a shared responsibility.
2. Project definition (scope), i.e. objective, collaboration, governance and continuation, on-boarding, finance, and feedback loop.
3. To define and agree on the services to be provided.
4. To identify the data flows that need to be exchanged between data holders and users of the use case.
5. To apply the appropriate design – identify how to technically share data (i.e. API's, semantics, nodes, digital twins, etc).
6. To implement the appropriate tools (i.e. dashboards, nodes) to allow data to be seamlessly exchanged and shared.
7. To test – the data being exchanged, the applicable technical setting, stakeholder commitment.
8. To deliver – including validating the measured impacts, such as contributions to policy objectives, benefits, and savings.
9. Communication and evaluation.

Committing various stakeholders to share data requires a lot of care, clear understanding what's in it for who with what purposes, proportionate action, a sound governance structure, and a common sense of purpose. Often, stakeholders lack digital competence (see Annex 2), thus jeopardizing data-based logistics project development.



8 NON-FUNCTIONAL REQUIREMENTS

A non-functional requirement (NFR) specifies the criteria that can be used to judge the operation of a system, rather than specific behaviors. It relates to both end-user as the infrastructure provision itself.

8.1 Non-functional requirements for end-users

The non-functional requirements are listed hereunder (system is the implementation of the Index functionality by an end-user):

Non-functional	Description
Performance	i.e. the system's ability to respond to user requests in a timely and efficient manner. It includes factors such as response time, throughput, and scalability.
Performance efficiency	i.e. the system's ability to use resources (such as memory, CPU, and network bandwidth) in an optimal way. It includes factors such as efficiency, speed, and optimization.
System security	i.e. the measures taken to protect the system and its data from unauthorized access, modification, or destruction. It includes factors such as data encryption, access control, and authentication.
Reliability	i.e. the system's ability to perform its intended functions without failure over a period. It includes factors such as fault tolerance, error handling, and disaster recovery.
Maintainability	i.e. the ease with which the system can be modified, repaired, or enhanced over time. It includes factors such as modularity, documentation, and code maintainability.
Usability	i.e. the system's ability to be used effectively and efficiently by its intended users. It includes factors such as ease of use, accessibility, and user satisfaction.
Availability	i.e. the system's ability to be accessible to users whenever they need it. It includes factors such as uptime, downtime, and service level agreements (SLAs). It also relates to denial-of-service cyber-attacks of servers. Availability comprises MTBF (mean time between failure) and a contingency plan. It can also be the failure of a single component of one stakeholder in its role of data holder.
Scalability	i.e. the system's ability to handle increasing amounts of data, traffic, or users over time. It includes factors such as horizontal scaling, vertical scaling, and load balancing. This is of relevance in the case of a single platform; a P2P environment can probably handle more. Indicate aspects/means for testing and expected form of results.
Compatibility	i.e. the system's ability to operate with other hardware, software, or systems. It includes factors such as interoperability and compliance with industry standards.
Contingency plan	i.e. any fallback procedures when (crucial) systems capabilities fail. Are there procedures, and if so, outline type of procedures and to be tested aspects.
Onboarding	i.e. procedures for including new stakeholders to the LL. Are there procedures, and if so, outline type of procedures and to be tested aspects.
Extendibility	i.e. the systems capability to support (profiles of) new services and alignment with other ontologies.
Flexibility	i.e. the capability for configuring the system or having hardcoded solutions.

There are lots of solutions to address the previous non-functional requirements, i.e. applying Kubernetes or running Docker containers for a node or gateway and its configurations. These non-functional requirements are also relevant to IT backend systems, they need to be able to provide data on time and process (SPARQL) queries. An intermediate solution to deal with these requirements is to utilize a node or gateway and upload data from an IT backend system to a triple store or graph database running on the node or gateway. In case data changes dynamically in backend systems, this solution requires lots of interactions between that backend system and a node or gateway, especially if visibility events are considered. It is recommended to implement an adapter for these backend systems.

In most cases, configurability is a trade-off between performance and extendibility/flexibility. Extendibility and flexibility require configuration, but performance drops by an increased number of configuration parameters. Virtualization by Docker or Kubernetes can improve performance by flexible utilizing hardware resources, which can have an impact on energy consumption. Another approach is to produce specialized nodes or gateways for particular services. Furthermore, support of the multimodal ontology by a node or gateway can be improved by for instance those subtypes that are relevant to an end-user (based on its profiles) and combining super – and subtypes. This will impact event processing and can have impact on configurability for extendibility and flexibility.

8.2 *Non-functional requirements to the network*

Internet access is mostly provided by an Internet Service provider using underlying communication technology. An ISP will provide a service level to its users that will include unauthorized use of the network. Encryption can be applied for supporting this, acknowledgment receipts of data can be added, etc. Protocols like CEF eSens support this functionality, they also include resubmission of data to address unavailability of server(s).

However, an end-user is also depending on the availability of the communication technology (wireless, mobile, cable, or satellite network). To prevent any delays of accessing data at crucial times, it is recommended to access data after receiving links and temporarily store it in a node or gateway. An end-user must be aware that any updates of this data might not be available after initial downloading, so checking of updates is required.



9 RECOMMENDATIONS

In this Master Plan, an approach on how to operationalize the DTLF federative network of platforms concept is provided. The underlying **supply chain trend** is to streamline digitized information flows through data sharing between businesses and public authorities aimed at seamless business as well as compliance procedures. This trend fundamentally touches on the **current paradigm** within logistics, being *data sharing via propriety data within a closed ecosystem based on the application of data standards and technical components*. A **new paradigm** – the federated approach – is pursued: *the sharing of data at source through an open, neutral, and trusted infrastructure provision applying semantic data – semantic web technology – and a set of capabilities and agreements enabling non predefined querying and pull based service development*. This paradigm can be identified as the federated approach.

The adoption of the federated approach requires a sound **revenue model** for its participants. The 23 FEDeRATED Living Labs showed this is not manifest for all, yet. What was missing is an overarching EU harmonising Framework approach, to motivate operators and public authorities to venture into federated data sharing, and an easy-to-use operational framework and practical tools to get started. Preferably this should be made available based on OpenSource technology to all stakeholders in the logistics chain. This Master Plan fills this gap.

Moving towards a majority stakeholdership for establishing an attractive revenue model for the federated approach, some recommendations are proposed in the following paragraphs.

9.1 Adoption of this Master Plan by DTLF

DTLF is advised to adopt, and where necessary complete, this Master Plan, including the Index API that is configurable by the semantic model for services and profiles, as a (defacto) standard for integration of an end-user with the infrastructure provision. This should preferably be done in close coordination with all DGs and multiple stakeholders. The EU Data Space strategy should be affiliated.²⁶

In addition to the above, DTLF is advised to develop a Community visibility framework strategy for the supply chain to prevent the further emergence of a patchwork approach, which is confusing to many stakeholders. The proposed framework strategy concept should contain baseline standards relating to the required capabilities for all operators of the supply chain, as well as specific technical

²⁶ There are various initiatives for data sharing, both public – and private, like those in the context of the EU Data Strategy, IDSA, Cartena-X, and GAIA-X. These initiatives all focus on so-called 'horizontal' data sharing functionality: an architecture, specifications, and software components that can be applied by different industries. These are all data agnostics. Where the focus of FEDeRATED is on semantically build capabilities, prototypes are based on standard (open or freeware) software components. Eventually, these prototypes can be replaced by so-called data space components, if the generic interface to IT backend systems is the same, i.e. the configurable Index API. These data space components can be developed by private initiatives like the Eclipse Data Space Components or public ones, like those that will be developed by the EC SIMPEL project for cloud middleware.





rules where warranted. In all cases, the framework should allow for regular, simple updates. Overall, the proposed EU framework could greatly contribute to overall Supply Chain Visibility through collaboration with, and involvement of, stakeholders not limited to their current sphere of operation, rather reaching out to enable data sharing both within a multimodal transport perspective as well as embracing the entire chain from manufacture to delivery.

Adoption of the proposed EU framework strategy approach by DG MOVE is recommended.

9.2 Governance policy developed by DTLF

One of the first actions of a strategy is to identify the ambition of governance. What should be governed by an independent body in relation to standardization and open-source development can be explored by drafting different scenarios with evaluation criteria. Governance should be as minimal as is required.

Whereas the architecture and capability development can both be part of an open-source project, the architecture (and the multimodal ontology that could become an open standard) and its application by service developers can also be governed by an independent body like the DTLF.

Specific governance issues that should be mentioned are:

1. **Standardization** – Standardization of the semantic model (upper ontology) that is the core for capabilities, and the Index APIs is recommended:
 - a. The semantic model must be separated into two parts, namely:
 - i. Horizontal (upper ontology) – a part that is applicable to data sharing in various areas. This considers the data sharing module and the structure with ‘event’, ‘Digital Twin’, ‘infrastructure’, and ‘person’.
 - ii. Multimodal logistics – a specialization of the previous upper ontology for all modalities and cargo.
 - b. The Index API is an implementation by OAS (Open API Specification) of the data pull mechanism with events with links to data and event logic. The event logic is based on the upper ontology.
2. **Open-Source project.** An open-source project, preferably initiated in and managed by the Eclipse Foundation is a preferred option. The open-source project covers the Reference Architecture and supporting software components.²⁷

Open-source development can be with tools like Github or Gitlab. However, an open-source project requires a project manager and committers, those that actively contribute to development. Communities that are adopting the FEDeRATED architecture are examples of potential committers, but participants of EU funded projects can be requested to become committers of the open-source project during their project lifetime.

²⁷ Preferably, the open-source project is funded by its participants, either voluntarily or via EU R&D (HEU, DEP, CEF, etc.) and national funding instruments.





9.3 Adoption by first movers

Installing a program for the adoption of the infrastructure provision by first movers and its application for data requirements of supervising bodies can be beneficial. In case, DTLF/EU governance and standardization are not taking place, a quality assurance team is recommended to be established. European Mobility Data Space (EMDS) can play a role

First movers can be found amongst logistics enterprises, (innovative) software – and service providers, and supervising bodies. First movers must be willing to invest in innovative solutions, where these solutions add value to business operation. This business value or business case is about waste reduction, improved targeting, improved customers satisfaction, optimization of a capacity utilization, resilience, etc.

If governance, standardization, and open-source software development project are not (properly) put in place different implementations (fragmentation) could occur. This neither contributes to the objective of open, neutral, and trusted infrastructure provision for all nor provides a level playing field. It will lead to 'community-based data spaces' (standalone data spaces or ecosystems) that will have to be federated at a later stage. A quality assurance team might be established preventing this from happening.

9.4 Research and innovation

The continuous improvement of the infrastructure provision and its application by EU (R&D) funding instruments is recommended. Innovation is twofold, namely in supply and logistics and with respect to the infrastructure provision. EU funded projects must focus on the exploration of logistics innovation with the existing architecture and those that require the architecture to innovate. EU funded projects can be requested to contribute to the open-source project for the infrastructure provision.

Various developments – i.e., Large Language Models (LLM), AI, cloud interoperability and interoperability - will restructure IT for supply and logistics. The number of standardised services (IIS, section 6.3) will increase, a data sharing infrastructure provision will be 'smarter', etc., all contributing to a model of a 'forwarder might be incorporated into an app'. This means that a forwarder can run its business by an app on a smart device, like an ISP (Internet Service Provider) can operate a network with an app.

Some R&D features contribution to the 'Smartness' of the infrastructure provision are..:

- The **standardisation and modularisation of functionality** of an infrastructure provision implementing value added services for supply and logistics, supported by various standardized services, for instance for chain planning with LLMs. Human decision making can improve by suggestions given by a smart infrastructure. This is the basis for development of a 'Virtual Watch Tower' (several Swedish LivingLabs) or 'Cross Chain Control Center'.
- The **configurability of the provision** based on LLM. There are already LLM based chatbots for generating (SPARQL) queries to the infrastructure. These chatbots could be applied to generate event structures and directly configure the Index API. When a GUI (Graphical User Interface) also becomes more flexible, i.e., a graph-based GUI combined with a tabular one based on semantic technology, these new events can immediately be shared and accessed.





Combining this chatbot for events and data with an LLM configured for data transformation will provide flexibility for integrating with IT backed systems. The FEDeRATED semantic model functions as intermediary language for data transformation. Service development and deployment is at runtime, on-the-fly.

Existing legacy systems are the **bottlenecks** in these types of 'smart' data sharing. There are already RDF plugins to databases, but a state of the art and future research needs to be identified to overcome these bottlenecks.

- **Verifiable Credentials (VCs)** can have various roles like the one identified in this Master Plan. More common is the role where a VC contains a credential like permits, driver's license, passport, etc. These types of VCs are already considered by some EU Member States. Other types of applications of VCs are in physical access to a building or area and VCs for data access. For instance the latter could be applied by a customs authority to retrieve additional data from the infrastructure via federated querying, where only a data holder and customs can access the data and the data is not available to intermediaries. This type of data access could also be supported by so-called Private Enhanced Technologies (PETs) where data is not shared, but calculation results of the data that can be used.

9.5 EU regulatory framework

An EU framework strategy for supply chain visibility could possibly be transposed into a regulatory framework. Such a legal framework should relate to all real time data exchange operations in the supply chain being proposed (and adopted) by the EC – i.e., Customs, EMSWe, eFTI, ESG, emission monitoring, corporate social responsibility reporting in the supply chain, and Digital Product Passport. In combination, they constitute a patchwork limited in scope, and not resulting in a systematic interoperability approach.

An EU regulatory framework will at least have two benefits:

- Preventing (or remedy) a patchwork, which is rather confusing to business and public authorities, leaving them a bit clueless whether to engage towards federated data sharing.
- A solid governance, including change management system, based on interaction between the EU and the EU Member States.

A decision towards developing an EU regulatory framework shall depend on the commitment of the DTLF and all stakeholders to commit to an EU framework strategy for supply chain visibility (see 10.2). In addition, an impact assessment should be executed.

Based on the experience gained, any such community measure should at least:

- Strike a balance between highly prescriptive total visibility and the need to ensure a free flow of trade whilst allowing for a gradual tightening and harmonization of baseline data sharing standards or interoperability requirements.
- Cover all freight transport operations and a low threshold to participate.
- Ensure every operator in the supply chain is responsible for providing or using real-time data for its own actions. It cannot renounce this responsibility and be made responsible for other operators' activities. The aggregate of individual measures to manage visibility provides for the visibility standard of the complete supply chain.





- Recognize that for the execution of their public tasks, the state is dependent on supply chain visibility. Supply chain management is industry's responsibility. A cooperative state/industry approach is necessary.
- Adopt the federative approach and thereby set specific standards for operators involved in the supply chain for complying with the minimum set of capabilities of a Node to share data in a trusted and federative manner. The four capabilities required within the various business operations are:
 - Semantics – enabling operators to communicate in a common language based on linked data.
 - Service Registry – enabling operators discoverability.
 - Identification and Authentication – providing operators security.
 - Index – enabling organisations to share links to their business process data in a machine-readable format (M2M).
- Develop a governance structure both on an EU level and an EU Member State level, to provide for a change management system approach for the capabilities and to further develop the set of agreements.²⁸

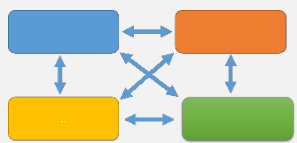

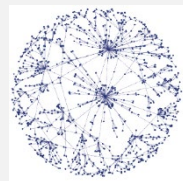
“Advice is a dangerous gift, even from the wise to the wise, and all courses may run ill,”
J.R.R. Tolkien, The Fellowship of the Ring

²⁸ An attempt for a possible EU legal framework has been developed: [An informal sketch assisting the development of a possible EU Communication and proposal for a Regulation on enhancing supply chain visibility](#) - NON PAPER, not committing the FEDeRATED partners)





ANNEX 1 THREE TYPES OF DATA SHARING

1 BILATERAL Peer2Peer	2 PLATFORM	3 FEDERATED Multiple, open, and neutral
		
One organisation shares data with another organisation through a direct link	A central entity provides the platform to which individual parties connect, enabling these parties to share data with each other, greatly reducing the links for parties to share with each other	Any party (node in a grid) is capable to non-prescribed M2M querying of any other party (node) and to share readable data through an access point with any other party, while keeping the data at source and applying security mechanisms

Data sharing Designs and the European Interoperability Framework (EIF)

1 BILATERAL Peer2Peer	2 PLATFORM	3 FEDERATED Multiple, open and neutral
TECHNICAL INTEROPERABILITY		
Message architecture	Open API	Semantics
SEMANTIC INTEROPERABILITY		
Message model	Message and Data model	Semantic model - ontology
ORGANISATIONAL INTEROPERABILITY		
Individual business case	Multi stakeholder business case	Multi stakeholder and sustainability business case
LEGAL INTEROPERABILITY		
Bilateral agreement	Platform setting	Transnational agreement – possibly legal setting





The Design Characteristics (including pros and cons)

1 BILATERAL Peer2Peer	2 PLATFORM	3 FEDERATED Multiple, open and neutral
IDENTIFICATION & AUTHENTICATION		
<ul style="list-style-type: none"> • Use webtokens or Open OAUTH standard 	<ul style="list-style-type: none"> • Use webtoken or Open OAUTH standard • Platform can provide security in a data space. • Verifiable Credential (VSs) issued by Registration Authorities can be applicable 	<ul style="list-style-type: none"> • Must apply independent mechanism. • Requires application of Verifiable Credential (VCs) issued by Registration Authorities
LINKING WITH EXISTING PLATFORMS		
<ul style="list-style-type: none"> • Not easy – an agreement on what and how is needed 	<ul style="list-style-type: none"> • Linking to central platform required • Easy - Message exchange through platform between already connected parties 	<ul style="list-style-type: none"> • Quick linking possible due to M2M prepared linking to new parties
UNAMBIGUOUS CONCEPTUAL FRAMEWORK		
No: must be discussed specifically	Yes: enforced by message format standard	Yes
DATA DIRECTLY FROM SOURCE		
Yes	Yes	Yes
ADVANTAGES		
<ul style="list-style-type: none"> • Easy to implement for limited number of links • Often adopted and implemented in supply and logistics. <ul style="list-style-type: none"> • Trust is no issue • Liability clear 	<ul style="list-style-type: none"> • Easy to connect many parties • Large variety of interfaces (often API) between organisations • Wide range of standard services • Secure data and data communications <ul style="list-style-type: none"> • Liability clear 	<ul style="list-style-type: none"> • Data at source • Scalability • Open to all based on set of agreements. • Interaction patterns for data sharing of real-world objects and their status (Digital Twins, events), makes it possible to fully digitize processes. • Low risk vendor lock-in due to open standards
DISADVANTAGES		





<ul style="list-style-type: none">• Complicated and time consuming to scale-up• Management issue (many links)	<ul style="list-style-type: none">• Limited space for innovation• Hard to deviated from existing services• Follow data sharing rules• Often conservative business model• API requires IT investments (SME problem)	<ul style="list-style-type: none">• Technology under development• Few semantic industry standards available• Liability issues need set of agreements• Generic governance model
--	--	---





ANNEX 2 DIGITAL COMPETENCE

A challenge in supply chain and logistics operations is creating a level playing field where all operators can participate in data sharing. Especially, the dominance of strong organisations and platforms on SMEs to implement a large variety of solutions must be addressed. The annual report of the European Commission states that SMEs make up over 99,8% of all business in the EU²⁹.

In general, SMEs lack digital leadership skills at the top, a shortage of IT professionals, and adequate skills amongst users. Skills shortages, gaps and mismatches hinder organisations to define their growth strategy, to implement it, and to enable employees to use new technologies³⁰. Online platforms can be a great solution for SMEs to increase their customer base, reach scale without mass, find innovation opportunities and assets, and access digital solutions and business intelligence services³¹. They can also provide important channels for growth to SMEs “going digital”³². However, SMEs face challenges and risks in operating on online platforms. The lack of digital skills and the need to adapt business models can be important barriers. Fee structures of the platforms and the sharing of sensitive business data with implicit acceptance of matching algorithms on which SMEs have no influence or even information also present challenges. There are also risks related to digital security, competition distortion and possible lock-in effects.

The development of the competences and the enabling mechanisms go hand-in-hand. The one does not go without the other. In practical terms:

1. The **enabling mechanisms** assist companies and public authorities to:
 - Connect with any IT platform;
 - Know what data and which stakeholders are trustworthy;
 - Find the data they need to;
 - Know the IT system requirements;
 - Translate paper information into data.

This Master Plan mainly deals with the enabling mechanisms.

2. The **competences** of companies and public authorities to engage within a grid empowering them to answer questions like:
 - Why don't I know what my clients will order tomorrow?
 - Where are my goods actually located?
 - Why is it impossible to produce an actual sales report?
 - Why does my planning always gets mixed up?

²⁹ European Commission and Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs and Joint Research Centre and Di Bella, L and Katsinis, A and Lagüera-González, J, Annual report on European SMEs 2022/2023 – SME performance review 2022/2023, Office of the European Union, 2023.

³⁰ European Commission and Executive Agency for Small and Medium-sized Enterprises, Skills for SMEs – Cybersecurity, Internet of things and big data for small and medium-sized enterprises, Publications Office, 2020.

³¹ OECD, The Digital Transformation of SMEs", 2021 (<https://www.oecd-ilibrary.org/content/publication/bdb9256a-en>).

³² World Bank, Trading for development in the age of global value chains, 2020 (<https://www.worldbank.org/en/publication/wdr2020>).





- Why is my forecast so poor?

This competences relates to the issue of digital readiness.

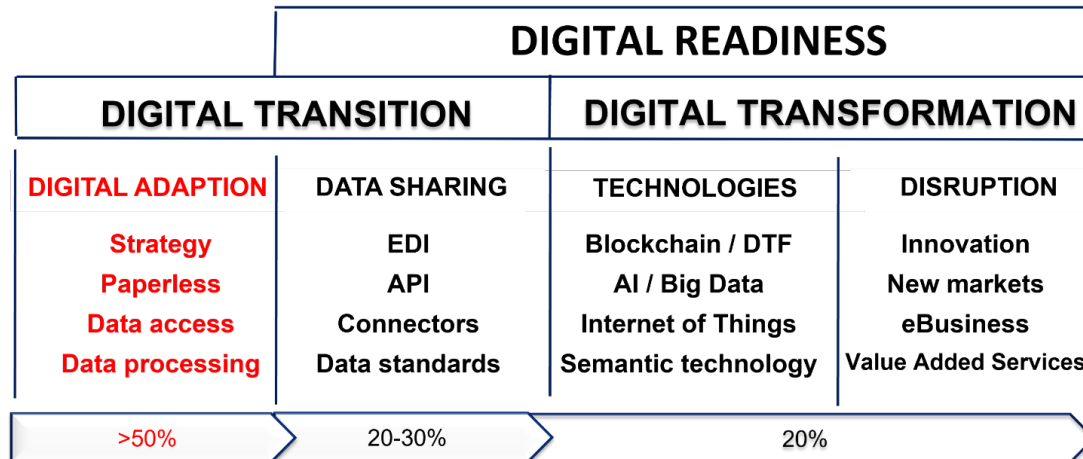


Figure Maturity level of Digital competence

The above figure illustrates the level of maturity of various companies relating their digital competence – digital readiness. It shows that most companies are not ready for data sharing yet. Digital adaptation is a bridge to cross. Over 50% of companies and public authorities are not sufficiently digital ready yet. The figures are based on a dutch questionnaire involving 380 companies, most SMEs, executed in 2021.³³ A Finnish logistics digitalization study from May 2019 pointed out similar results and findings. Although, the management level is already internalized the benefits of digitalization and data sharing, those has not yet achieved the level of implementation. Based on the survey results the digital readiness level and capability to utilize digital tools and data sharing solutions gets weaker, when moving down on company hierarchy from management to operative levels. However, the same survey pointed out that the importance of these topics has already flowed through organisations (From fragmented to distributed, from documents to data, from an actor centered approach to interoperable ecosystems).³⁴

³³ [Digital readiness NL market survey 2021 \(federatedplatforms.eu\)](https://federatedplatforms.eu/digital-readiness-nl-market-survey-2021)

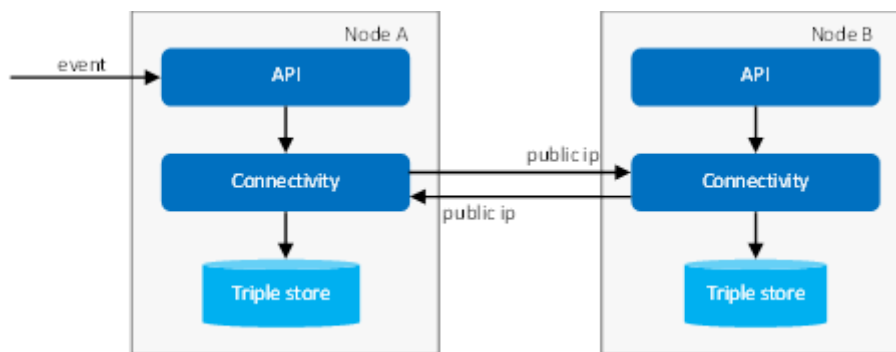
³⁴ [Finnish Transport and Communication Ministry 2019:12](#)



ANNEX 3 NODE INSTALLATION

There are a few steps that need to be performed to successfully install a Node. A Node is composed of several components; all these components must be installed by each of the participants in the network. After successful installation of the components a Node has to perform a registration process in order to be able to participate in the network. During this registration process a Node acquires a certificate required for identification and access to the network.

Nodes communicate with each other over TCP (Transmission Communication Protocol)³⁵. A Node needs to have at least a (public) IP address on which it can be reached by other nodes in the network. A Node stores the events it sends and receives in its local (GraphDB) triple store with the semantic model. The Node API can be configured to support events; it will not perform any validation or data transformation when not configured.



Example of two nodes, the components and communication between them.

For ease of installation, all components are made available as containerized images. The following images must be installed and configured for each Node:

- API
- Connectivity component
- Triplestore

Specific images are hosted on Docker hub: <https://hub.docker.com/u/federatedbdi>. Installation and configuration instructions are available on: <https://github.com/Federated-BDI/Docker-BDI-Node>.

There are Helm scripts available for installation of a Node on a Kubernetes cluster: <https://github.com/Federated-BDI/Kubernetes-BDI-Node>. Note that these scripts might have to be modified to match specific infrastructure requirements.

³⁵ TCP – The Transmission Communication Protocol is an important part of the Internet protocol suite. It is a transport layer that facilitates the transmission of package from source to destination.

