INTERIM MASTERPLAN

Final version

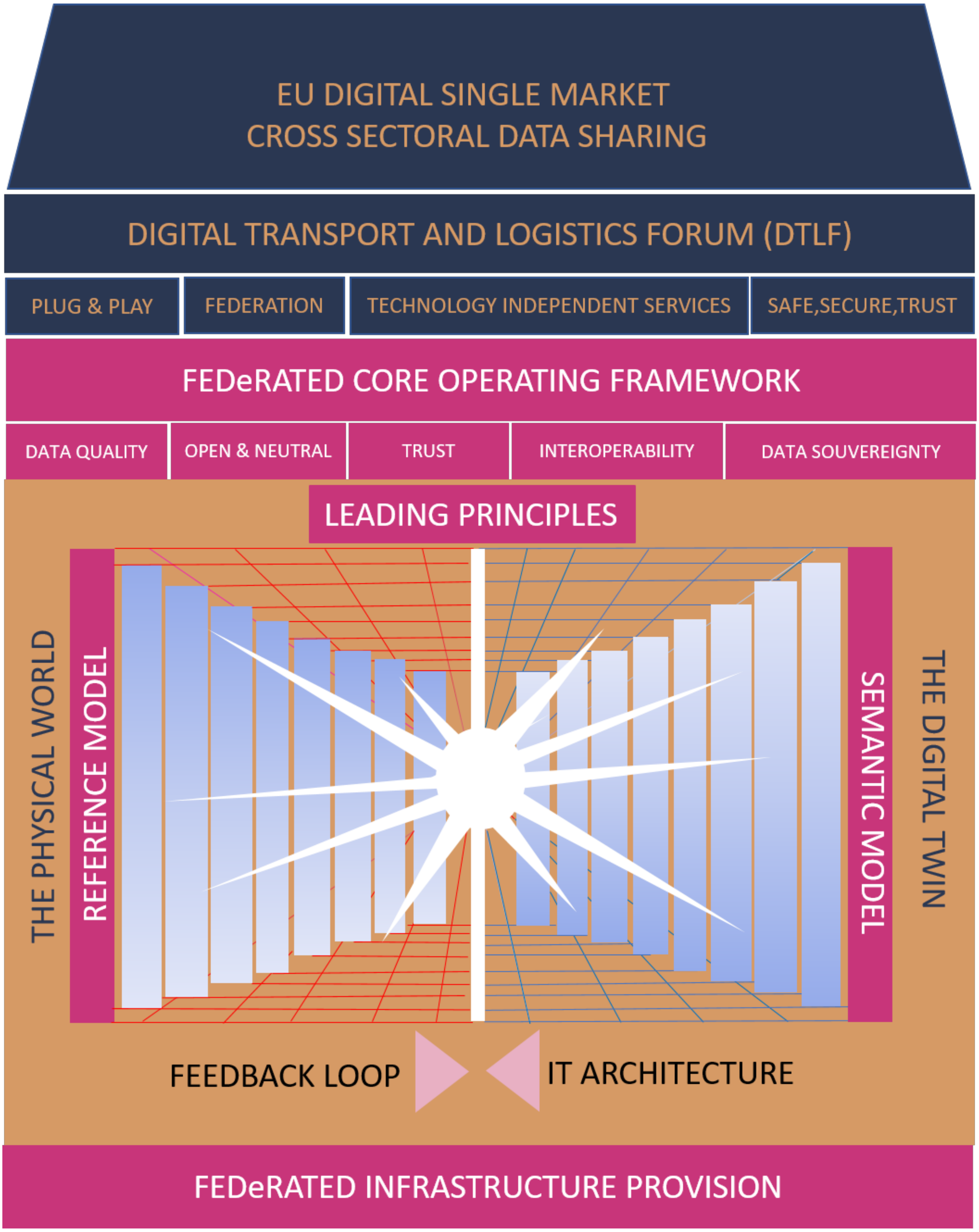
FEDeRATED MILESTONE 2

27 March 2020

www.federatedplatforms.eu

FEDeRATED
NETWORK OF PLATFORMS

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



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. www.federatedplatforms.eu

TABLE OF CONTENTS

INTRODUCTION 4
1 GLOBAL CONTEXT 6
1.1 The virtualization of transport 6
1.2 The EU Single Digital Market 6
1.3 The emergence of the data sharing theme 7
2 DIGITAL TRANSFORMATION 9
2.1 The Core Operating Framework 9
2.2 Supply and logistics chains 9
2.3 Key business process elements to be covered 12
2.3.1 Shared behaviour of enterprises 12
2.3.2 Shared behaviour of authorities towards supply and logistics chains 13
3 REFERENCE MODEL 14
3.1 Overview 14
3.2 Examples of use of the reference model 16
3.3 Events in the reference model 17
4 LEADING PRINCIPLES 18
4.1 Introduction 18
4.2 The principles 19
4.3 Compliance with existing rules 24
5 THE SEMANTIC MODEL 26
5.1 Overall structure of the semantic model 26
5.2 Details of the semantic model 27
5.3 Detailing and applying the model 32
5.4 Business services 32
5.5 Dates and times in logistics 33
5.6 Cargo perspective 34
5.7 Transport means perspective - itineraries 35
6 FEDeRATED IT ARCHITECTURE 38
6.1 Federated platform 38
6.2 Services provided by a Federated Platform 41
6.3 Requirements for data, application of standards and API’s 43
6.3.1 Data 43

6.3.2 Standards 46
6.3.3 API layering 47
6.3.4 Protocols, Semantics and Distribution 50
6.3.5 Aspects of APIs 50
7 VALIDATION PLAN 51
8 NEXT STEPS 53
8.1 Related Milestones 53
8.2 Next Steps 53
Governance issues 54

INTRODUCTION

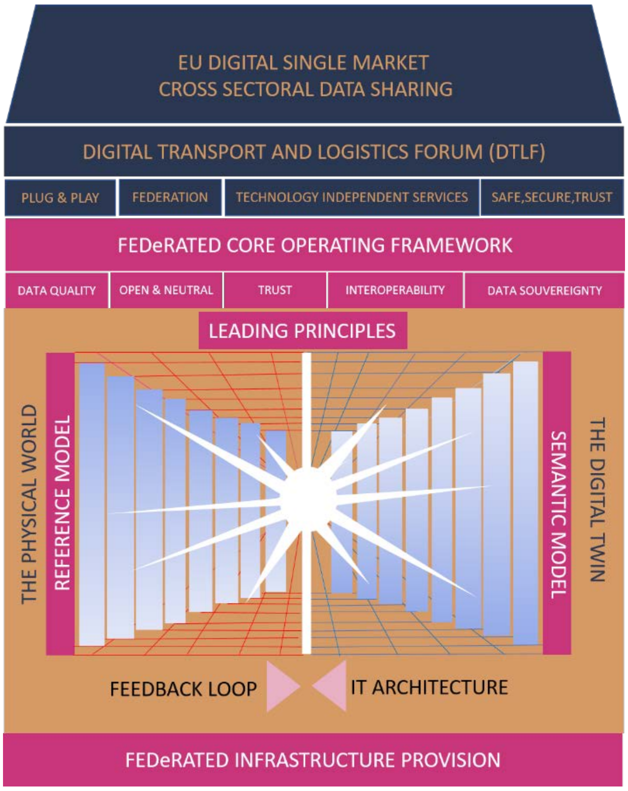
This document contains the FEDeRATED Interim masterplan 2020. It should be considered as a state-of-play and living document. Benchmark date: 30 March 2020. The aim is to assist the EU Member States and business to build a future proof federated network of platforms for data sharing in logistics and freight transport.[1]

The major question this Interim Masterplan tries to answer is: ***How to build a data sharing infrastructure provision for freight transport and logistics in the EU?*** This Interim Masterplan is a first step towards answering this question. The FEDeRATED project will try to fully the answer this question on a systematic basis between 2020-2023. The answer will depends on shared knowledge, consultation, coordination, human resource management, validation through pilot projects and living labs and openness towards different appreciations on to effectively build this infrastructure provision.

The underlying issues at stake are complex. Logistics constitutes interactions between an unlimited number of companies, public sector authorities and other stakeholders. They all constitute the global context for technology, supply and logistics chain insights and policy approaches.

In order to be able to build the FEDeRATED infrastructure provision this Interim Masterplan:

1 Sets the context of the work, i.e. the EU Digital Single Market. Elaborates on the DTLF building blocks and FEDeRATED Core Operating Framework
2 Provides a generic description of supply and logistic chain realities that can all benefit from data sharing in logistics
3 Proposes leading principles that serve as a guide to formulate the boundaries, the services and the functionalities for a data sharing infrastructure provision
4 Presents a reference model that describe the actual world components that require a digital twin
5 Describes a semantic model that allows the reference model to be translated into data
6 Proposes elements of building for developing an IT architecture with a focus on interoperability and data sharing.
7 Identifies the validation criteria for pilot projects and living labs (feedback loop)
8 Shows a list of next steps for further action between 2020-2023



[1] , in accordance to the EU DTLF (Digital Transport and Logistics Form) report of 2018 and its current work on data sharing and the FEDeRATED Vision document of 17 December 2019.

This Interim Masterplan constitutes the basis that requires validation in the coming years through projects and further collaboration. It presents the fundamentals of how a FEDeRATED data sharing infrastructure provision can be build 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?

This Interim Master Plan will be validated in 2021, 2022 and Mid 2023, based on new insights, i.e. based on lessons learnt in various projects being developed and executed within the context of the FEDeRATED Action and the DTLF framework (EU Digital transport and Logistics Forum). The validation process might enable the process to develop specific technical, functional and organisation requirements. The current state of play in developing a FEDeRATED infrastructure provision does not allow yet for a specific list of these requirements. Many provisional requirements can be derived out of the presented Leading principles and Reference Model. However, a provisional requirement is useless. The definition of a requirement requires validation. This is not the case yet, but will be in 2023.

The FEDeRATED Action is a CEF Action ((pre-)implementation study) and not a Horizon 2020 research project. The goal is to practically show how data sharing could work. Therefore, the Interim Masterplan main report is presented as a “How to” (shortcut) guide. The chapters 1-7 are the main section of the report. This Interim masterplan report as well as its Annexes elaborating on various elements identified in the main report, can be accessed on the FEDeRATED website, www.federatedplatforms.eu, (menu: library, milestone reports).

The partners of the FEDeRATED Action aim to realize a future proof data sharing environment within their different business processes. Thereby international, EU, national and local legislation and practice should be taken into consideration.. The FEDeRATED preferred option is to interact and engage many stakeholders by also providing this guidebook. The understanding being that this guidebook is not 100% bullet proof. The proof of the pudding is in the eating, based on projects, assessment of other ongoing practices and agreed and common knowledge.

1 GLOBAL CONTEXT

1.1 The virtualization of transport

On a global and regional level, administrative procedures have been established for freight transport and logistics. On a global level, the various transport modes are regulated within the United Nations framework and are also addressed by the WTO, WCO, ISO and other international fora. On a regional level, various policy considerations and legislation exist within the context of the EU and its EU Member States, EU neighbouring states and on a local level.

In transport, the traditional role of public authorities was to provide for the physical infrastructure – developing, building, and maintaining - and to foster safety of traffic, later elaborated by various sustainability criteria. Due to the substantial increase in freight transport, also leading to substantial congestion problems, and the emerging role of IT, public authorities have obtained responsibilities for virtual infrastructure development.

Supply chain business interoperability increasingly depends on seamless data interconnectivity. This has led to new collaboration concepts, platform development and different roles of the traditional logistics operators, including public authorities. Digitized services are fostered to pursue smart mobility solutions leading towards a next level of customer integration into the supply chain (supply chain excellence)

The effective exchange of data, including the proliferation of data requirements by various service providers, has become a major management concern and challenge for both the public and private domain. An agreed balance between the modernist realm “Less is more” and the postmodern “Better be safe than sorry” has not emerged. The answer depends on a sound analysis of problems, interests, definition of responsibilities and assessment of the outcome of technology investment.

1.2 The EU Single Digital Market

Since the turn of this century, various EU legal obligations require EU Member States to establish harmonized procedures for the electronic submission and transmission of legal obligations. Seamless – electronic data interconnectivity, in global supply chain management within the business community, is an important feature for already some 20 years. Due to high investment costs and the non-standardized procedures, many SME have not found sufficient opportunity to allocate much time and money into upgrading their business into a data driven business process.

The previous Juncker Commission and the current Von der Leyen Commission have put digitalization of Europe, including freight transport, into the heart of their policy agendas. In 2015, the development of an EU Digital Single Market features as an important EC policy pillar. In this perspective, the Digital Transport and Logistics Forum (DTLF) was established. The DTLF contributes to establish a sound basis for applying a digital-by-default principle in logistics and freight transport within an EU Digital Single Market. Apart from identifying the need for paperless transport – both for cargo, persons and transport – during its first mandate DTLF developed the data sharing design principles, not the least to support sustainable implementation of current EU legal acts, i.e. Regulations for EMSWe and eFTI, and enable cross-sectoral data sharing. The four design principles are plug and play, federation of networks, technology independent services and trusted, safe and secure.

The Von der Leyen Commission fully pursues the need to develop a greener image for freight transport and promote multimodal transport operations. The EC Green Deal and Data Economy Communication shall have a big impact on the execution of this Interim Masterplan. Within the concept of a functioning internal market it is also very important to take all EU companies on board, including SME. In general, the level of the EU SME digital maturity is not very sophisticated yet.

1.3 The emergence of the data sharing theme

Over the last two decades, data flow management has become increasingly important and complex. Public transport policy strategies have indicated the need to synergize the data requirements requested in the public and private domain. In order to facilitate trade and freight flow management processes, the need for further simplification of reporting requirements and the reduction of the administrative burden within the Customs domain and various transport related issues - like maritime transport, waste transport, transport of dangerous goods - have emerged. Legislation was developed in direct response to these strategies.

As an outcome of the process towards simplification, the need to establish a lean and mean approach to facilitate seamless transport and an eGovernment perspective has also been identified, both on a global as well as regional level. 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 hand-in-hand. A digital infrastructure can solve current bottlenecks in the physical world, also by creating a digital twin.

The FEDeRATED Vision (Milestone 1) is **to provide for an infrastructure provision containing a set of arrangements 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.** The Vision document also identifies the Core Operating Framework, within the FEDeRATED Vision has to be developed and materialize**.**

This FEDeRATED infrastructure provision covers various dimensions, thus stakeholder interests. To mention the most common:

1. Public authorities, policy as well as law enforcements agencies, inspections, Port administrations Customs;
2. Supply and Logistic chain operators – terminal operators, transporters (seagoing maritime, rail, hauliers, inland navigation, aviation), forwarders, shippers, sellers, consignors and buyers, private port operators;
3. IT companies (software and hardware);
4. Additional service providers, i.e. PCS;
5. Scientists and researchers;
6. Consultants;
7. Standardization organizations (ISO, CEN, GS1).

DIGITAL TWIN IN FREIGHT TRANSPORT AND LOGISTICS

Moving cargo is a very physical business. Cargo is physically picked up at a real warehouse, lifted into a heavy truck, and transported to another real-world location. What could be more down to earth and real than moving cargo? It is not surprising that a lot of paper documents are still used to support logistics and transport processes. Or is it? Virtually every part of the logistics and transport business is rapidly pursuing digital transformation and every part of the process is being digitalized, leading to the concept of ‘Digital Twin’. When we take a closer look at paper documents, we’ll see that these were almost certainly prepared using for instance a sophisticated Enterprise Resource Planning (ERP) - or some similar system. Therefore, paper documents have digital origins representing the physical, real world. Its Digital Twins, to be precise. Digging a bit deeper, we’d see that the entire process around these documents, like planning, booking, tracking, invoicing etc. are all supported by similar enterprise systems. Therefore, these real processes also work with Digital Twins of the real world: cargo, trucks, containers, vessels, airplanes, etc.

Digital twins are a big thing because unlike their physical counterparts, they are not subject to the limitations of gravity, space and time. Digital twins are a data – and process representation of real-world objects, where the data can be accessed from anywhere in the world at any time and that’s just for starters. Things get more interesting when we equip the cargo itself with sensors that determine its geographical position and the condition of the contents such as temperature and humidity of flowers or pharma products. We can detect the wellbeing of animals being transported or the security of valuable shipments. Now we can check exactly how our cargo is doing without the need for a local pair of eyes. This idea is further extended to the equipment used for transport. Containers are being equipped with sensors. As are the trailers that they are on and the truck or train itself or the airplane or vessel it is transported on. Anything and everything that is used for the movement of cargo is increasingly paired with a Digital Twin, having computational capabilities themselves based on assessing their environment by means of sensors like camera’s and other devices. It not only allows to assess and share data about the real world, but also supports predictions and prescriptions for behavior like Estimated Time of Arrival and dynamic planning. Certificates, logs, identity, etc. digitally represent people as the last member in the family of digital twins. The drivers, pilots, safety inspectors and anyone that is part of the process.

Why do we need Digital Twins?

It may seem obvious that in a world where our private lives are entwined in a digital world of social networks, online shopping, dating, entertainment etc., that a digital twin of the logistics and transport chain is a real thing. True, but the motivation goes much further.

For the past couple of decades, supply and logistics has been working on digitalizing its artifacts and processes and the reason was always the same: accelerate information such that cargo can move seamless and be handled more efficiently. This has been shown to work but it turns out that digital twins can go a lot further than just speed and efficiency.

Think back to your digital private life. At first, we had email and electronic newsletters, now we have multiple avatars, identities, roles, social status, etc. in a variety of social networking platforms.

Supply and logistics is currently (still) at that email and newsletter stage. Going forward, digital twins will transform this into a data space where customers can explore options from 360 degree omniscient viewpoints. They will be able to consider thousands of scenarios for their freight as it moves and respond to issues in real time. They will be able to deploy AI bots to keep an eye on their goods and operations, in future implement at that level, whilst they focus on future strategies.

Imagine that every organization in supply and logistics has this sort of access to data. Not only will every digital twin of every physical artifact, process or thing be at their fingertips, they will be able to create virtual constructs that reflect the way they think about their business. Shippers will see their complete supply chain as a constructed digital twin. Warehouse managers can navigate around their virtual storerooms and see a timeline of its occupancy. Carriers will see their transport equipment on a map or they can see where each vehicle is in the maintenance queue. Customs officers will a flux of goods starting from manufactures long before it reaches their borders.

2 DIGITAL TRANSFORMATION

The FEDeRATED Vision aims to develop an infrastructure provision that enables current bottlenecks in the physical world to be resolved through data sharing. This digital transformation requires the use and integration of digital technologies into existing (and new) business processes as well the four layers of the European Interoperability Framework (EIF), namely: legal, organisation, semantic and technical interoperability

2.1 The Core Operating Framework

The Vision identified a Core Operating Framework for FEDeRATED. This constitutes:

- the key principles that need to be adhered to in order to ensure that the interoperability issues are safeguarded in such a way as to enable a federated network of platforms approach;
- the high-level requirements that should be applicable to the interoperability layers and be constraints to formulating the leading principles as part of the FEDeRATED Master Plan.

The Vision identified that the further development of a federated network of platforms has to rely on the comprehensive consideration of certain definable design requirements as well as legal and organisational boundaries, constituting the following key principles:

1. ensure data sovereignty;
2. create trust among platforms and participants;
3. provide a framework to enable interoperability;
4. be open and neutral to any participating party;
5. ensure data quality

Within the context of these key principles of the Core Operating Framework the following issues have to be developed:

- coherent and comprehensive legal interoperability requirements;
- governance;
- organising principles;
- layering approach;

To this end the FEDeRATED Leading Principles should support and further elaborate on the key principles and supporting issues as identified above.

2.2 Supply and logistics chains

An infrastructure provision adhering to the FEDeRATED principles supports data sharing between business processes of various stakeholders involved in supply and logistics. FEDeRATED will allow for:

- smooth interaction between and among the different logistic chain operators and public administrations involved;

- enterprises to optimize their supply chains to achieve seamless goods flows;
- dynamic planning to enable various ways of collaboration and optimize capacity utilization;
- recognizing existing (partial) systems;
- streamlining multimodal transport;
- decreasing or removing costs derived from lack of interoperability.

The following figure depicts an example of a multimodal logistics chain, a road transport of consignments from a shipper to a stuffing center. Containers, with one or more consignments of potential different shippers, are carried by barges to a port of loading. Vessels transport containers to many ports, based on a voyage scheme. Transport to the hinterland is covered by rail to a stripping centre and the consignments are shipped to their final destination by road.

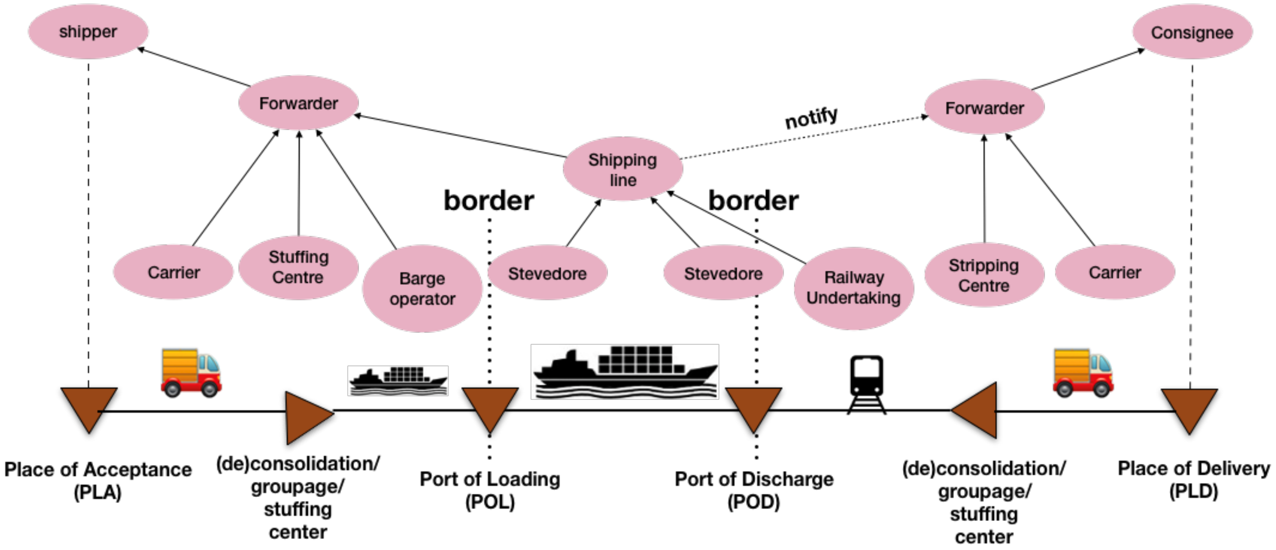


Figure 1. An example of a multimodal logistics chain,

Figure 1 illustrates the hierarchical relationships between the various stakeholder (roles) involved in transport. For instance, a forwarder in a country of exit manages the transport and stuffing of shipments to a POL, including the booking and ordering of transport by a shipping line. A shipping line always has contracts with stevedores in each port.

An overall picture of all supply and logistics to be covered by a FEDeRATED infrastructure provision cannot be drawn. Many different chains are executed and developed on a daily basis by a multitude of operators. The following parameters determine the number of variations of business scenarios or chains:

- Type of goods or commodities – particular type of goods may require additional procedures and formalities. For instance, agricultural goods require a Certificate of Origin by a national Food and Safety Authority. Other types of goods may be subject to re-export formalities resulting in additional details to be provided to an authority. Different authorities may also align their inspections, resulting in what is called coordinated border management.
- Handling of cargo – the cargo might require specific handling like transport of temperature-controlled cargo. Yet dangerous cargo may not be stowed with other types of cargo or may only be transported on certain routes.

- Authorities – there may be different authorities responsible for the safety and security of the infrastructure, e.g. port authorities, (air/sea/rail/road/inland waterways) infrastructure managers, maritime authorities. These might be private, public or mixed facilities. The Rotterdam Port Authority for example has a private and a public function, while UK ports are run by private organisation called “port companies”. This will result in additional interfaces.
- Cargo movement - Authorities may impose restrictions on cargo movement, either based on (inter)national regulations or local decisions made by for instance city councils. Access restrictions to city centres are examples of the latter. These restrictions must be made known to supply and logistics enterprises in such a way that they can be configured in their decision support - and planning IT systems.
- Insurance and payment – insurance companies and banks can be introduced addressing insurance and payment of transport charges. This again will lead to additional information flows.
- Incoterms – these may differ for different modalities and/or types of goods. For instance, the Dutch Flower Auction as one of the main global hubs of flower trade and transport has other terms and conditions than the Incoterms. The Incoterms themselves may also lead to different responsibilities and payment structures, thus resulting in other configuration of logistics chains.
- Hinterland transport – the hinterland transport, pre- and on-carriage, may be carried out by two or more modalities, resulting in additional coordination needs of a forwarder arranging and controlling the hinterland transport. The planning of the hinterland transport and its adaptation (changing from a mode to another) based on the availability of the infrastructure, congestion etc. (synchromodal planning) creates enhanced information needs and interfaces.
- Transport modes and nodal points – each mode or nodal point has its own IT systems and interoperability solutions, for instance ports and airports might have their community systems, inland waterways have River information Services to support traffic management, and road transport has national gateways for road traffic information. These systems can be used to assess the status of flights, congestions of the infrastructure, locating barges, booking air transport, etc.
- Combined services – large LSPs offer combined services at a global scale with potentially their own transport means. They have for instance their own vessels, trains, trucks, airplanes, and barges, and provide transport – and customs services. They may also own particular hubs for specific cargo types, e.g. distribution of packages. These LSPs acts as single point of coordination to shippers and consignees and combine various roles. In case of the example, a forwarder might for instance combine import and export and may have its own trucks for pre- and on-carriage.

  Besides forwarders, shipping lines also provide this functionality. They distinguish for instance between carrier – and merchant haulage: in case of carrier haulage, the shipping line organizes hinterland transport (door-to-door) and in case of merchant haulage, the shipper or consignee is responsible.

  Since these combinations of roles are feasible, the proposal is not to distinguish roles but identify business services provided by all types of organizations. Particular data governance rules might be applicable to these services, for instance transport services are not allowed to have the details of the cargo, whereas customs services require the details. These types of rules have consequences for an enterprise.

- Systems innovations – introduction of new (innovative) IT systems like visibility solutions integrating with IoT (Internet of Things; an OBU system is an example for road transport) and eTransport Documents will add complexity to the landscape of the IT infrastructure. It will lead to additional interoperability requirements and integration effort of IT back office systems.

Besides the diversity of supply and logistics chains based on the previous variations, each chain will also have a variety of interaction sequencing. In the previous example, for instance, a shipper orders transport by a forwarder, where the forwarder orders main transport by sea based on port call information and arranges transport to the port. Since sea transport is containerized, cargo has to be stuffed in a container and the container has to be transported to the Port of Loading. So, a road carrier will receive a transport order to pick up the cargo and transport it to a stuffing center. The stuffing centre will receive an order to stuff cargo in container(s), and so on.

Furthermore, enterprises of different size and different IT maturity levels participate in these supply and logistics chains. For instance, large shippers, forwarder, and carriers share data with a large number of smaller carriers for last mile deliveries. The FEDeRATED infrastructure provision has to deal with all stakeholders (level playing field).

The sequences of interactions between stakeholders in supply and logistics chains are based on the fact that each participating organization is autonomous: it makes its own decisions according to its outsourcing strategies and has implemented its own business processes. To have them remain autonomous, any internal strategies and process implementation are outside scope.

2.3 Key business process elements to be covered

In supply and logistics chains, organizations share data to support and optimize their business processes. Therefore, the behaviour of business processes of organizations has to be considered and supported by a FEDeRATED infrastructure provision. The subsequent shared behaviour of business processes relates to the following (provisional list):

2.3.1 Shared behaviour of enterprises

- Publish, search, and find business services, available capacity, timetables, etc.;
- Business services to be covered are at least: transport, transhipment, and warehousing;
- Stuffing and stripping, cleansing, etc. are considered as additional business services;
- 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);
- 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 that is required for planning – and operational purposes (resilience);
- Compliance with reporting requirements.

2.3.2 Shared behaviour of authorities towards supply and logistics chains

- Border control processes for cargo or passengers, with any means of transport ((deep sea/short sea) vessel, airplane, truck, barge, train);
- Safety and security processes 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 cargo/passengers;
- Publication of any data that would improve logistics processes given legal constraints.

3 REFERENCE MODEL

3.1 Overview

In Chapter 3 the real world has been described. A mirror is required to transfer this real world into a virtual world. Therefore, you need a reference architecture, i.e. a model. The FEDeRATED reference model addresses basic physical activities like transport and transhipment of cargo, where various stakeholders share data to coordinate their various activities. Figure 2 shows these main aspects.

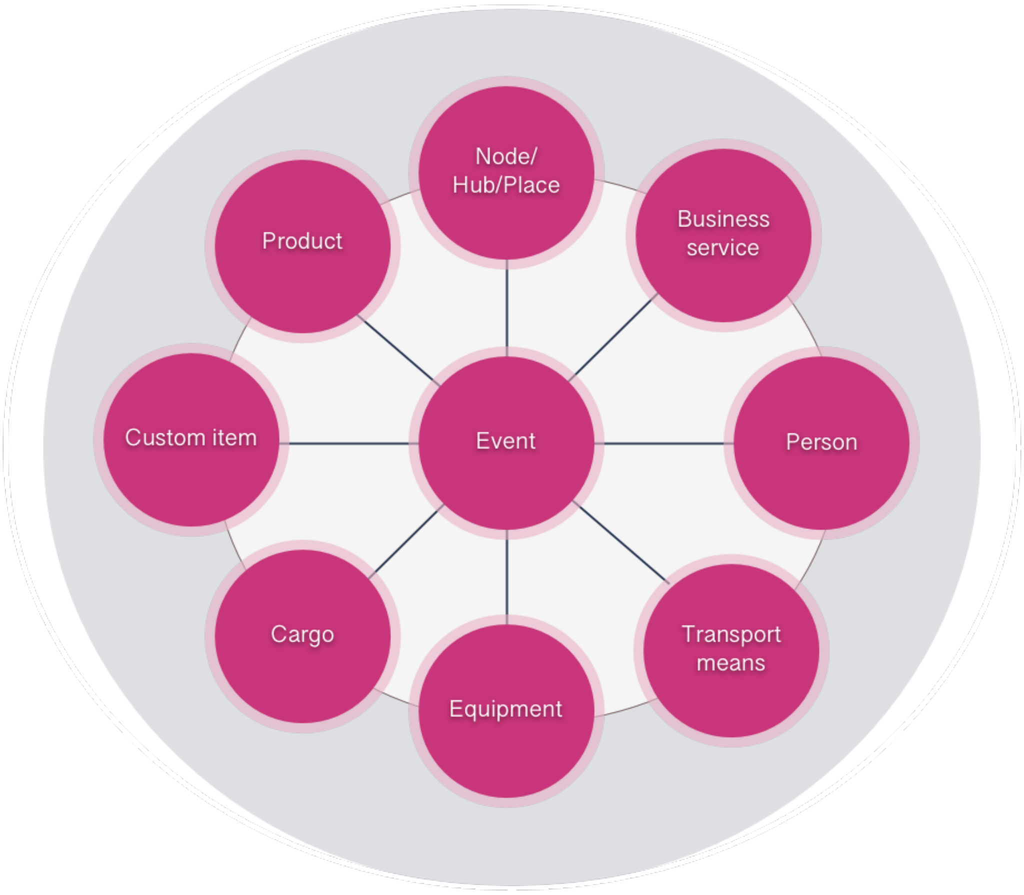


Figure 2. The main concept of the FEDeRATED Reference Mode

The main transport concepts are described as follows; they will be refined by the pilots and Living Labs:

- Area of interest (hub/node/place/..) – a terminal, location, port, city centre, etc. where a cargo physical activity like transhipment or storage can take place. It can also be a border crossing, facilities in the infrastructure like locks or bridges, or a city centre with certain access restrictions. A node will have a name in the context of a particular transport activity, e.g. a Port of Call for a vessel, a Port of Loading to indicate where a container is (to be) loaded onto a vessel, or a Place of Acceptance to indicate the origin of the cargo, i.e. the place of acceptance is known as the place where a carrier or forwarder takes over responsibility of the cargo from a shipper.

- Cargo – the goods that are transported from origin to destination. Cargo may be bulk or containerized. Cargo is defined by generic description of products that are transported such as fruit or textile. Cargo can be packed, repacked, consolidated, reconsolidated etc. Trailers may be a transport means but can also be cargo itself, on a vessel for example.
- Transport means – these are the vehicles that transport the cargo, such as tricks, vessels, trains, airplanes, barges etc. Each transport means has a specific transport mode; some might have more than one mode.
- Business services - the commercial relations between any two enterprises in a chain based on business services. A business service is the basis for several business transactions, for instance a shipper will have several business transactions with a forwarder over time. Data that is shared may form the basis of documents that are required for regulatory or legal reasons.
- Products – the actual objects that change ownership between a seller to a buyer. For transportation purposes, products are packaged as general cargo that can be loaded into containers.
- Customs item – the classification of products or cargo for customs purposes according the Harmonised Systems codes (HS). One can basically have three classifications: export, import, and incoming/transit. Export and import relate to products and incoming/transit to cargo.
- Equipment – any asset used to facilitate transport and handling of cargo.
- Person – any individual that is a crew on board of a transport means. A crew, a person can have a role, e.g. a truck driver or captain. These roles also relate to qualifications.
- Events represent actions, milestones, transactions or any other real-world activity. These will typically involve one or more interactions or associations between location, business service, transport means and cargo. For instance, a vessel is expected to arrive at a given time in a port. Similarly, for a container: which will be loaded on and discharged from a vessel in ports.

This transport model is further refined:

- Area of interest – these are refined according their logistic function, e.g. port, storage, transshipment, production, or infrastructure function, e.g. a road, a city center, a river, railway track.
- Cargo –these are refined into general cargo (pallets, packages, etc.), bulk cargo (oil, grain, etc.), and containerized cargo. Note that also a transport means can be cargo, e.g. trucks on a ferry (ro-ro).
- Transport means – these are fined into vessel, truck, barge, airplane, and train for each of the transport modes. Further refinements can be made such as for vessels into deep sea and shortsea vessels, and ferries.
- Business services – these are refined into transport, transshipment, storage, administrative services, etc. Additionally, these include the process aspects like business transactions (booking, ordering).
- Equipment - can be refined in for instance container, ULD, trailer, and wagon.

These refinements imply additional business constraints. For example, containers can only be transported by vessels equipped for container transport.

3.2 Examples of use of the reference model

The reference model can be viewed from different perspectives, based on evaluating the event association between various concepts. 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.
- Document data sets – 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 data set – a data set combining operations on cargo and a transport means at particular locations. An itinerary has links to cargo data, transport means, and nodes; 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 during 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 eMSW 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

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

Examples like the previous ones are the basis for developing Application Programming Interfaces (APIs):

- For instance, an API for booking of a transport means can be specified based on location, cargo and the requited transport means.
- Another API query may support the route and a third the cargo carried by a transport means.
- An eFTI API will cover a transport means (a truck with its licence plate), its itinerary (trip) with locations for loading and unloading particular cargo, and, from the cargo perspective, links to eCMR data sets stored by an eFTI platform.
- An eMSW API will have a transport means and one of its port calls that is of interest, the relevant data of cargo on-board and cargo to be loaded/discharged in the port and provide an overview of passengers and crew. In case the cargo is containers and the port is the first port of call in the EU, the eMSW API will also provide the content of containers by their TARIC code. In the latter case, one container will have one TARIC code, meaning that there will be one customs item for each container

These APIs can be predefined at different levels. For instance, each stakeholder requiring access to data can define and publish its query for eFTI and eMSW queries that are formulated at EU level.

3.3 Events in the reference model

Events are an important concept. Collectively, these events form the lifetime of these interactions and associations. For example, an association between a container and a vessel is created after loading the container on a vessel and ends after its discharge. These interactions and associations start and end with milestones, which are physical action. High level milestones are:

Generic milestone	Description
Arrive	A transport means arrives at an area of interest at a time. In case this area is a terminal, the milestone could be given as 'gate in'. In case a transport means arrives in a country, it will be called 'border crossing' and the location is called 'border crossing place'.
Depart	A transport means departs at a location at a time. In case this area is a terminal, the milestone could be given as 'gate out'.
Load	Cargo is loaded into a transport means or equipment like a container. Loading indicates that the owner/operator of the transport means accepts responsibility for the cargo.
Unload/ Discharge	Cargo is discharged or unloaded from a transport means or taken from an equipment, like a container. The receiving party such as a freight forwarder will now take responsibility for the goods.

The associations and interactions between the main transport concepts define business constraints. For instance, a container cannot be at different places at the same time. Another rule would be that when transport means after loading of the cargo leaves a location it implies that it has departed and that the association (from a data perspective) between a location and cargo has ended. This also implies a handover of responsibility to a carrier after loading cargo. These types of business logic rules will be specified in a detailed architecture.

Events create a trace of the life of a transport concept, i.e. cargo, location, business service or transport means. For instance, the sequence of events between a transport means and arrivals and departures to and from locations, show the itinerary of that transport means. This itinerary can be according a timetable like a voyage scheme or a flight schedule provided by a third party service provider. Similarly tracking and tracing a container can be represented by the locations and the transport means between any of the locations on its route.

4 LEADING PRINCIPLES

4.1 Introduction

The leading principles serve as a guide to formulate the system boundaries, services, and functionality for the federated network of platforms.[2] The FEDeRATED vision describes the federated network of platforms as an infrastructure provision for data sharing establishing a set of agreements and technical application for authorised user based on a publish and subscribe approach.

The FEDeRATED leading principles relate to a virtual organisation[3], address the interfaces between individual organisations and to have be implemented by many organisations that what to use the shared infrastructure provision. This also requires a number of relevant considerations, such as the encoding for sharing data or the sharing of links. They allow the various FEDeRATED partners, also in connection with each other and the European Commission Services, to further develop the appropriate FEDeRATED infrastructure provision.

The FEDeRATED infrastructure provision can be described as a method:

- To electronically receive or obtain either the legally or the business process required information regarding cargo and transport movements in or connected to the EU;
- To allow electronic data sharing between a data provider and - receiver of the information; and,
- To identify and authorize different data providers and - receivers, in order to safeguard data sovereignty;
- To facilitate data sharing between business and the various national competent authorities, either with consent of a data provider or within legal boundaries;
- To enable business and public authorities to access high quality data based on available within a trusted environment
- To empower all parties within the logistic chain to interconnect with one another to do business without discrimination.

These principles leading up to developing a data sharing infrastructure provision relate to answering the following questions:

- How to get / receive the data
- What data are we dealing with
- How to safeguard the data (integrity, quality, authorisation)
- Who can use the data
- What data can be made available
- What can be done with the data
- How to connect data to users.

In addition to identifying these questions in the leading principles, answering these questions also deals with issues like the Reference model (chapter 4), Semantic model, (chapter 6), elements of building (including applicable standards), etc..

[2] The leading principles are rooted in ICT architectural approaches such asTOGAF

[3] This is different from most IT architectures that provide specified leading principles for individual organisations

4.2 The principles

Hereunder, the FEDeRATED leading principles for data sharing are defined. They are described per principle and identified relating applicability in relation to the FEDeRATED Core Operating framework elements, the DTLF design principles (also called building blocks), and the applicable roles.

LEGENDA - The following columns are given:

- Principle – a brief name for the principle
- No. – a number for reference to the principle
- A description of the principle
- 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 building block of the DTLF SG2 to which the principle is linked. The building blocks are encoded according the team numbers:
  - 1 – plug and play;
  - 2 – technology independent services;
  - 3 – federation of platforms;
  - 4 – trusted, safe, and secure
- 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;
  - DP – Data provider;
  - DR – Data Receiver.

FEDeRATED LEADING PRINCIPLES					
Principle	**No.**	**Description**	**Core Operating Framework**	**DTLF Building Blocks**	**Role**
Level Playing Field	1	All supply chain operators and public authorities involved in freight transport and logistics have to be able to participate.	ON	4	E/A
Electronic/digital format	2	The information is to be encoded digitally, using a revisable structured format.	IN	1 2 3	DP/DR

FEDeRATED LEADING PRINCIPLES					
Principle	**No.**	**Description**	**Core Operating Framework**	**DTLF Building Blocks**	**Role**
	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.[4]				
Compliance with existing rules	3	Data sharing must be compliant to existing legislation (e.g. GDPR) and privately agreed rules.	IN	4	E/A
	Principle 3 refers to legal interoperability				
Business service	4	Each participant has to formulate the business service(s) it provides (service provider) or requires (customer).	IN	1	C/SP
	Principle 4 addresses organizational interoperability for enterprises				
Business relations	5	Trust between enterprises is primarily driven by their real work relationships.	TR IN	4	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 their outsourcing hierarchy from the perspective of for instance a shipper and/or consignee.	IN	2, 3	E
Data requirements of enterprises	7	Business services and commercial mechanisms supporting negotiation between a customer and service provider specify the data that they will share.	IN	1	E
	Principle 7 contributes to semantic interoperability.				
Data requirements established by an authority	8	Data requirements set by an authority are related to the legislative basis afforded to that authority.	EN	1	A/E
	Principle 8 refers to legal interoperability and organizational interoperability for authorities				
Data processing	9	Any organization can specify its internal processing.	TR ON	1	A/E

[4] 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	Core Operating Framework	DTLF Building Blocks	Role
		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.	TR	4	A.
	Principle 10 refers to legal- and organizational interoperability				
Publication of data requirements	11	Public authorities publish their data requirements in a machine-readable form.	TR IN	1	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 harmonized search criteria	IN ON	1	E
Data as proof	13	A public authority or enterprise must be able to proof compliance or non-compliance with data.	TR	4	A
	Principle 13 stipulates data needs to be stored in a non-repudiated manner to allow such proof.				
Authorities providing data (authority services)	14	Public authorities can share their data with enterprises for policy reasons within a legal framework	IN	1	A
	Principle 14 refers to legal interoperability and organizational interoperability for authorities				
Push/pull	15	A legally allowed data sharing mechanism allow in case of: • a push, data to be duplicated by enterprises to authorities; • a pull, data being made accessible to authorities.	IN	3	A/E
	Principle 15 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. The eMSW data set consists of additional data sets like passengers and waste, which is for further development. However, the eMSW data set will be made available in a similar manner				

FEDeRATED LEADING PRINCIPLES

Principle	No.	Description	Core Operating Framework	DTLF Building Blocks	Role
Publish/subscribe	16	An organization must have the ability to subscribe to any relevant new data in accordance with fit for purpose (public authority) or a commercial relationship (enterprise).	IN	3	A/E
	Principle 16 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	17	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.	IN	1	A
	Principle 17 refers to legal interoperability and organizational interoperability for authorities				
Identification of organizations	18	Each organization is able to identify itself uniquely according agreed attestations with transparent validation processes of these attestations (e.g. Chamber of Commerce Registration, AEO certificate)	TR	1	A/E
Identification of users	19	Persons that act on behalf of an organization are able to identify themselves as such and should be known and employed or delegated by that organization	TR	1	A/E
User capabilities	20	The capabilities. i.e. the actions that may be performed, of an identified user are transparent to all other relevant users/organizations	IN	1	A/E
Data sensitivity	21	Sensitive data should not be accessible or changed by unauthorized users or organizations.	TR	4	E
	Principle 21 implies access to data that is stored or shared via some solution/platform. is applicable to for instance commercial sensitive data.				
Metadata of data sharing	22	Any metadata specifying which data is accessed or shared between any two enterprises is not accessible by unauthorised users or organizations.	TR	4	A/E
	Principe 22 addresses that business patterns can be derived from data shared between any two enterprises and should be hidden from third – non authorised - parties. It implies that metadata of data sharing between public authorities and enterprises is open data.				
Identification of	23	IT systems of an organization that support the	TR	1	

FEDeRATED LEADING PRINCIPLES

Principle	No.	Description	Core Operating Framework	DTLF Building Blocks	Role
systems		roles data provider and -receiver, are uniquely identifiable			
Data sharing policy	24	A common policy or agreement specifies the use and reuse of data as well as the manner in which it is stored or removed.	DS	4	A/E
Data sovereignty	25	A data owner determines the data it will share and retains full rights and controls over this data	DS	4	DP
Data at source	26	Single sharing of links, multiple (controlled) access to data	IN	1 2 3	DP
	Principle 26 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 organizations that share the data. To have data at the source, these organizations only share links to that data.				
Data sets	27	The data sets of which links can be shared is given by the reference architecture (see chapter 5).	IN	2	A/E
	Principle 27 addresses semantic interoperability.				
Baseline standards	28	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.	IN	2 3	DP / DR
	Principle 28 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 CEFACT Core Component List (see chapter 7)				
Data timestamps	29	An event for sharing milestones has its own timestamp that can differ from the timestamp of a milestone.	IN	2 3	E
	Principle 29 identifies the need for difference between these timestamps to be small in the context of process synchronization				
Unique identifier(s) of data (sets)	30	Unique identifiers are used to create and share links of relevant data sets between any two enterprises.	IN	3	DP / DR
	Principle 30 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.				

FEDeRATED LEADING PRINCIPLES					
Principle	**No.**	**Description**	**Core Operating Framework**	**DTLF Building Blocks**	**Role**
Data sharing solution	31	Organizations select a solution of choice for data sharing with others (platform, peer-to-peer)	ON	3	A/E
Federation	32	Organizations are able to share or access data with others	ON	3	A/E
Data validation	33	Data is either validated by a data provider or a – receiver against data sharing specifications (e.g. XSD).	DQ		DP / DR
	Principle 33 identifies that a data receiver will always receive an indication of validation to prevent any double validation. Data validation is on completeness and correctness.				
Data Exchange integrity	34	Accuracy and consistency of data over its entire lifecycle is required	DS DQ	4	DP DR
	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	35	Historical data sets are stored for optimizing business processes (public authorities and enterprises), based on legal requirements (e.g. archiving),			A/E
	Principle 35 iterates that data can also be used to support Research & Development and statistics.				
Logging and audit trail	36	Organizations store a (shared) immutable log and audit trail of the data they have shared.	TR	4	A/E
Monitoring	37	Each organization is able to trace with whom and at what time particular data has been accessed/shared with any other organization.	TR	4	A/E

4.3 Compliance with existing rules

Three aspects come to mind that need further scrutiny:

1. Personal data. EU Member States will ensure compliance with GDPR. The application of restrictions in the scope of the obligations and rights in order to secure specific national interests may vary between Member States.
2. Confidentiality and commercial data. The common perspective of the commercial data that has to 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 particular organizations do not have access to particular data to prevent for instance additional insurance fees (liability) and access to cargo content by unauthorized persons (theft).

5 THE SEMANTIC MODEL

The FEDeRATED Semantic Model[5] is based on open baseline standards as will be described in this section. Data semantics represents all relevant real-world aspects and governance of logistics. Real-world activities are for instance transport, transshipment, and storage. These translate to what is called 'logistics service' at business level: an enterprise is able to perform or outsource a real-world activity within the scope of its business. The limitations of the scope may be defined by permits or other restrictions or capabilities. For example by a permit for dangerous goods transport or its assets, such reefer facilities for temperature-controlled cargo.

5.1 Overall structure of the semantic model

This section provides the Semantic Model underlying the Reference Architecture. The concept of Digital Twin is central to the model: a Digital Twin is a representation in information systems of real-world physical objects. These Digital Twins can be specialized in more detail; their event-associations are always the same. The business service concept is introduced to change the state of these physical objects by sharing data.

The semantic model is depicted in figure 3 represents the highest level of an ontology:

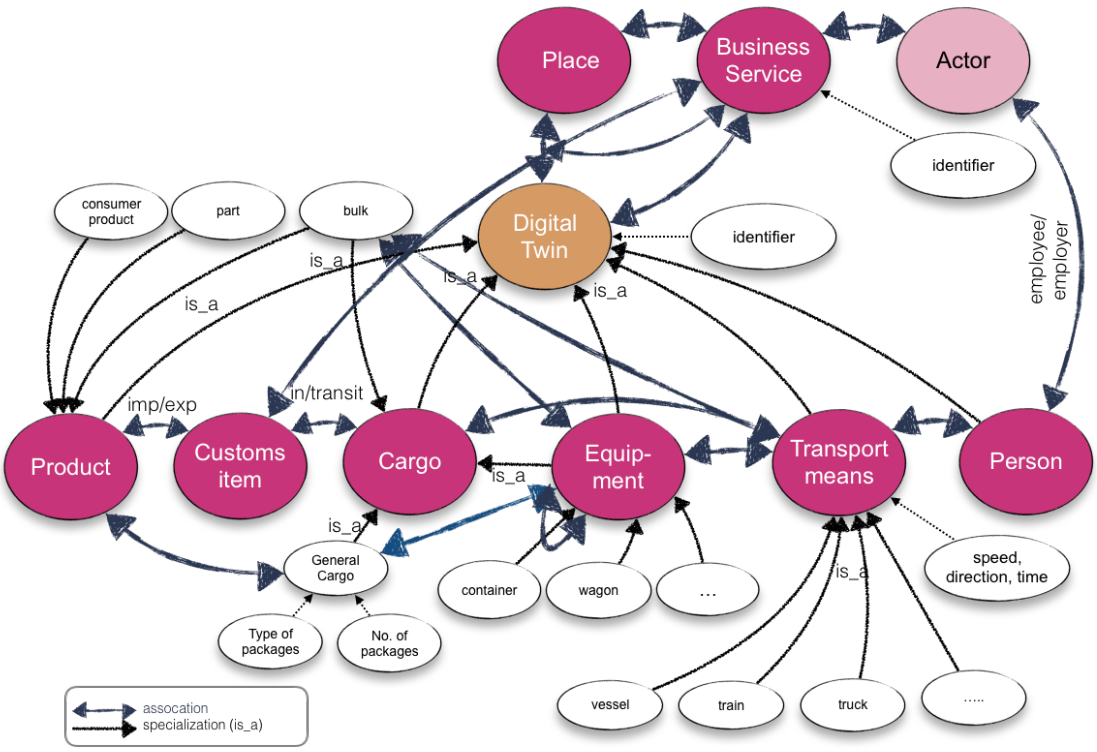


Figure 3 The FEDeRATED semantic model

[5] In basic terms, a Semantic Model is a description of the semantics of all data objects that are needed to manage a particular process and their relationship, grouping data into classes, describing the attributes (properties) and visualising the process through diagrams.

Associations between the various concepts represent what is called ‘Event’ in the Reference Model. It implies that various types of ‘Events’ are distinguished, each with their properties and lifetime.

This proposed semantic model contains the logistics and transport concepts like cargo and transport means. This model can also be depicted as a type of hierarchy, with entries Digital Twin, location (or area of interest), business services, and customs item. The ‘event’ that has been introduced in the previous section, reflects the associations between the various concepts in the semantic model, e.g. between a Digital Twin and a Node.

The Reference Model and the Semantic Model represented the two opposite sides – the two faces of the FEDeRATED mirror.

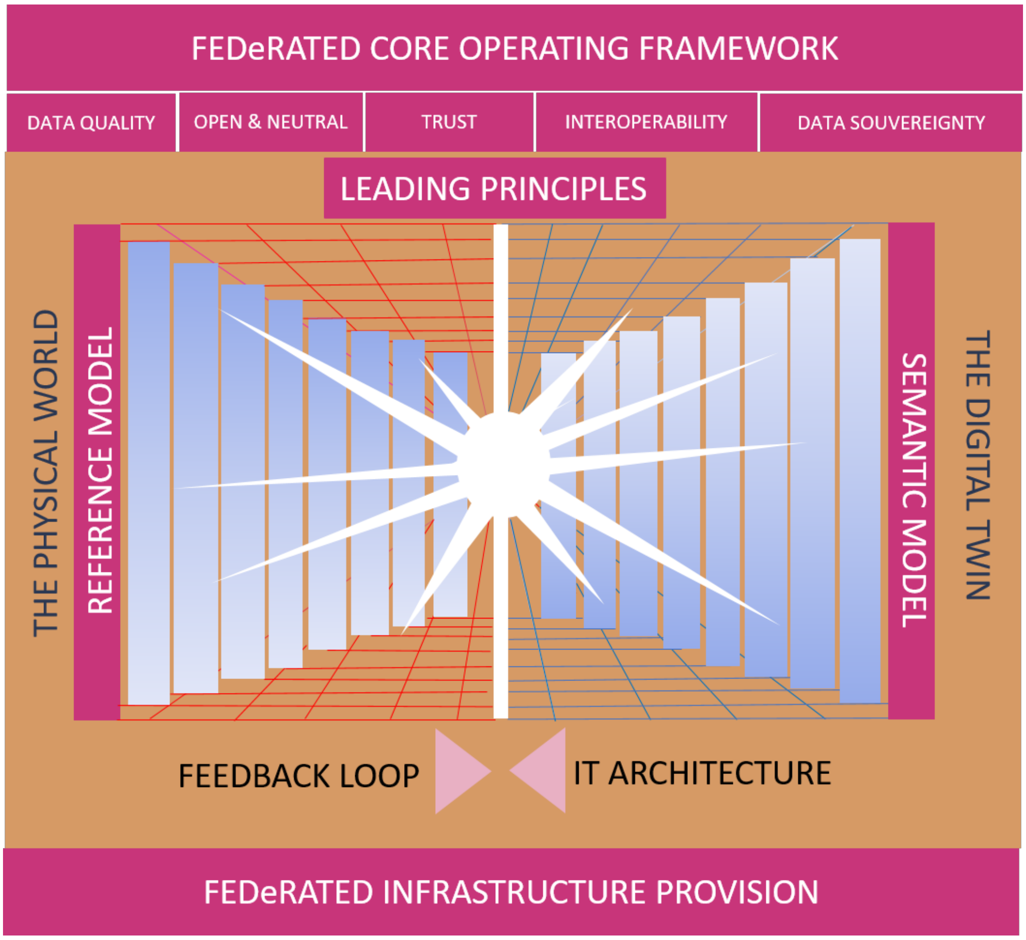


Figure 4. The FEDeRATED mirror has two faces – covering the reference and semantic model

The next sections provide definitions and details (i.e. properties) of the semantic model. The semantic model will be detailed by the various Living Labs. Furthermore, each of these Living Labs will create its view on the semantic model, meaning stakeholders in a Living Lab only select those concepts and properties that are relevant to them. In such a way, the semantic model will evolve over time in a natural, also beyond the scope of the FEDeRATED Action.

5.2 Details of the semantic model

The ‘Digital Twin’ concept is the core of the model: a data representation of any real physical object from a logistics perspective.

The following terminology is used:

Semantic Element	Definition	Identification
Customs Item	An item of cargo that is imported, exported, transited or (temporarily) stored under customs regime in a customs zone	HS (Harmonized Systems) code
Parent: **Business Service Overview**	All relevant data shared by enterprises for commercial reasons	
Business Service	Any service that is provided to a customer by a logistics or transport service provider.	Defined at more detailed level
Business Transaction	All data shared by interactions for executing a business service	Defined at more detailed level

Parent: **Digital Twin**	Any real-world physical object	
Product	Any commercial good that is bought and sold	Defined at more detailed level
Cargo	That which is handled by logistics activities, like transport, storage, and transshipment	Defined at more detailed level
Equipment	Re-usable equipment to facilitate transport of cargo, for example a wagon or a container	Defined at more detailed level
Transport Means	An asset that can move on its own power and that can carry cargo or equipment.	Defined at more detailed level
Location	Any physical location relevant for logistics	Defined at more detailed level
Person	An individual	Defined at more detailed level

Parent: Product		
Consumer product	Any product destined for use by consumers. Consumer products may be packaged in quantities.	Product code issued by a seller
Commercial product	Any product destined for use by enterprise. Consumer products may be packaged in quantities.	Product code issued by a seller
Part	Products destined for use in machines owned by consumers or enterprises	Product code issued by a seller
Bulk product	Unpackaged raw material	Identified by quantity or volume (and quality) in the context of a customer order

Parent: **Cargo**		
Bulk cargo	Any bulk product transported in large quantities. This may be further classified as liquid or dry bulk	Identifying properties are in the context of a business transaction: volume/weight and quality. These are the same for their subtypes.
General cargo	Any product is packaged for transport purposes.	Identifying properties are in the context of a business transaction: no. and type of packages; or each package has a unique identification (e.g. SSCN of GS1) or a way bill reference
Containerized cargo	Any products or packages of products that are stuffed into containers or ULDs (Unit Load Devices)	Container or ULD type and identification codes

Parent: **Equipment**		
Container	Transport containers serve to containerize products. They have standardized dimensions and can be loaded and unloaded and stacked	Container number
ULD	Unit Load Devices are light weight containers for air transport and facilitate loading cargo into aircraft	ULD type and ID code
Railway wagon	Unpowered railway vehicles that are used for the transportation of cargo	Wagon number
Trailer	Unpowered road vehicles that are used for the transportation of cargo	Trailer license plate
Swap body	Types of standard freight containers for road and rail transport	Identifier

Parent: **Transport means**		
Vessel (sea)	Any transport means used for transporting cargo by water. • These may be further classified as Deepsea vessels for ocean transport, • Feeders (short range via sea) • Any of the two above for a particular cargo type (e.g. container – or bulk vessels) • Ferries for transport of other transport means like trucks and/or trailers.	Vessel name or Radio Call Sign, or AIS (Automatic Identification System)

Barge	Vessel used for transporting cargo on inland waterways	Vessel name or AIS (Automatic Identification System)
Truck	Any transport means for road transport.	License plate (issued by national authority)
Locomotive	Any traction for a train composed of one or more wagons	Loc identifier (unique per owner; might be by a transponder).
Airplane	Transport means by air. This may be a dedicated freighter aircraft or belly space on a passenger aircraft.	Flight number or aircraft registration

Parent: **Location or area of interest**		
Logistical function	**Any location where a logistical activity is performed (see also business services)**	**Defined at more detailed level**
Infrastructural function	Any part of an infrastructure used for performing logistical activities	Defined at more detailed level

Parent: **Logistical function**		
Hub	**A place cargo is exchanged between vehicles or/and between transport modes.**	**Location Code**
Port	Location where vessels pick or drop of freight. Freight will be delivered or picked up by other transport modes. This may also be a hub where freight is transited from one airplane to the next. There may also be temporary storage facilities.	Seaport code or Location code
Airport	Location where airplanes pick or drop of freight. Freight will be delivered or picked up by other transport modes. This may also be a hub where freight is transited from one airplane to the next. There may also be temporary storage facilities.	Airport codes or Location code
Terminal	A freight terminal for different modes is a processing node for freight	Location code
Transshipment	An intermediate destination for transiting cargo to another destination.	Location code

Parent: **Infrastructural function**		
City	A generic geographical location that may have ports, seaports, terminals etc.	City codes or Location code
Trajectory	Any part of an infrastructure identified by its infrastructure manager	Road number, stretch number, river name, …
Area	Any area relevant to logistics operations	City centre, region, country code
Others		

Parent: **Business service**		
Transport Service	A service provided by a logistics for transport of cargo	Company name and related identifications Company name and related identifications
Transshipment service	A service for transshipping cargo from one transport means to another	Company name and related identifications
Storage service (cargo)	A service for (temporary) storage of cargo. This may include special cargo storage such as cool storage, animal hotels, and dangerous goods storage.	Company name and related identifications
Storage service (product)	A service for storage of products (warehousing)	Company name and related identifications
Groupage service	A service for grouping of cargo into equipment	Company name and related identifications

Parent: **Business Transaction**		
Framework contract	A contract with a long term validity period between any two enterprise with agreements of business service delivery	Contract ID
Booking	Agreement with a limited validity period between two enterprises for one or more orders	Booking number
Order	Agreement between two enterprise for actual execution of a business service according a booking or framework contract.	Order number

Parent: **Person**		
Crew	**Any person working on a transport means**	**National ID documents**
Master/driver/captain/pilot	The person responsible for operating a transport means	National ID documents, operating license for the transport means

5.3 Detailing and applying the model

The previous table is not complete. Not all concepts and properties are listed. The table lists not any derived concepts like itinerary, route and train.

Relevant details will be provided by the FEDeRATED Living Labs and any other relevant initiatives. Each Living Lab needs to formulate which of the concepts are applicable and will be further detailed. Any Living Labs that focus on identical functionality and concepts, will try to align these concepts and their properties.

Whenever the FEDeRATED Action is completed, the semantic model developed by the Living Labs can be applied in the same way by all other relevant initiatives.

5.4 Business services

There can be various business services. The basic services are transport, transshipment, and storage. Additional services relate to the seamless movement of a transport means and handling formalities. The following business services are identified:

For logistics, the following business services are distinguished:

- *Physical services*: e.g. transport, transshipment/cross-docking, (temporary) storage;
- *Value added services*: e.g. (re-)packing/stuffing, unpacking/stripping, ironing (of textile), consignment grouping, vendor managed inventory;
- *Supporting physical services*: e.g. vessel waste management, container cleaning;
- *Administrative services*: e.g. production of transport accompanying documents (certificate of origin, Bill of Lading, (e)CMR);
- *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*: corridor management services, path allocation services, sea traffic management services, piloting services, tug services, etc.
- Information services: traffic information services and forecasts, weather conditions and forecast, water depths and forecast

Business services result in business transactions between a customer and service provider. A business transaction should contain all data required by a service provider to deliver the business service. For instance, transport should contain two locations, the cargo to be transported, and the time (windows) at which the cargo will be available for transport at one location and has to be delivered at the other. In case cargo requires specific handling or has to be accessible to authorities, additional cargo details have to be given (e.g. temperature setting for reefer cargo, waste indicator, and dangerous goods classification). Additionally, commercial conditions and prices will be given, for instance delivery conditions.

5.5 Dates and times in logistics

There are basically four types of dates for associations between any two concepts of the Semantic Model:

- Expected – the time provided by a customer. It is provided by an order. It may actually be time windows for earliest – and latest pickup and delivery.
- Planned – the time at which a service provider will execute an order. In case of a voyage scheme, it is the time of call of a vessel in the Port of Loading. This can also be a time window. The planned time can be updated with new values, the so-called Estimated Times (e.g. Estimated Time of Arrival or ETA).
- Requested – the time at which a service provider is able to perform a logistics activity and requests a customer to be available. This can also be a time window.
- Actual – the time at which a relevant milestone took place, e.g. actual loading. This is provided by for instance container status data.

So, the association between Digital Twin and place has different properties depending on the types of business services.

- A transport service has typically eight properties: two locations with their dates and times.
- In case of transshipment -, storage -, and groupage services, there are seven values: one location with six values for time split into arrival and departure.

In addition to these services, there is a multitude of milestones with their associated times like security inspection, quarantine, and dangerous goods inspection. These are all specific instructions of authorities with a requested time (window) and location at which such an activity can take place.

The requested time can be used by a node/hub operator or infrastructure manager to optimize the handling and flow of transport means.

Process synchronization requires that these values of dates and times of adjacent legs have to be identical or overlapping. The actual dates and times have to be identical for adjacent legs, e.g. the actual arrival time of a transport means at a hub provided by a carrier should be identical to that provided by a hub/terminal operator.

Typically, each business service will have its own characteristics, associated times from the list mentioned above, and potentially derived values like a turn-around time at a terminal. These will also be developed and harmonized by the Living Labs.

The associations between the various subtypes of Digital Twin have two concepts of 'time': the time at which the association is created and at which it is expired (e.g. loading - and discharge time respectively). Time might not always be given but is relevant. Additionally, these associations have a number: the number of units that is subject to the association. The following associations have these properties:

- Product-general cargo: packaging of number of products of a type, e.g. in boxes and/or on pallets.
- General cargo – equipment: split of general cargo (number of units of packaging) over equipment.
- Bulk (cargo) – equipment
- Bulk (cargo) – transport means
- General cargo – transport means

5.6 Cargo perspective

As stated before, the following types of cargo are distinguished:

- Containerized cargo – cargo transported in containers. These are normally expressed as Twenty feet Equivalent Units (TEU) for sea and Uniform Load Devices (ULDs) for air transport. Thus, a 40-foot container is 2 TEU. ULDs come in many shapes and sizes to fit an airplane contour.
- Containers can transported by vessels, trucks with trailers, that can be transported by vessels (ro-ro or roll-on roll-off), and trains consisting of railway wagons (that can also carry trailers with containers).
- General cargo – this can be anything that is packaged with some type of disposable (or maybe re-usable) packaging material. These can be pallets with boxes, drums, postal bags or anything else. There is a UN Recommendation on Package types. As the example shows, packages can contain other packages, eventual leading to the (commercial) products that are transported between a shipper and consignee.
- Bulk cargo – this is any type of cargo that can only be expressed in weight and volume. A distinction between dry – and liquid bulk is made, e.g. oil and chemical are liquid bulk, sand, coal, and grain are dry bulk. Bulk cargo can also be transported in containers.

Depending on its way of packaging, agricultural products like fruit can also be transported as dry bulk in containers or directly in vessels. It all depends on logistics operations at a shipper and agreements with a consignee for transporting products. This has to be reflected by customs declarations.

At each handling location, but also during movement, the cargo of consignments and shipments can change. Therefore, it is relevant for customs to distinguish individual transport legs, detect any delays, and have additional information of the parties involved. Basically, two types of operations can take place on cargo:

- Convergent operation – cargo is packed together with other cargo into larger units. The identifications of the packed units is lost; the identification of the larger unit is used in data sharing. This operation is also known as ‘stuffing’, ‘packing’, and ‘loading’. It can be on various levels, like stuffing pallets in a container, but also on loading trailers on a train or containers in a vessel.
- Divergent operation – the individual units are taken from the larger unit. This operation is known as ‘stripping’ or ‘degrouping’ (containers), ‘discharging’ (transport means like vessels), and ‘unpacking’ (boxes from pallets). The identifications of the smaller cargo units become available.

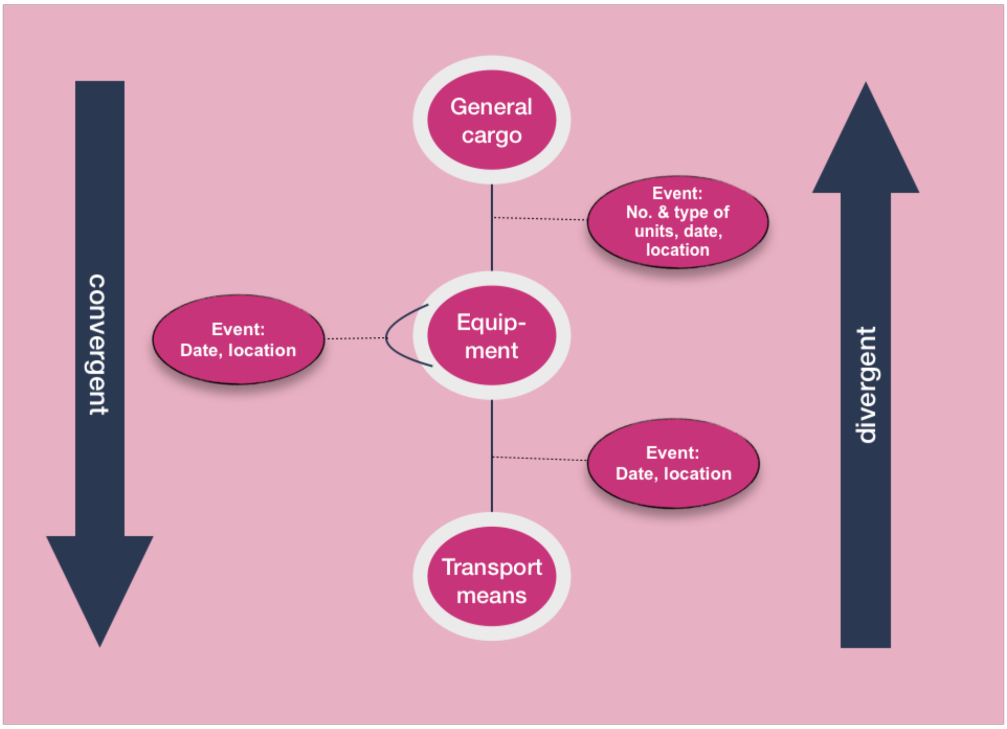


Figure 5. Particular operations are reflected by their data perspective

Figure 5 shows that general cargo, e.g. pallets with boxes, can be grouped into containers. One cargo item of one consignment can be split into two or more containers (equipment). Therefore, an association between general cargo and equipment contains the number and type of units that is stuffed in a container.

Each consignment has a unique identification between a customer and its service provider; each cargo item or package will have a unique serial number within that consignment. In practice, cargo items themselves do not necessarily have unique identifications, e.g. boxes don't have unique numbers. Cargo items are uniquely identified by their type and marks and numbers, which is anything written on these cargo items. Grouping of cargo items in a container can be retrieved from a container stuffing list, linking to a consignment.

In most cases, a stuffing list is not present or there is only an indication that particular consignment(s) are stored in containers. Thus, only an association between those containers and the consignment(s) can be constructed.

The association between two pieces of equipment, e.g. a container on a trailer or a trailer on a wagon, is based on their unique identification. The association is constructed at a location and time (convergent) and deleted at another location and time (divergent).

5.7 Transport means perspective - itineraries

A transport means is an asset that moves from one location to another. The movement can have different names, e.g. a trip for a truck, voyage for a vessel, or flight for an airplane. These are called itineraries. There are two types of itineraries, namely:

- Itinerary-to-order – the itinerary is established by planning software for assigning orders to a transport means, resulting in an itinerary of that transport means. This type of itinerary is completed when all cargo has been transported. It might never end, if the planning is updated during its execution, meaning for instance a truck just drives (indefinitely) and transports cargo. This would be relevant to especially autonomous transport means. A similar situation can be foreseen with barges, where any free capacity due to discharging cargo can be booked.

- Order-to-itinerary. An itinerary like a voyage scheme, flight or timetable of a train is published by a service provider like a shipping line, airline or railway undertaking to the ledger. During booking and ordering, the itinerary is available to customers. An order is therefore linked to an itinerary.
  This itinerary has a lifetime spanning either geographical or in time. For instance, a voyage ends at its final destination. A vessel can have a new voyage at that destination. A flight or timetable, which is scheduled periodically like daily or weekly, will end at a certain time. Whether or not it is replaced by another one depends on the agreements of the service provider with one or more infrastructure managers and/or hubs, like slot allocation at an airport or path allocation for trains.
  Itineraries might change during execution, due to unforeseen circumstances or for commercial reasons. These changes might impact authorities. For instance, if a vessel had Rotterdam as first port of call in the EU, but changes its voyage to Antwerp as first port of call, Belgium customs should have the Entry Summary Declaration data (ENS) of all containers discharged in EU ports.

In many cases, forwarders may sequentially combine these itineraries, Forwarders may construct multi-modal chains with multiple hub transhipments based on timetables and using back-to-back business services of multiple transport means operators. A state diagram of orders and their cargo represents the possible milestones, which are considered relevant for the current version of the supply chain visibility ledger.

ARCHITECTURE IN THE PHYSICAL AND THE DIGITAL WORLD

In the physical world, each building can be considered an amalgamation of elements. In physical terms this would be represented by: the foundation, the floor, the wall, the ceiling, the roof, the door, the window, the façade, the balcony, the corridor, the fireplace, the toilet, the stairs, the escalator, the elevator, the ramp. Through technological advances, regulatory requirements, and new digital regimes the origins, contaminations, similarities, and differences of these elements have evolved into their current iterations and turned remote areas with some houses into complicated networks of interconnecting urban areas.

In the virtual world, architecture is as essential as in the physical world. This does not only relate to building and further developing the original internet design, but also to developing interconnecting network provisions to serve a wide range of stakeholders. Process, technology and organizational requirements are considered. The FEDeRATED infrastructure provision aims to allow various IT systems – platforms - to structurally connect and allow its users to make optimal use of the available electronic information – the data. Interconnected within a larger infrastructure, interoperable platforms have to comply with certain elements of building.

The provisional list of elements of building for a platform or IT system to fit into the FEDeRATED infrastructure provision as identified in Milestone 1 Vision report reads as follows:

1. Foundation:
   - Semantic model, building upon existing standards;
   - Business process choreography – describing the interaction sequencing in a commercial relation between two enterprises;
   - State transition diagrams – describing the business logic for event-associations between any two concepts of the Reference Model;
   - Regulations specifying data requirements and access mechanisms required by authorities.
2. Cement – technology choices – support of APIs and messaging, using one or more data syntaxes (XML, EDI, JSON(-LD), RDF).
3. Floor and walls – Solution specific APIs - views on the semantic model, business process choreography, and state diagrams tailored to a use case.
4. Ceiling – Privacy – commercial protection express comfort, control, convenience, even humanity.
5. Roof – Security and safety provisions addressing particular risks
6. Door – Access Point – the software to integrate generic data sharing functionality with IT back office systems based on standardized APIs.
7. Key to the building - identification and authentication, authorisation - dedicated entry point
8. Stair – constructing composite solutions upon basic ones.
9. Toilet – existential zone of interaction – the governance between architecture and human involvement.
10. Window – Trust in performing particular logistics activities, compliant with regulations.
11. Façade – business services, timetables, and metadata to assess the capabilities and data sharing options of a stakeholder
12. Balcony – projecting private identity publicly (now made redundant by the digital realm)
13. Corridor – data at source – sharing relevant links to all data (in some cases allowing temporary data storage facilities)
14. Fireplace – registry or postbox where all relevant business services, timetables, and metadata can be found.
15. Elevator – available technologies to analyse data
16. Escalator – platforms interoperability to support actual data sharing between any two organizations.

The elaboration of these elements of building may serve as a construction guide. Thereto the above list will be validated within the course of the FEDeRATED project. This construction guide relates to tools, requirements, enabling the FEDeRATED infrastructure provision to support data sharing for a seamless, compliant goods flow in (inter)national trade.

6 FEDeRATED IT ARCHITECTURE

The federated network of platforms has a focus on data sharing and interoperability requirements rather than an IT system development project in the classical sense. As such, it is preferred not really speak of "systems" but rather components or constituent parts required in order to enable the whole. This is in effect a mix of physical systems and protocols, standards and semantics, etc.

Based on the work and outputs of the DTLF, the boundary conditions prescribed by the **leading principles** and further elaboration from partners it is possible to describe a first base IT architecture on three levels:

- **Decomposition**. This identifies the form and function of the solution broken down into constituent subsystems.
- **Modularity**. This describes how to avoid changes causing a ripple effect in the behaviour of other parts of the ecosystem through e.g. decoupling between modules and through platform-module interface standardisation. This is addressed through the inherent nature of the elements of building (components) as described below and the attributes of the technologies and rules being identified in the Leading Principles.
  Design Rules – The rules that platforms expect module developers to obey to ensure interoperability with the rest of the ecosystem. The first tier is the Core Operating Framework and the second the Leading Principles.

This chapter further elaborates on decomposition, i.e.:

1. The federated platform.
2. The platform services.

6.1 Federated platform

The template hereunder provides the technical requirements that need to incorporated into platforms allowing a FEDeRATED infrastructure provision to function.

Federated platform	Definition	Description
Access Point	The ICT component integrating the end-point of an individual end-user to its back-office ICT system. An Access Point can implement functionality like data transformation, communication, etc.	These are the ICT components that support the interaction between back-office systems of end-users and their connector or platform. They may consist of graphical user interfaces only, especially for SMEs.
Certification Authority	Any ICT component that can authenticate the identity of an end-user	The authentication of the identity of users are managed by organizations called certification authorities, based on open standards.

Federated platform	Definition	Description
Chain modeling toolset	A subset of the configuration toolset to develop views on the models, including a business transaction hierarchy for modelling supply- and logistics chains.	This toolset supports enterprises in modeling and implementation of the FEDeRATED concepts in their supply and logistics chains, for instance by constructing transaction hierarchies (see the example in section 2.2).
Configuration toolset **Connector**	The set interoperable ICT components that support an end-user in specifying its data requirements, connect to a platform (or install a connector), and configure its Access Point.	When computer systems need to interact with other systems, engineers need to ensure that the connections are compatible. These connections are configured by special tools.
	A component providing peer-to-peer data sharing services according a particular Quality of Service	Organizations may decide that they don’t want to use a specific platform, but implement the required functionality themselves. This is via a connector, see for instance the International Data Space Association architecture.
Endpoint	The unique identification (“address”) on a platform or connector enabling an end-user to share data with any other end-user having an endpoint.	An endpoint could be a URI (Uniform Resource Identifier or a web address. It identifies an organization with respect to the FEDeRATED network or platforms. One organization may have more than one endpoint.
Connector	*Synonym:* Single Entry Point, Unique Resource Identifier	
End-user **Federated platform**	Any organization (public or private) operating in supply and logistics, e.g. LSPs, RUs, IMs, carriers, shippers, Food Safety Authority, customs authority.	This refers to organizations that operate the ICT systems, either from a business – or authority perspective.
	The set of interoperable platforms of different providers, each with its own business model, providing logistics enterprises and authorities with a single entry point for data sharing to support their business.	Looking at all the connectors and platforms that need to be connected as whole, is holistically referred to as the Federated Platform. It does not refer to a single system, but the combination of all of them together.
End-user	*Synonym:* Federation of platforms, Federative Infrastructure	

Federated platform	Definition	Description
Identity Provider	Any ICT component that is able to provide a certified Identity to an end-user	Computer systems cannot "see" who they are interacting with and therefore Identity Providers are needed to certify that a user really is who they say they are through the use of a digital identity.
Maintenance toolset	A subset of the configuration toolset to manage and maintain views on the models.	Data sharing requirements can change over time due to regulatory or market developments, requiring adaptation of connectors and platforms. This requires maintenance tools to simplify the work.
Modeling toolset	The subset of the configuration toolset to develop a semantic model and business process choreographies as a basis for generating platform services.	Semantics are the language of logistics and transport. They have many vocabularies that are related, and these words and their relationships are recorded in semantic models. Similarly, the interaction sequencing between organizations can be modelled by a choreography. Such a choreography identifies the various interactions, leading to data requirements of for instance a booking or a transport order.
Platform	Any ICT system providing (a subset of) the platform services to two or more end-users in a federative platform.	A platform is another name for a computer system that provides services to companies and their end-users, the so-called platform services
	Synonym: Node	
Platform Services component	A component of the federative platform providing one or more platform services.	Platforms can provide parts of the platform services. Each of those platform services is supported by a component of the platform.
	Synonym: Registry component providing Registration – and Connection Services; Visibility component providing Visibility Services, etc	
Registry component	An ICT component of the federative platform supporting the Registration – and Connection Services.	In a network of platforms, organizations need to know where to find oth-

Federated platform	Definition	Description
		ers. Therefore, a registration component needs to be available, identifying the endpoints of an end-users, with reference to a platform if that endpoint is implemented by a platform. This only implies that particular data can be accessed via this endpoint, which may include a reference to data stored elsewhere.
	Synonym: Registration Services component	
Storage component	An ICT component of the federative platform or linked to it for (temporarily) data storage by providing data storage as Common API.	Data will always be stored somewhere, either by one (or more) of the platforms or by one (or more) of its end-users.
	Synonym: Blockchain node or -cluster	

6.2 Services provided by a Federated Platform

Business and authorities both operate and maintain IT systems providing (digital) services to end-users in support of logistics and transport (business) processes. These "platforms" provide services for the handling, processing and/or distribution of data between users of the system i.e. on a commercial, community, enterprise (organisation) or sector-wide level, etc. There are also "platforms" which provide specific services in support of the above through the provision of e.g. data exchange and connectivity solutions.

Stakeholders interface with each other via different implementation guides and/or different IT systems supporting these implementation guides. In addition, there are many platforms, each with slightly different functionalities, and their number is growing,

There is a multiplicity of different open and defacto standards, supported by a variety of platforms and solutions, but still not leading to seamless information sharing amongst all stakeholders in the supply and logistics chain. There are still too many bilateral agreements, proprietary solutions, and different platforms preventing a data sharing solution similar to the Internet functionality.

The Internet functionality is *one registration and connection to only one platform or solution of choice provided by one of the many service providers to be able to do business with all relevant partners*. The objective is to create such a commodity based on the leading principles.

The template hereunder identifies the services that a platform has to provide.

Federated platform services	Definition
Agility service	A class of Logistics Service API supporting cancellation of an order due to unexpected conditions like delays, losses, or theft of cargo and/or vehicles

Federated platform services	Definition
	and potentially triggering re-planning of (part of) a logistics chain.
Booking service	The class of Logistics Service API for negotiating of prices and conditions to execute a logistics service (e.g. according a timetable like a voyage scheme) or conclude a framework contract according customer requirements.
Business process choreography	The sequence of interactions between any two organizations. A business transaction relating to a business service typically has a transaction choreography.
Common APIs	A class of platform services to support the Logistics Service API, e.g. communication, data transformation, reliable data sharing, secure data sharing, data storage.
Connection Service	The class of Logistics Service API to integrate ICT back office systems with the selected platform services by means of an Access Point.
Federative platform protocol	The set of agreements for data sharing between platforms to support platform services
Logistics Services API	A class of platform services implementing the transaction choreography.
Logistics – or business service	The set of values of properties of a (composition of) business activity(-ies), e.g. a transport service or a transport service that is further decomposed into a logistics chain by its provider.
Information services	A class of VAS APIs to access (open) data to support a business transaction, e.g. weather forecast data, traffic information, corridor management, ETA calculation service, and CO_2 shipment/package monitoring service. Information services support resilience and agility.
Ordering service	The class of Logistics Service API for actual execution and detailed planning of a logistics service according prices and conditions of a booking or a framework contract.
Platform Service	The set of Logistics Service API, Common APIs, Value Added Service APIs,, and Platform Support APIs whereby the federative platform implements the transaction choreography.
Platform support APIs	A class of platform services to provide trust and support billing and payment of the use of platform services, e.g. audit trail, logging, access control, monitoring.
Quality of Service	A set of parameters that specifies both functional and non-functional features of a service, e.g. its reliability, performance, and availability.
Quotation and marketplace services	The class of Logistics Service API to search and find (a chain of) logistics services meeting customer demands. These class of platform services need

Federated platform services	Definition
	to implement a high precision and recall, all logistics services, timetables, and spare capacity meeting customer demands have to be found.
Registration Service	The class of Logistics Service API that enable an end-user to use the federative platform via its single entry point, e.g. publishing its logistics services, timetables, and spare capacity, to receive an identity as a trusted end-user, and to select the required platform services.
Resilience service	A class of Logistics Service API assessing risks in completion of particular supply – or logistics chains or individual transport legs based on information services. Resilience services implement supply chain resilience.
Semantic model	Concepts and their associations specifying data semantics of a particular domain or (sub-)system.
	Synonym: ontology, data model
Value Added Service APIs (VAS APIs)	A set of services specified by APIs that are developed by third parties and are available for users to embed in the Logistics Service API. Identity - and Authentication Provision, Data Transformation, ETA (Estimated Time of Arrival) prediction and (dynamic) chain planning are examples of VAS.
Visibility service	A class of Logistics Service APIs providing details of the execution of a logistics services and its planning (including for instance a VAS API for ETA prediction at the requested destination or Carbon footprint tracking) according an agreed transport plan.

6.3 Requirements for data, application of standards and API's

To construct a FEDeRATED infrastructure three common features or aspects of behaviour are identified, namely Data[6], Standards, and APIs. The requirements are elaborated.

6.3.1 Data

6.3.1.1 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 or eAWB, a transport order and a load list.

6.3.1.2 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. URIs to data or real-world identifications like container

[6] Data is machine readable

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).

6.3.1.3 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 provider to one receiver.
- Publish & subscribe – a link published by a data provider and data is automatically distributed to all data receivers that have registered themselves as subscribers and are authorised to access the data as such.
- Push-pull transformation – a data provider is not always able to share links or has systems that provide access to data when a data receiver pulls it. In this case, a data provider can upload (push) the data to a facility that generates a link to an intended receiver who may access (pull) the data by evaluating the link.
- Pull-push transformation – a data receiver is not always able to receive links and pull data. In this case, a data receiver has a facility that automatically pulls data based on links received and forwards the combined data set to the data receiver.

6.3.1.4 Data security

Only authorized access to data is required to prevent any risks (see annex). This is at the following levels:

- Identity and authentication – any user accessing data via a function (or API) needs to have a verified identity that can be authenticated. The following ‘users’ are distinguished:
    - Persons that are employed by an organization. Persons have roles and capabilities which grants them access to data. Each organization is responsible for organizing identification and authentication of their employees.
    - Systems identifications. This concerns both IT back office systems of organizations as well as assets with a sensor (Internet of Things – IoT).
- Access control – the rules by which a user is able to access data. Particular rules can be related to a data classification (e.g. open data versus data shared in a commercial relation) and data that needs to be accessible to authorities. Access control can be formulated by for instance XACML (XML Access Control Markup Language), based on the semantic model. There is a processing model underpinning XACML, consisting of for instance policy enforcement points that have to enforce access control.
- Data encryption – the data that is shared cannot be accessed or changed by any unauthorized user during its exchange.
- Data authentication – the source of the data can uniquely be identified.

Data encryption and authentication are often combined with the application of asymmetric encryption methods. The data is first encrypted with the public key of the recipient (so only the recipient can access the data) and this encrypted data is again encrypted (or complemented by a hash) by the sender with its private key (so a recipient is able to validate the origin with the public key of the sender). This is a well-known and often implemented mechanism.

Whereas access control has to be implemented by any organization and access can be shared via links to data, identification, authentication, and data encryption and authentication can be implemented as follows in a federated network of platforms:

- End-to-end – solutions are applied over the network of platforms. Organizations sharing data over the various platforms receive trust independent of the underlying platforms and links.
- Links – each link implements the solutions, meaning that a chain of trust is created. Each link between IT back office systems and a platform, and between platforms needs to implement the solutions.

Link security is required. It is up to users to agree on applying particular end-to-end mechanisms. End-to-end identification and authentication contribute to trust amongst organizations that do not know each other, and needs to be developed to enable synchromodality, agility, and other types of logistics innovations.

Link security is supported by PKI certificates from an eIDAS certified organization over for instance https or other protocols that support encryption. It requires that each platform can be trusted and has implemented solutions to address other types of cyber-security than passive and active attack to data, see for instance the articles in the eFTI Regulation on this topic.

Applying end-to-end mechanisms will impose restrictions on platforms and solutions, like argued hereafter.

For end-to-end data encryption and authentication, we distinguish between the actual data that is shared end-to-end (the ‘payload’), and control information required by a platform to take actions like routing the payload to its proper recipient.

End-to-end data encryption can only be based on an infrastructure that is completely agnostic of the payload. Distributed Ledger Technology (DLT), connectors of the International Data Space Association (IDSA), the proposed solution of sharing links via triple stores adopted by IATA, and the eSENS Delivery component perfectly fit this requirement. The payload can be encrypted; control data is required for routing the data to the intended recipient(s). It implies that such a data sharing solution does not add functionality, e.g. it cannot perform any data transformations of the payload. These solutions are all peer-to-peer solutions; they require link security for identification and authentication.

In the same way, end-to-end data authentication and encryption is feasible on the payload. End-to-end authentication by encrypting the payload with the private key of the sender is also feasible in the same manner.

In case the solution or platform has to provide additional functionality like data transformation, the payload cannot be encrypted. Data authentication is provided by adding a hash to the data based with the private key of a recipient and known data elements. In case data is transformed into another structure, the values of these data elements have to be found in a transformed payload.

The latter solution of hashing is a digital signature to data that refers to a user. The user either signs the data in its own system, which means the proper rights are applied, or the user signs the data in the system of someone else. In the latter case, the user should have access to its proper private key and be able to sign the data with that key, without disclosing the key to the platform used. This relates to identification and authentication of a user.

Whenever private keys are used to encrypt or authenticate data, these keys should be stored in a tamper proof environment and never leave this environment. The tamper proof environment, like a password manager or an electronic wallet, should destroy itself and its contents whenever an unauthorized user tries to access it. Access should be controlled by multi-factor authentication (see next text).

In case a user requires access to data stored in another system, end-to-end identification and authentication is required. Of course, platforms can have their mechanisms for multi-factor authentication based on for instance a card, a PIN or password, and a form of biometric identification. For instance, electronic banking applications running on smart devices are protected by a PIN, where the device is also protected by (another) PIN. Potentially, also SMS can be applied to share an additional PIN or a barcode could be scanned to access the application.

End-to-end identification and authentication requires the installation of:

- Each organization is responsible for its internal user management, including rights of these users. The rights can also cover the ability to share data with other organizations.
- It is up to each organization to install its own Identity Provider and Certification Authority or to outsource it to third party. Most organizations with internal IT applications have this functionality installed.
- In case Identity Provision and Authentication are outsourced for data sharing with other organizations and the organization still has its own internal Identity Provider and Certification mechanism, this latter needs to be synchronized with the external one. This is to prevent any situation where a person is not an employee anymore but is still not deleted as such from the external provider.
- Each Identity Provider and Certification Authority has to be accessible via open standards like OAuth2.0. Multi- or two-factor authentication might be applied, where another channel (e.g. SMS) than the one used for data sharing is applied for sharing for instance a PIN.
- There need to be one or more Registries with known and trusted Identity Provides and Certification Authorities.
- A Registry needs to verify the identity of an organization with one or more attestations, e.g. a Chamber of Commerce Registration or an EORI number.
- Whenever any two organizations require end-to-end identification and authentication, the registration of both should be based on one or more attestations of each organization that the other one accepts.

This mechanism for end-to-end identification and authentication, including the construction of one Registry has been developed by the Dutch iSHARE Foundation. Whenever users select end-to-end identification and authentication, they need to select this mechanism.

Services, like the registry provided by iSHARE, can be federated with similar services that have a common agreement on identification and authentication policies. As such users that need end-to-end identification and authentication across different territories or stakeholder segments can identify and authenticate with one such identity and authentication provider and gain secured access to data from services whose identity has been authenticated by another provider. This is referred to as Federated Identity and Authentication.

6.3.2 Standards

All semantics and the structure of data sets that are shared, will re-use relevant open and defacto standards, that are called baseline standards: a baseline standard is an open standard that is applied to develop other (open and defacto) standards. In this context, the following definitions are applicable:

- Open and defacto standards - open standards are those that have been developed via an open and transparent procedure and governance where experts can propose improvements, they are public available and can be downloaded free of charge; defacto are those that are applied by a particular (large) user group.
- Semantic and technical model - conceptual specifications given by a semantic model, i.e. concepts and their properties, are separated from their technical representation provided by baseline standards, i.e. data element formats, code lists, and other types of constraints.

The following baseline standards are identified:

- The United Nations Trade Data Elements Directory (UNTDED) is a baseline vocabulary;
- The UN CEFACT Core Components Library provides a set of (composite) data types with formats;
- UN ECE Recommendations
- ISO standards like the ones for country codes and date/time formats
- Encoding schemes
- ….

Standards like UN CEFACT MMT, WCO Data Model, GS1, EU Customs Data Model, IATA ONE Record, Sea Traffic Management (STM), RIS (River Information Services), Port Collaborative Decision Making (PortCDM), and many others build 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.

6.3.3 API layering

Application Programming Interfaces (APIs) is a technology for accessing systems via the Internet for the purpose of data sharing. A distinction between Common - and Logistics APIs will be made to allow rapid deployment of new functionality for (logistics) end-users of a solution. The Common APIs are the basis for deployment of the Logistics APIs. The APIs can be depicted as:

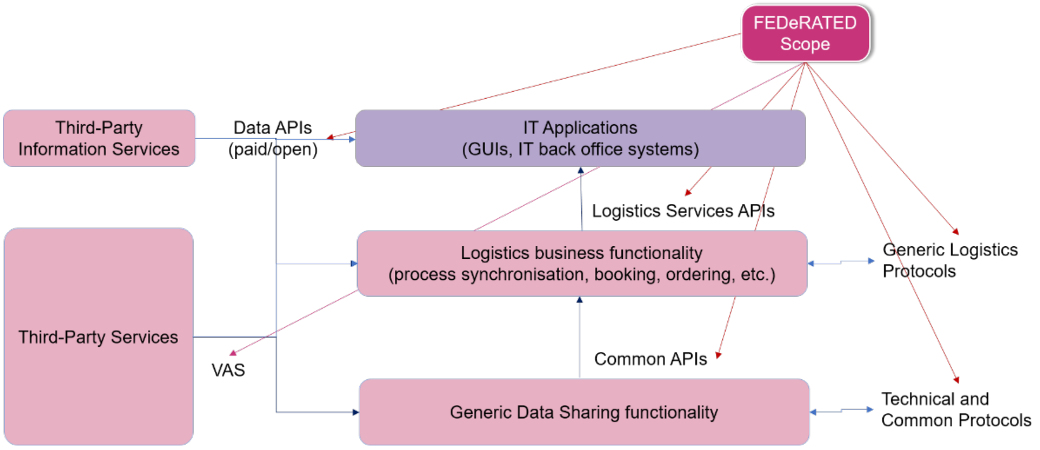

FEDeRATED Scope
Third-Party Information Services
Data APIs (paid/open)
IT Applications (GUIs, IT back office systems)
Logistics Services APIs
Logistics business functionality (process synchronisation, booking, ordering, etc.)
Generic Logistics Protocols
Third-Party Services
VAS
Common APIs
Generic Data Sharing functionality
Technical and Common Protocols

Figure 7. The API layering.

Figure 6 shows that the APIs are in scope of FEDeRATED. The functionality for providing these APIs is out of the FEDeRATED scope. In addition to the APIs, the protocols are addressed by FEDeRATED; these can also be implemented by APIs.

6.3.3.1 Common APIs

APIs providing functionality that is independent of an application domain and can be used by all types of data sharing applications. Identification and authentication, data storage, data sharing (e.g. by URIs or messaging), etc. are examples of functionality provided by Common APIs.

6.3.3.2 Logistics APIs

These are specific APIs operating on the concepts of the Reference Architecture. Logistics APIs make use or are part of a scenario containing also the common APIs. For instance, a user first has to identify itself and be authenticated to be able to receive any visibility data.

Logistics APIs require that the payload for data sharing (see data security) is not end-to-end encrypted. End-to-end encryption might be applied on the payload shared via the Common-APIs.

6.3.3.3 Decomposition of Logistics APIs

The following approach is taken based on the proposed data-oriented approach for decomposition of the Logistics APIs:

- Logistics Object APIs – a set of APIs to manipulate data of (associated) concepts of the Reference Architecture, where these APIs refer to sharing of data of those between any two organizations. An example is the sharing of container data for a container that is transported. The Logistics Object APIs utilize the Common APIs, for instance for sharing or storing data of logistics objects.
- Generic Logistics Services APIs – a set of APIs supporting the state or state change of collaborating enterprises as specified by the business process choreography for logistics services. A transport contract represents the state as agreed between a carrier and its customer. Sharing a transport order is represented by a state change of both the sender and recipient of that order. These APIs utilize the Logistics Object APIs.
  These APIs refer to the concept of logistics services that specify at business level the capabilities of enterprises, for instance the transport of containers by road. These are the afore mentioned Branch APIs. The business perspective is described hereafter.
- Solution Specific Logistics APIs – these are the APIs that are implemented by a specific solution or platform of a service provider or community system. These APIs may focus on a particular market, e.g. container transport by sea, and a specific part of the choreography, e.g. booking and ordering for instance of INNTRA and container tracking implemented by for instance Tradelens.
- Authority APIs – these are APIs used by authorities to access the data they require according the regulation(s) they govern. One could imagine one generic API supported by particular access control policies implemented for instance by XACML (XML Access Control Markup Language). Another approach would be to make a specific API per authority or regulation, where this API can only be called upon by a particular authority. It will lead to a vast

number of APIs, which are potentially difficult to change. Thus, an approach based on access control policies is preferred.

Settlement of data sharing between different platforms needs to be explored. It could be based on the amount of data that is shared or the number of calls a platform or solution makes. It implies that an organization having its own peer-to-peer solution basically could integrate with all relevant platforms according the federation protocol(s) and share data with all other stakeholders. Any two organizations implementing peer-to-peer solutions will not pay for the data they share, unless one of them acts as a source of paid data.

6.3.3.4 VAS APIs

Value added services (VAS) APIS are a set of services specified by APIs that can be developed by third parties and are available for users to embed in the Logistics Services APIs. Identity and Authentication Provision, Data Transformation, ETA (Estimated Time of Arrival) prediction, CO_2 footprint tracking and (dynamic) chain planning are examples of VAS.

6.3.3.5 Decomposition of VAS APIs

In a similar way, the VAS APIs can be decomposed into those that are generic and those specific to transport and logistics:

- Common VAS – services that are independent of any application. Identity Provision, Authentication Provision, and Data Transformation are examples of Common VAS; these can be implemented by each user and/or specific providers. These are part of the basic functionality (see before).
- Logistics VAS - ETA (Estimated Time of Arrival) prediction and (dynamic) chain planning are examples of Logistics VAS, where these services can be specific to a modality, cargo type, and/or region (geographically).

In case end-to-end encryption of the payload is applied (see data security), certain VAS APIs operating on that payload can only be applied at the interface between the Logistics APIs and the IT back office systems implementing these Logistics APIs, e.g. data transformation VAS API.

Settlement of any commercial VAS APIs is also part of federation.

There are already examples of Common VAS for which their applicability will be investigated, for instance the iShare APIs for identification and authentication and the ONE Record API developed by the air transport industry for data sharing.

Some of the Common APIs might be called by the Generic Data Sharing functionality, e.g. the identification and authentication mechanism, whilst others might also be called by the Logistics Business Functionality layer or even what is called an Access Point integrating IT back office systems with the Federated platforms. An example of such a Common VAS is data transformation.

The VAS functionality can be provided by any external party, as long as that party has sufficient data for development of the VAS. The VAS functionality might not necessarily store data but could be trained with data. The quality of the VAS will increase by increased data volumes used for training.

6.3.4 Protocols, Semantics and Distribution

6.3.4.1 Federation (protocols)

Federation relates to the set of agreements and their technical implementation for seamless interoperability between any two platforms or solutions. These protocols have to be specified at two levels, namely supporting the Common APIs and the Logistics APIs. The protocols supporting the Common APIs, the Common Protocols, also included technical protocols for actual data sharing.

6.3.4.2 Distribution mechanism

Distribution mechanism relate to the passing on of changes to the right logistics parties. Data is often commercially sensitive, so that not everyone is allowed to access all data. A distribution mechanism ensures that the right parties receive data and do not have to collect data.

6.3.4.3 Access policies

Whereas Identity and Authentication can be Common VAS, access policies need to be implemented locally as access control. Access policies are part of data sovereignty. Authorities also need to formulate their access policy rights, rooted in legislation. Access policies and their control mechanism refer to a pull mechanism (APIs). In case of the push mechanism (i.e. messaging), access policies are specified by a message structure for data that is to be submitted to an authority. Authorities can publish their access policies by a Policy Retrieval Point (PRP, see XACML – XML Access Control Markup Language). Enterprises need to implement so-called Policy Enforcement Points (PEP). Potentially, the access policies could be implemented by an API, thus combining the functionality of the various architectural parts of XACML.

6.3.5 Aspects of APIs

Aspects reflect a particular perspective by including particular data and/or applying functionality like data encryption. The various aspects are specified by the web services architecture.

7 VALIDATION PLAN

Pilots and Living Labs are being developed. These have the objective to implement and adopt (aspects of) the federative network of platforms in accordance with the Leading Principles and general notions as presented in this Interim Masterplan. The Pilots and Living Labs are based on continuous improvement of solutions in more than one cycle and the results of the pilot projects are validated whether they contribute to a data sharing environment.

The validation criteria for every project relate the following criteria:

Criterium	Description
Objective/purpose	A clear objective. The objectives mentioned by the Vision, i.e. supply chain visibility and/or increased capacity utilization, should be (part of) the objective of a pilot or Living Lab. Other objectives might stem from regulations, like eFTI implementation. In case a pilot or Living Lab does not implement one of these objectives, it should be clearly explained.
Multi-stakeholder	Participation of more than two enterprises (and authorities) is required. The roles of the stakeholders will be identified
Widespread application and upscaling	The result of a pilot/Living Lab has to be applicable on a larger scale than only the participants.
Leading principles (see chapter 4)	To identify what leading principles are to be validated and how these will be implemented in the scope of a Living Lab. This may result in particular outputs like a model of a supply and logistics chain (see section 2.2 for an example), selected platform service(s), data requirements, etc.
Reference model	Identification of the components of the Reference model being applied
TEN-T corridor	The CEF corridor where the project will be executed
Business case	A business case is elaborated – preferably identifying the mechanisms to distribute these business benefits amongst participants
Trust chains and trusted tradelane	Participants of a pilot/Living Lab define the various trust relations and supporting mechanisms. These trust relations consider customer - service provider, trust of a customer in the outsourcing of his service provider to another service provider, and the trust in authorities accessing the data. It also includes strategies like trusted trade lanes of customs provided by a trader. Trust chains require (initially) full visibility of the chain by a customer and implementation of security mechanisms.
Layering	Classification of the technical deliverables (i.e. APIs and messages) in terms of the layered model presented in section 6.3.3.
Baseline standards	Identification of the baseline standards that will be touched upon
Data Security	To provide any choices and solutions made with respect to data security,

	possibly accompanied by a risk assessment
Federated Platform	To provide a technical architecture comprising the various components of the Federated Platform as listed in section 6.1. This may refer to particular design choices.

Due to the evolving nature of the work it is anticipated that regular updates of the Interim Masterplan should be provided, reflecting any major impacts observed or experienced through the pilots, living labs and supporting studies to this document.

8 NEXT STEPS

8.1 Related Milestones

This Interim Masterplan is only the beginning of describing in more detail the functional, technical and organisation requirements of the FEDeRATED infrastructure provision. The Core Operating Framework, in combination with the leading principles and introduced elements of building allow for validation and further research and consultation between 2020 – 2023.

Within its current project planning, the FEDeRATED project allows various FEDeRATED Milestone moments to issue intermediate updates of this Interim Masterplan. It is important that the work remains tangible for users and as such significant (preliminary) findings should be reflected upon as and when the sphere of influence has been recognised and/or established.

The following Milestones provide concrete moments when updates based on consensus and/or test findings can be introduced:

31/10/2020	Milestone 5: Peer Review Report 1[7]
31/12/2021	Milestone 8: Interim Testing Report on Pilots & Living Labs
31/10/2022	Milestone 10: Pilot and Living Labs Assessment Report

The Interim Masterplan updates will reflect on the status of all aspects already contained in the Interim Masterplan as well as introduce the status of specific aspects not as yet fully included but identified in the listing below. Apart from updates of this Interim Masterplan, various contributions to further detailing the Interim masterplan will be incorporated in the FEDeRATED website.

8.2 Next Steps

Further, all beneficiaries will participate in the relevant works, either as member of the FEDeRATED IT Architecture Board, and specific (elaboration) Groups (possibly on Legal issues, Semantics, governance). These group preferably closely cooperate within the DTLF framework.

The following next steps are foreseen:

General:

1. Stepwise to further involvement of SME[8]
2. Elaboration of the Leading Principles

Architecture & Semantic Model:

3. Elaboration on Reference Model
4. Detailed Semantic Model
5. Detailed IT-architecture, Elements of Building

[7] Note: Milestone 5 is currently entitled “Peer Review Report”. Recognising the expertise and relevance of the DTLF, there is a possibility that the Peer Review Group will in fact be a representation of the DTLF. As such, the Interim Masterplan could then be updated based on further consensus and alignment with the ongoing work of the DTLF.

[8] Preferably, it should be made clear whether SME needs specific additional digital tools, Apps or specific measures to allow for more data integration within the supply chain.

6. API library/API Registry (including governance)
7. Common specification API's
8. Guidelines for API (general applicability, unique and identify in a certain way, signature definition
9. Translation FEDeRATED infrastructure provision benefits into sustainable transport goals

Data:

10. Storage of data
11. Data sovereignty and ownership
12. Data quality
13. Reuse of Data – Data protection and confidentiality
14. Identification elementary data set(s) – based on scenario reference use case

Impact analyses:

15. Alignment with eFTI, eMSW & Security
16. Compliance with existing rules / timelines
17. Legal impact analysis
18. Organisational impact analysis
19. Links to EU systems and use of CEF Telecom digital building blocks
20. Identification of the contribution of the FEDeRATED infrastructure provision on the greening of transport

Governance:

21. Governance issues

Governance issues

For the governance issues, a document will be developed relating to the governance of the FEDeRATED network of platforms developing the following aspects:

A. **Government of services.** Based on the analysis of the processes, the operational flows, the document exchange and the services a service management model can possibly developed.

B. **Platform Governance.**: Digital Identity, containing everything related to roles, permissions and other similar elements can be taken into consideration to develop a:.

   a. Incentive Model, with the purpose of increasing the number of users and, therefore, of data providers of the FEDeRATED network of platform.
   b. Data Governance, analyzing this section in a comprehensive manner to allow know, with certainty, the traceability of the data, its quality, its ability to be subject to verification, the security of such data, their storage conditions, their life cycle and other issues related to the governance of the data that may be relevant.
   c. Operation Governance, in relation to the terms in which the platform will operate, fundamentally with regard to normalization and standardization of data exchange processes carried out on the platform.

C. **Technical governance.** Referring to the analysis of the following elements:

a) System configuration and operation - The minimum content in this epigraph should address the configuration, monitoring and operation of the systems and contingency plan.
b) Software life cycle - The minimum content in this epigraph corresponds to the description of the life cycle it covers from the development process to the continuous integration processes.

D. **Institutional Governance.** It would be recommendable to identify whether a specific standards is necessary - with indication of its regulatory range - to ensure the viability of operation and efficiency of the platform.