Digital Transport and Logistics Forum (DTLF)

Subgroup 2 – Corridor Information Systems

Workprogramme

(Version 24092019)

1 Objectives, vision and content of the work programme

1.1 General objectives

The overall objective of DTLF Subgroup 2 – Corridor Information Systems aims to create a common understanding and solutions for data sharing in supply and logistics that are a basis for innovation and cost reduction, and contribute to societal challenges like safety, security, and sustainability.

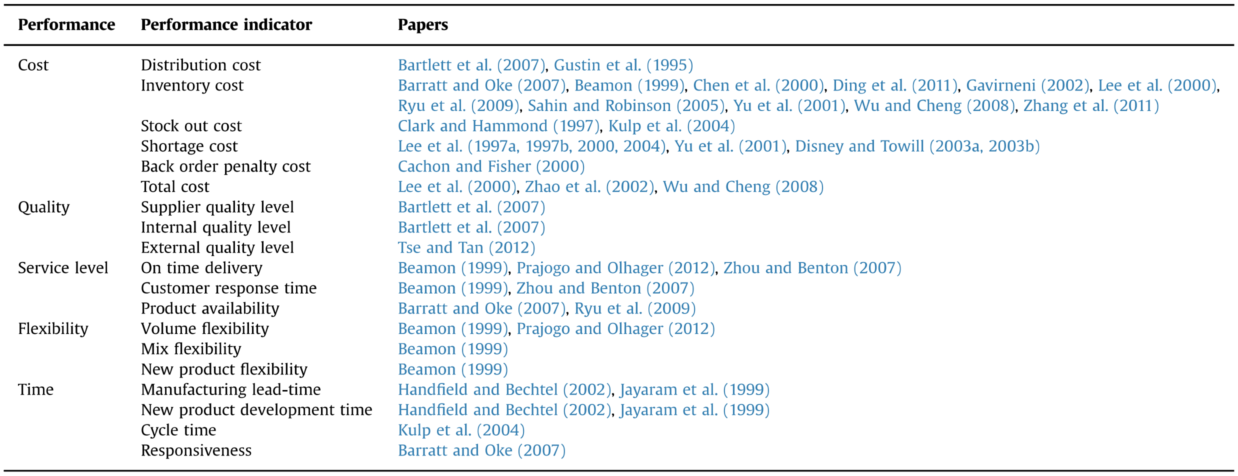
In particular, DTLF SG2 shall develop in its second mandate specifications and a governance structure for federated platforms to facilitate data sharing in supply and logistics from a public and private sector perspective. The specifications of the federated platforms comprise their behaviour, i.e. technology independent services, that support organizations in sharing data without prior agreements, i.e. plug and play, and the protocols for platform interoperability.

These platforms can be developed and provided by different service providers, either existing ones or new entrants, each with their own business and governance model and based on their technology of choice. Public and private stakeholders have to be able to integrate with their platform of choice and to share data with any other stakeholder of choice based on clearly defined business and legal activities.

1.2 The vision

Many public and private sector organizations have already solutions and platforms in place facilitating data sharing in support of business and compliance processes. These business and compliance processes can be rooted in legislation, e.g. governance of safe and secure trade flows compliant with trade agreements and national VAT rules, or can be of a business nature like the transport of goods for replenishing stocks in time.

The various ways of data sharing have resulted in public sector governed solutions. Examples are platforms for sharing structured data between the public and private sector and private sector governed solutions. These platforms support implementation guides of one or more standards. Each user of such a platform will have (relative) high switching costs and, in case business is cross-border, (relative) high costs of ownership for connecting with different platforms and supporting different implementation guides. These high switching and operational costs are a barrier to innovation and cost reduction by public and private sector. The following table for example shows that realizing supply chain visibility will have a great many advantages:



Performance	Performance indicator	Papers
Cost	Distribution cost	Bartlett et al. (2007), Gustin et al. (1995)
	Inventory cost	Barratt and Oke (2007), Beamon (1999), Chen et al. (2000), Ding et al. (2011), Gavirneni (2002), Lee et al. (2000), Ryu et al. (2009), Sahin and Robinson (2005), Yu et al. (2001), Wu and Cheng (2008), Zhang et al. (2011)
	Stock out cost	Clark and Hammond (1997), Kulp et al. (2004)
	Shortage cost	Lee et al. (1997a, 1997b, 2000, 2004), Yu et al. (2001), Disney and Towill (2003a, 2003b)
	Back order penalty cost	Cachon and Fisher (2000)
	Total cost	Lee et al. (2000), Zhao et al. (2002), Wu and Cheng (2008)
Quality	Supplier quality level	Bartlett et al. (2007)
	Internal quality level	Bartlett et al. (2007)
	External quality level	Tse and Tan (2012)
Service level	On time delivery	Beamon (1999), Prajogo and Olhager (2012), Zhou and Benton (2007)
	Customer response time	Beamon (1999), Zhou and Benton (2007)
	Product availability	Barratt and Oke (2007), Ryu et al. (2009)
Flexibility	Volume flexibility	Beamon (1999), Prajogo and Olhager (2012)
	Mix flexibility	Beamon (1999)
	New product flexibility	Beamon (1999)
Time	Manufacturing lead-time	Handfield and Bechtel (2002), Jayaram et al. (1999)
	New product development time	Handfield and Bechtel (2002), Jayaram et al. (1999)
	Cycle time	Kulp et al. (2004)
	Responsiveness	Barratt and Oke (2007)

Source: Caridi, Moretto, Perego, & Tumino, The benefits of supply chain visibility: a value assessment model, International Journal of Production Economics, 2014.

Examples for innovative services, business models etc. are described in literature and are listed in the final report of DTLF SG2.

1.3 The issue – lack of interoperability

DTLF I concluded that peer-to-peer business interoperability leads to incompatible implementation guides of (open) standards for data sharing. Airports or ports for instance have often established an own community platform and require enterprises to register with each of these platforms when doing business with these communities. For instance, shipping cargo via Hamburg, Rotterdam, and Antwerp requires registration with three platforms.

Figure 1 depicts variations of the situation that two enterprises, one of these enterprises acting as customer to the other, share data with each other.

Enterprises have to be compliant with (inter)national legislation, providing data to (push, e.g. customs declarations) or access to data by (pull, e.g. access by an authority to CMR data) authorities. Business interoperability is about coordination of business activities and supporting processes of two enterprises in compliance with regulations. This can be for instance the transportation of cargo from a place of acceptance to a place of delivery according to a particular time schedule. Supply chain visibility improves process synchronization leading to cost reduction due to reduced waiting times, and, eventually, seamless compliant cargo flows based on improved quality of data provided to authorities.

Figure 1 visualizes four different cases for implementing business interoperability, namely:

- <u>A - Peer-to-peer data sharing:</u>
  Each of the enterprises implements its particular access point and the mechanism for sharing data to support business activities. These enterprises share data by for instance exchanging bookings, orders, and events or reports of progress of for instance transport or loading by means of EDI (Electronic Data Interchange) interfaces. Each of the enterprises has a registration function listing its capabilities; enterprises may also decide to share such a function. In case of more than one registration function, interoperability amongst these registration functions is required.

- B – Single platform:
  Both enterprises connect to the same platform and share data via this platform according to platform services. An example is a platform used by two enterprises to share visibility data via a publish/subscribe mechanism. In this case, a customer subscribes to particular visibility data, which will be shared as soon as the platform service provider receives and publishes the relevant data. Another example is a platform for transhipment in a (air)port, where the platform is able to develop value added services based on data shared amongst its users. Each of these platforms will have its particular registration and connection mechanism, platform services supported by for instance with APIs, and business model. In case an enterprise wants to change to another platform, the enterprise most probably has to re-configure its access point to implement the platform services of the new platform.
- C – Multiple platforms:
  In this case, two enterprises each connect to a different platform, each with its registration mechanism and platform services. To be able to share data, these platforms have to be interoperable. Interoperability is achieved in two ways, namely technical interoperability and interoperability of the platform services (functional interoperability). The harmonization of platform services also plays a role. If these platform services are functional not identical, data will be lost when interconnecting platforms. If for instance one platform provides loading and discharge visibility for containers on vessels and the other covers also the hinterland, hinterland visibility cannot be shared amongst users of these platforms. Registration mechanisms also need to be aligned. If for instance a user wants to subscribe to visibility events of another user, the platform of the latter user needs to support a publish/subscribe mechanism and be able to exchange and store subscription data. Platform interoperability will most probably be implemented by gateways between the platforms, constructed on a bilateral basis and leading to potential loss of functionality provided to end-users. Harmonization of platform services and platform interoperability is required to prevent data loss and contributes to federated platforms. Since platforms will have different business models, they also need to harmonize clearing and settlement.
- D – Single platform and peer-to-peer:
  In this case, one of the enterprises connects to a platform, whereby the other in principle implements a peer-to-peer solution. It means that the latter enterprise does not want to register with any platform; it has its own registry. Furthermore, agreements have to be reached of clearing and settlement between the latter enterprise and any platform of its business partners. One could say that an enterprise with a peer-to-peer solution acts as a privately owned platform and its access point has to behave as such.

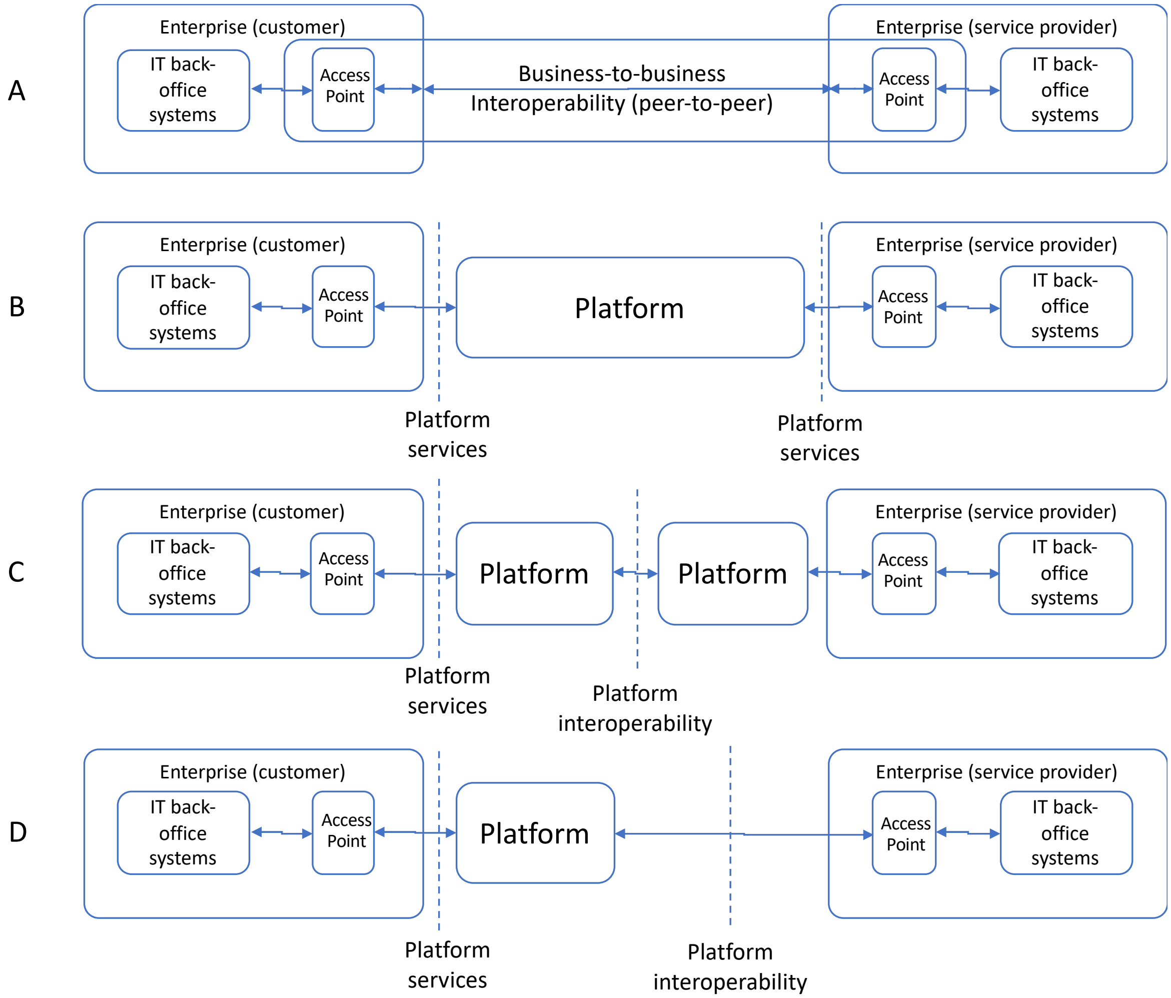


Figure 1 – business-to-business interoperability

The last case where an access point of an enterprise behaves as a platform is basically identical to a peer-to-peer implementation (case A); with the exception that the access point has to register itself with the platform and the enterprise connecting its access point to a platform has to pay for using the platform. Case C requires agreement on payment, settlement, and registration of services of the different platforms. Case C is currently only developed by different platform providers on a bilateral basis; there are no standards for platform interoperability.

Most probably, the eFTI (electronic Freight Transport Information) Regulation will provide one of the business – and use cases for realization of the federation of platforms. Dependencies with DTLF II SG1, that addresses eFTI, will be discussed and described independent of this work plan, but might lead to changes of the planning.

The deliverables of DTLF II SG2 will still include existing systems and technologies like Electronic Data Interchange (EDI), but will also give room for application of innovative technologies. There is no prescription as to which technology should be applied, as long as the solutions adhere to the specifications and are part of the overall governance. Thus, DTLF II SG2 does not prescribe any implementation aspects; it considers conceptual specifications for data sharing in supply and logistics and identifies potential solutions to share data (e.g. Application Programming Interfaces (APIs)). These are all technical aspects, supporting business scenarios and use cases.

Since the deliverables of DTLF II SG2 are modality and cargo independent, an important deliverable will be a guide that organizations can use to implement the platform services in their particular use case, that supports their specific business case. This guide will be based on user stories collected as part of the activities described in this work plan, complemented by those developed in the CEF funded projects FEDeRATED and FENIX.

1.4 Building blocks

The work programme is structured along the four functional building blocks defined by the DTLF under its first mandate.

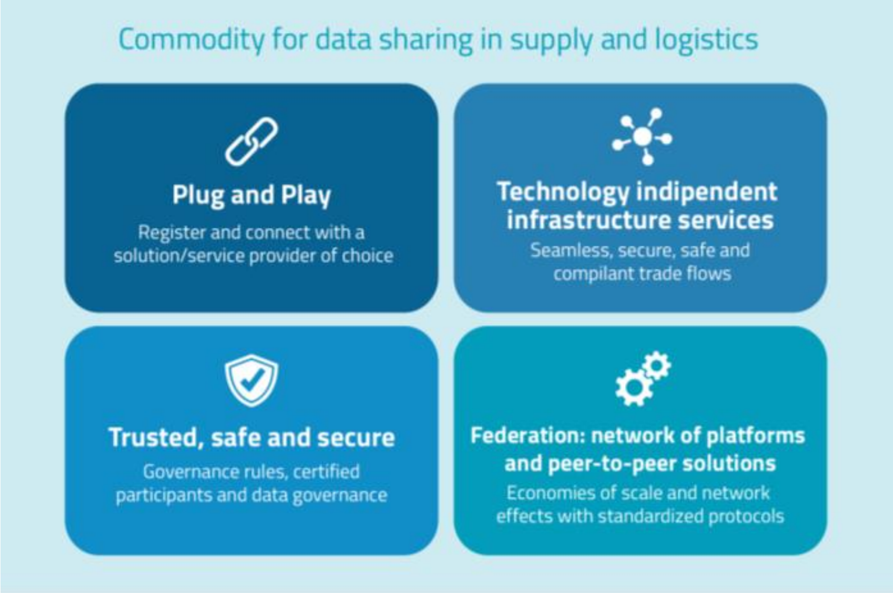

Commodity for data sharing in supply and logistics
Plug and Play
Register and connect with a solution/service provider of choice
Technology indipendent infrastructure services
Seamless, secure, safe and compilant trade flows
Trusted, safe and secure
Governance rules, certified participants and data governance
Federation: network of platforms and peer-to-peer solutions
Economies of scale and network effects with standardized protocols

Figure 2 – building blocks (DTLF I SG2 – executive summary and final report)

Together these building blocks establish the concept of federated platforms; they are defined as follows:

- Plug and play – the focus is on individual stakeholders, both in the public and private sector, and to enable them to register and connect to a platform of choice and to share data.
- Technology independent infrastructure services (platform services) – this building block prevents a lock-in of a user with any platform, and enables all users to use the federated platforms including SMEs (level playing field).
- Federation of platforms or platform interoperability – harmonized connectivity and interoperability of different solutions (platforms).
- Trusted, safe and secure – general mechanisms like identity and authentication that ensure trust into federated platforms, and the technical, legal and organizational governance of the solution.

1.5 Data sharing between organizations

DTLF II SG2 focusses on data sharing between any two stakeholders in supply and logistics compliant with all relevant national and international (EU) Regulations. Any internal processes of a stakeholder will thus not be addressed by DTLF II SG2. The implication of this constraint is that authorization is in principle outside scope, each stakeholder will be able to formulate its authorization policies. However, any restrictions on these authorization policies enforced by for instance Regulations will be part of DLTF II SG2. These can be privately – or publicly governed regulations and rules, like the Rotterdam Rules that state restrictions to data sharing for transport of goods by sea.

1.6 Content and structure of this document

This document has the following structure:

- Section 2 – overall planning, list of deliverables, and milestones
- Sections 3, 4, 5 and 6 – detailed planning for each of the building blocks

1.7 Background reading

The following documents produced by DTLF SG2 in its first mandate are relevant input to activities and deliverables given in this work plan (https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=4855):

- 2018-06-01 DTLF_SG2_ExSummary_to_be_edited.pdf (a final version is found at http://www.dtlf.eu/resource-center/downloadable-material)
- 2018-06-01 SG2 Final Report to be edited.pdf
- DTLF SG2 Recommendations approved.pdf

2 Overall planning

This section provides the overall planning, deliverables, and milestones for the various building blocks. Besides these aspects, choices will be described for structuring the tasks for the building blocks. These choices lead to dependencies of particular building blocks.

2.1 Main dependencies between the building blocks

The following main dependencies between the development of the building blocks are identified:

- Operating principles – there is a need for generic set of operating principles for federated platforms that can be used by both enterprises and authorities. These operating principles include for instance modelling bilateral data sharing (i.e. between any two organizations for B2B, B2G, and G2B) to support business services or value propositions. The operating principles will be developed as part of the building block 'Technology Independent Services', based on the results of DTLF I SG2.
  The term 'operating principles' is introduced in this document; another term could be 'design principles' like used by the CEF FEDeRATED project.
- Architecture – there is a need for an overall architecture of federated platforms. The architecture will identify components and interfaces between those components, e.g. it will identify a registration component. The architecture will be developed as part of the building block 'Federation or platform interoperability'.
- Functionality scoping – federated platforms will expose functionality via platform services, potentially implemented by APIs. Functionality scoping will be supported by business scenarios. This functionality will support business services as defined in the final report of DTLF I SG2. It will be the basis for formulation of a business transaction choreography, a semantic model, and registration of individual organizations. The operating principles will be developed as part of the building block 'Technology Independent Services'.

These choices create dependencies between the tasks of the various building blocks, which needs to be reflected in the planning.

2.2 Overall planning

The overall planning is given by the diagram on the next page.

		2019					2020												2021												2022								
		8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9
Plug & Play				░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░			
	Business service specification			▨	▨	▨	▨	▨	▨	▨	▨	▨																											
	User stories												▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨									
	Registration services												▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨									
	Data requirements specification												▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨									
	Access Point specification																														▨	▨	▨	▨	▨	▨			
	Implementation Guide Development																														▨	▨	▨	▨	▨	▨			
Technology Independent services			░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░															
	Interoperability principles		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																											
	Business scenarios		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																											
	Business transactions												▨	▨	▨	▨	▨	▨	▨	▨	▨																		
	Semantic model																▨	▨	▨	▨	▨	▨	▨																
	Platform services																▨	▨	▨	▨	▨	▨	▨																
	Standards support																▨	▨	▨	▨	▨	▨	▨																
Federation of platforms			░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░										
	Architecture		▨	▨	▨	▨	▨	▨	▨																														
	Technical protocols			▨	▨	▨	▨	▨	▨																														
	Vertical interoperability									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨															
	Horizontal interoperability									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨															
	Payment, clearing and settlement																								▨	▨	▨	▨	▨	▨									
	Configuration components																								▨	▨	▨	▨	▨	▨									
Trust, safe, and secure			░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░	░
	Best practices		▨	▨	▨	▨	▨	▨	▨																														
	Stakeholder groups			▨	▨	▨	▨	▨	▨																														
	Governance structure									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																		
	Identification and Authentication									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																		
	Procedures																					▨	▨	▨	▨	▨	▨	▨	▨	▨									
	Security requirements																					▨	▨	▨	▨	▨	▨	▨	▨	▨									
	Adoption and implementation instruments																														▨	▨	▨	▨	▨	▨	▨	▨	▨

2.3 List of deliverables

The following table provides the list of deliverables per building block.

		Deliverable name	Deliverable description
Plug & Play			
	$D_{PP}1$	Business service specification	A specification of the business services and their data requirements, e.g. transport – and transshipment services, and timetables
	$D_{PP}2$	User story(-ies)	One or more user stories for describing how enterprises and authorities can use the different platform services.
	$D_{PP}3$	Registration	Interaction sequencing, semantic model, and selection of a rules language for registration of enterprises (customers and services providers) and authorities. The registration process should specify the ability to rename interaction types (synonyms) for particular users and to select a subset of technology independent services, which allows these users to map platform services to their terminology.
	$D_{PP}4$	Data requirements formulation – authority	Specification of rules language to generate data requirements to support authorities. This deliverable depends on the availability of the business transaction choreography ($D_{TIS}3$) and the semantic model ($D_{TIS}4$)
	$D_{PP}5$	Data requirements formulation – service provider	Specification of the mechanism to generate data requirements to support particular business services. This deliverable depends on the availability of the business process choreography ($D_{TIS}3$) and the semantic model ($D_{TIS}4$). It includes any data requirements of authorities, including mechanisms that can be supported to facilitate trade (e.g. Certificates of Origin, Long Term Supplier Declaration)
	$D_{PP}6$	Data requirements formulation – customer	Specification of the me chanism to generate data requirements to support goals of customers. This deliverable depends on the availability of the business process choreography ($D_{TIS}3$) and the semantic model ($D_{TIS}4$). Data requirements should include those that a service provider should have for compliance to legislation.
	$D_{PP}7$	Access point specification	Specification of an Access Point functionality that supports data - and process transformations to support the selected technology independent services.
	$D_{PP}8$	Implementation guidelines	Guidelines for organizations for the implementation of federated platforms in their supply and logistics chains and organization.
Technology Independent services			
	$D_{TIS}1$	Business and authority interoperability principles	The boundaries of the system is modelled and a set of definitions for business interoperability, including compliance with regulations and modelling of supply and logistics chains.
	$D_{TIS}2$	Business scenarios	A high level drafting of business scenarios and identification of variants as input for modelling.
	$D_{TIS}3$	Business choreography	A specification of the business choreography for supporting any two enterprises to digitally perform their business. The business choreography consists of a number of interaction types with minimal data requirements.
	$D_{TIS}4$	Semantic model	A semantic model to support data sharing for identified business services, including their compliancy requirements with regulations.
	$D_{TIS}5$	Platform services	Specification of platform services derived from the business choreography.
	$D_{TIS}6$	Standards support	Support of existing open standards by the business choreography and its semantic model.
Federation of Platforms			
	$D_{PI}1$	Architecture	A set of definitions and the architecture of components with interfaces for the development of federated platforms.
	$D_{PI}2$	Technical protocols	A number of technical protocols to be applied for technical interoperability amongst different platforms.
	$D_{PI}3$	Functional interoperability – vertical	Interoperability at functional level between two platforms providing identical business functionality as specified by the business process choreography, including interoperability of registration.
	$D_{PI}4$	Functional interoperability – horizontal	Interoperability at functional level between two platforms providing adjacent business functionality as specified by the business process choreography, including interoperability of registration.
	$D_{PI}5$	Payment, clearing and settlement	Financial arrangements for data sharing between two users utilizing different platforms and users with a peer-to-peer solution having to interface with platform(s).
	$D_{PI}6$	Configuration components	Specification of interfaces and functionality of components for development and configuration of new platform services and their interoperability.
Trusted, safe and secure			
	D_G1	Best practices	An overview of best practices for governance in other application areas like the Internet.
	D_G2	Stakeholder groups	Stakeholder analysis from the governance perspective.
	D_G3	Identification and authentication mechanisms	Analysis of existing identification and authentication mechanisms and proposal for a mechanism to be used a global scale.
	D_G4	Governance structure and terms of reference	Governance bodies, their relations, and required skills and roles within the various governance bodies. Each body in the governance structure will have its terms of reference. The governance structure also includes a relation with (multiple) standardization body(-ies).
	D_G5	Procedures	Set of procedures for distributed extension and maintenance of business services, the technology independent services and platform interoperability.
	D_G6	Security requirements	Requirements for creating safe and secure federated platforms.

2.4 Milestones

The following table lists the milestones per building block.

		Milestone	Description
Plug & Play			
	$M_{PP}1$	Business services	The fundamental business services for supply and logistics are further specified.
	$M_{PP}2$	Registration	The registration procedures and its semantic model is available facilitating the registration to different platforms, depending on the technology independent services provided by those platforms.
	$M_{PP}3$	Data requirements	Rules for generating data requirements to support business services are detailed. This enables users to plug their systems into federated platforms.
	$M_{PP}4$	Access Point	Specification of access point functionality are defined as a basis for the development or selection of software to integrate existing IT systems to the federated platforms.
	$M_{PP}5$	Implementation guidelines	Implementation guidelines that provide organizations the capability to implement technology independent platform services in their supply and logistics chains and processes are defined.
Technology Independent Services			
	$M_{TIS}1$	Main principles	Agreement on the main principles for the development of the specifications for technology independent platform services.
	$M_{TIS}2$	Generic business interoperability	Specification of a generic way for data sharing to support business interoperability. It comprises the business choreography and semantic model to support a number of business services ($D_{TIS}1$ - $D_{TIS}4$).
	$M_{TIS}3$	Platform services	Specification of platform services derived from the business choreography. This specification is required for platform interoperability.
	$M_{TIS}4$	Standards support	Support of existing open standards by the business choreography and its semantic model.
Federation of platforms			
	$M_{PI}1$	Architecture	Specification of the architecture for federated platforms.
	$M_{PI}2$	Functional and technical interoperability	Different platforms are able to interconnect and share data for technology independent platform services.
Trusted, safe and secure			
	$M_{G}1$	Trust, safety and security	All required mechanisms and ingredients required to create trusted, safe, and secure federated platforms are available.
	$M_{G}2$	Governance structure	The governance structure is defined and put in place
	$M_{G}3$	Procedures	The various procedures for maintenance and development of the solution is available.

2.5 Overall risks

The following challenges and risks are identified for all activities:

- Time: too slow – it might be that innovative solution providers develop solutions more rapid than the DTLF, in case of many stakeholders buying in into those solutions the proposed solution of the DTLF might become obsolete. The governance structure, adoption by relevant stakeholders (first movers in business, authorities, and IT service providers), and potential legislation offer a long-term vision for realisation.
- Skills – a combination of business (supply and logistics) and IT skills is required, including skills to derive process and data requirements from legislation. Potentially, support of another EC DG like EC DG DIGIT is required to assist DTLF SG2 and/or input could be received from the CEF funded projects.
- Fragmentation of industry (many SMEs and types of stakeholders) and lack of maturity of digital services might hamper the adoption of the federated platform concept. Showing/demonstrating the benefits can be a big driver for the industry to catch up.
- Pushing solutions – some stakeholders will push for particular solutions.

3 Plug and Play

This building block - plug and play - focuses on individual stakeholders, both in the public and private sector, to enable them to register and connect to a platform of choice and to share data.

3.1 Objectives

The objective is to develop concepts and procedures that allow individual stakeholders to share data according common agreements:

- Registration – procedures for individual organizations to expose business services (or value propositions) for all (or a subset of) available platform services. Business services define data requirements.
- Integrate their systems – to be able to integrate their (back office) systems with the (selected) platform services and be able to share data.

3.2 Tasks

The following tasks are identified:

3.2.1 Business service specification

This task focusses on the identification of types of business services (value propositions) in supply and logistics and their data requirements. It identifies the means for representation of business services. Transport – and transhipment services are examples, they might be represented by timetables, voyage schemes, etc., see also the final report of DTLF I SG2. Business services are the core of the model, since they (1) formulate data requirements and (2) are the basis for business transactions with their choreography of interactions. The choreography specifies the interaction types and their allowed sequence between any two enterprises, including data (access) provision to authorities for compliance. See also the final report of DTLF I SG2.

3.2.2 User stories – plug and play

This task is about the development of user stories describing how an individual organization will register its business services and interface its internal IT back office systems and business processes with the technology independent platform services. It requires the formulation of data requirements, based on the business services specified by the organization, and additional data requirements formulated by the business transaction choreography and compliance with legislation. Three user stories will be specified, namely one for service providers, another for customers, and a third for authorities. These user stories will include registration.

3.2.3 Specification of registration services

The objective of this task is to specify the registration services, the semantic model for registration, and select a rule language by which authorities are able to formulate when they require particular data of a user of the federated platforms. The registration services include the registration of organizational details, business services and goals, technology independent platform services to be supported digitally by a user, and the specification of rules for sharing data with authorities, including the mechanism to be used (push or pull). The rules formulated by authorities refer to legislation; they specify in which cases particular (high level) data is required. A well-known example of a rule in global trade by sea is for instance, that 24 hours prior to loading data of containers needs to be provided to the customs authority operating in the country of discharge. The semantic model specifies all data that will be stored by a registry and are accessible by logistics marketplace functionality.

In this particular task, the rules will not be specified, but a mechanism (i.e. a rule language) has to be selected by which authorities are able to formulate their rules. Rules formulated by authorities need to be built in the business transaction choreography and business processes of enterprises.

3.2.4 Data requirements specification

The objective of this task is to specify the mechanism for the formulation of data requirements. Data requirements will be expressed in terms of the semantic model specified for the technology independent platform services, more specifically those platform services that are selected during the registration. The formulation of data requirements is required for integrating the selected technology independent platform services with the IT back office systems of a user. Enterprises are able to register by two roles, customer and service provider; authorities will have one role only related to the legislation they govern.

- Customer – a customer will define its data requirements from either a supply or logistics chain perspective or the types of business services it will require of potential service providers. It might include aspects like transport of dangerous cargo or cross border movements that imply the need for compliance with legal rules.
- Service provider – a service provider is able to formulate its data requirements based on its registered business services, the selected technology independent platform services, and data requirements stemming from compliance rules.
- Authority – an authority specifies its data requirements for each of the rules formulated during registration. It might include the addition of concepts and properties to the semantic model, for instance to specify particular data requirements stemming from national implementation of international legislation.

3.2.5 Access point specification

The objective of this task is to specify the functionality of an access point for the integration of platform services with IT back office systems. Two types of transformations might be required, namely data - and process transformation. Data transformation can be at different levels, namely the integration of internal databases with the data requirements to support business or integrating individual parts of the implementation of the platform services (i.e. individual APIs or message types) with internal data structures. Process transformations might describe the flow between external interaction types (i.e. APIs or messages) with internal IT systems (e.g., more than one IT system might be included in interactions). Technical protocols to integrate an access point with a platform depend on the protocols supported by that platform (e.g. some type of queuing protocol).

An access point may also support peer-to-peer implementation. In that particular case it needs to support the platform interoperability protocols for the selected platform services (functional and technical). This should also be part of the specification.

3.2.6 Implementation guideline development

The objective of this task is to develop guidelines that can be used by individual organizations or communities for implementing the platform services in their organization. Particular chains may cover particular products (e.g. a supply chain for edible oils like palm oil), particular types of cargo (e.g. containerized cargo), transport modality (e.g. sea and inland waterways), or any combination of the above. Particular views will be created on the semantic model of the technology independent platform services and the interaction types of the business transaction choreography may have other names that can function as synonyms. Implementing such chains or on-boarding to an existing solution may involve the formulation of additional data requirements, leading to potential extensions of the semantic model.

3.3 Dependencies

Number	Deliverable	Description
$D_{PP}1$	Business service specification	A specification of the business services and their data requirements, e.g. transport – and transhipment services, and timetables.
$D_{PP}2$	User story(-ies)	One or more user stories for describing how enterprises and authorities can use the different platform services.
$D_{PP}3$	Registration	Interaction sequencing, semantic model, and selection of a rules language for registration of enterprises (customers and services providers) and authorities. The registration process should specify the ability to rename interaction types (synonyms) for particular users and to select a subset of technology independent services, which allows these users to map platform services to their terminology. User registration also needs to consider any relevant procedures developed by the BB Trusted, safe, and secure as part of the governance structure.
$D_{PP}4$	Data requirements formulation – authority	Specification of rules language to generate data requirements to support authorities. This deliverable depends on the availability of the business transaction choreography ($D_{TIS}3$) and the semantic model ($D_{TIS}4$)
$D_{PP}5$	Data requirements formulation – service provider	Specification of the mechanism to generate data requirements to support particular business services. This deliverable depends on the availability of the business process choreography ($D_{TIS}3$) and the semantic model ($D_{TIS}4$). It includes any data requirements of authorities, including mechanisms that can be supported to facilitate trade (e.g. Certificates of Origin, Long Term Supplier Declaration)
$D_{PP}6$	Data requirements formulation – customer	Specification of the mechanism to generate data requirements to support goals of customers. This deliverable depends on the availability of the business process choreography ($D_{TIS}3$) and the semantic model

		($D_{TIS}4$). Data requirements should include those that a service provider should have for compliance to legislation.
$D_{PP}7$	Access point specification	Specification of an Access Point functionality that supports data - and process transformations to support the selected technology independent services.
$D_{PP}8$	Implementation guidelines	Guidelines for organizations for the implementation of federated platforms in their supply and logistics chains and organization.

Milestone $M_{TIS}2$ – generic business interoperability – of technology independent platform services needs to be completed. Furthermore, the architecture - $M_{PI}1$ – needs to be specified.

3.4 Resource requirements

The following skills and expertise are required:

- Business expertise – relevant knowledge of the business services/value propositions provided or required by an enterprise. This can be marketing expertise.
- IT skills – skills of constructing particular views of the semantic model(s) and developing the specification for access points.
- Legal skills – skills for formulating legal requirements as regards when/which particular data are required and the formulation of data requirements derived from legislation and their national implementations.

3.5 Challenges and risks

The following challenges and risks are identified:

- There is a dependency on the deliverables of the other building blocks. The Technology independent services should for instance develop a semantic model required for plugging systems into the federated platforms.
- Compatibility with legal requirements like GDPR.
- One size fits all – the solution must not appear as one solution that fits all problems. Individual stakeholders have to be able to configure the solution to meet their requirements. Therefore, implementation guidelines have to be available to indicate how individual organizations can adopt and implement the solution.

4 Technology Independent Services

This building block - technology independent services or platform services - will prevent a lock-in of a user with any platform, enables all users to use the federated platforms including SMEs (level playing field), and allows platform providers to increase their market share.

4.1 Objective

The objective of this activity is to produce the technology independent platform services to be offered by the federated platform to support business interoperability for a number of selected business services and their compliance with legislation.

4.2 Tasks

4.2.1 Business and authority interoperability principles

The objective of this task is to define the basic principles for digital interoperability between enterprises and between enterprises and authorities operating in an organizational network. There are potentially thousands of chains in an organizational network and their number will increase in case organizations implement supply chain innovations like agility, dynamic and synchromodal planning, and resilience. The basic principles will set the system boundaries.

Two possible scenarios for which modelling is required are bilateral interoperability of any two enterprises and compliance with applicable legislation, and business goals and services of customers and service providers respectively to perform logistics activities.

4.2.2 Business scenarios

The objective of this task is to explore a number of business scenarios, additional to the ones developed by the first mandate of DTLF SG2, and identify potential variations. These business scenarios will set the scope for the technology independent services in terms of the process and data requirements modelled by the semantic model.

The objective of the business scenarios is to specify the system boundaries relevant for further development by DTLF SG2 in its current mandate.

The business scenarios need to contain at least the following elements:

- Physical environment - the physical flow of objects and transport modalities involved.
- Transaction tree – the transaction hierarchy between organizations involved in the business scenario. Within transaction trees, a distinction might be made between ordering/execution and payment/settlement, including the relation between those trees.
- Sequence diagrams – examples of sequence diagrams showing the flows of for instance bookings, transport orders and planning information (the choice of flows depends on a business scenario that is modelled).

4.2.3 Business transaction choreography

The objective of this task is to model the interaction sequencing for bilateral interoperability between any two enterprises, providing sufficient data at the proper moments to authorities. The choreography consists of a high level choreography showing the overall flow from publishing and searching for business services (marketplace functionality) to visibility for execution of physical activities and a detailed specification of these high level tasks (see also the final report of DTLF SG2 first mandate).

Interaction sequencing is modelled as a BPM choreography (BPM: Business Process Modelling, an OMG standard (www.omg.org/bpm)). The choreography itself can be more formally specified using for instance SHACL (Shape Constraint Language) for both the flow and the data required for individual transaction types like booking and order. The latter, data requirements of individual interaction types, is expressed in terms of the semantic model, either with its own semantic model (e.g. an order model) or minimal data requirements (this is for further research during this activity). The interaction flow might also be expressed in some other type of machine-readable structure than SHACL (also for research in this activity).

4.2.4 Semantic model

The objective of this task is to develop a first version of the so-called upper semantic model ('upper ontology') and one or more related semantic models ('lower ontologies') for the required platform services. The upper semantic model consists of all the concepts and properties that are relevant to supply and logistics chains, thus they need to be specified as technology and as organization independent. The upper semantic model reflects the various cargo types, modalities, and the concepts of business services.

Related semantic models specify for instance data for a particular document type (e.g. an eCMR), specifics of a modality (e.g. sea and air) or particular data requirements to support a particular piece of legislation or part of it. For instance, a related semantic model might support customs procedures, where that latter model is the basis for specifying import procedures. Related models might contain additional concepts and properties that are only relevant to that model and will not be part of the upper semantic model.

The semantic model will be based on the data requirements already implemented in existing (open) standards. These include standards like developed by UN/CEFACT, GS1, WCO, and others.

4.2.5 Platform services

The objective of this task is to transform the business process choreography into platform services. The transformation includes a number of implementation choices:

- Technical representation – the representation of interaction sequencing by for instance APIs, linked data, and/or messaging, and a syntax applied for sharing the data (e.g. XML, JSON, RDF).
- Technology choice – different parts of the choreography might require different technology choices. For instance, booking and ordering might require no data storage by any of the platforms, whereas visibility could require publish/subscribe mechanisms. These technical choices might require additional platform services that are not specified by the choreography. An example is the registration of a subscription to visibility events for 'publish/subscribe', where the subscription is as such not part of the choreography.
- Data representation – a conceptual data representation by a semantic model(s) will be implemented as views or combinations of concepts and properties into an additional element.

For instance, conceptually supply chain visibility is for instance of events for loading and discharge of containers or movements of vessels, where technically, it might be generalized to events of physical objects that can be of type ‘container’ and ‘vessel’, but also of type ‘truck’ and ‘barge’. These choices for technical data representation have to be specified for compatibility of platform services.

4.2.6 Standards support

The objective of this task is to construct a relation between concepts and associations with (groups of) data elements specified by (open) standards. Links to these data element (groups) will be included in the semantic model(s). This task may result in extension of the semantic model(s) and/or creating a specific view of a model.

4.3 Dependencies

The development of the semantic model (D_{TIS}4) and the business process choreography (D_{TIS}3) requires availability of D_{PP}1 – business service specifications.

4.4 Resource requirements

There is a requirement for the following skills and expertise:

- Business expertise – relevant knowledge of the business scenarios and business process interactions.
- IT skills – skills of constructing semantic model(s) (ontologies), business process choreographies, SHACL, to produce API specifications.
- Legal skills – skills for formulating legal requirements relevant to business process choreography.
- Standards expertise – knowledge of existing (open and defacto) standards.

4.5 Challenges and risks

The following challenges and risks are identified, additional to those mentioned in section 2:

- Choreography versus activity diagrams – it is of major importance to recognize the difference between choreography and activity diagrams: a choreography only models bilateral interoperability (behaviour of two organizations) and activity diagrams include the internal activities to achieve this behaviour. The latter is internal to any organization and is outside scope. However, many individuals tend to model their perspective of the world, namely activity diagrams relevant to their organization.
- Skills and expertise – this task requires particular business and modelling skills. The combination of skills is rare, potentially additional support is required from EC DG DIGIT and/or the CEF funded projects.
- Adoption - industry does not recognize the proposed models, standards and recommended practices and fails to implement these. Interaction with industry is required to fine-tune the specified platform services.

- Market change - market overtakes the DTLF efforts, which becomes obsolete due to significant market developments, including dominant platform solutions.
- Lack of understanding and alignment between stakeholders.
- Insufficient or ineffective change management.
- Absence of sufficient value or business case.
- Insufficient development resources at either DTLF or industry.
- Parallel development and emerging standardization activities from different organizations might challenge that different standards will be adopted.

5 Federation of Platforms

This building block - federation of platforms or platform interoperability - will establish harmonized connectivity and interoperability of different solutions (platforms).

5.1 Objective

The objective is to create interoperability between different platforms, even when each platform is realised with different technology. Platform interoperability goes hand in hand with technology independent platform services and can be expressed in two layers:

- Technical protocols – protocols that support platforms to actually share data amongst each other.
- Functional protocols – support of the platform services by each of the interoperable platforms. Functional protocols are specified in two ways:
    - Vertical interoperability – two platforms with identical platform services are interoperable.
    - Horizontal interoperability – two platforms with adjacent functionality are able to share data, for instance a logistics marketplace integrates with a booking site.

5.2 Tasks

5.2.1 Architecture

The objective of this task is to draft the architecture of a federated network of platforms, which includes peer-to-peer data sharing. The components will be identified, including their interfaces. A Registry and Access Point (see task ‘plug and play) are examples of such components, but also a message exchange component, publish/subscribe component, and an API registry might be identified (see task ‘technology independent services’). Potential interfaces between components will be associated with functionality required to support the business process choreography.

5.2.2 Technical protocols

The objective of this task is to identify and select the technical protocols that can be used to create connectivity between any two platforms, peer-to-peer solutions, and a peer-to-peer solution connecting to a platform. A technical protocol needs to support the technical requirements for data sharing, e.g. messaging and APIs. A number of protocols will be listed, based on desk research, and analysed their applicability.

5.2.3 Functional interoperability

The objective of this task is to support data sharing between any two enterprises, where each of the enterprises uses a different implementation, i.e. two different platforms, peer-to-peer solutions, or a peer-to-peer solution integrating with a platform. Two types of interoperability are to be developed, including particular mechanisms for their implementation:

- Vertical interoperability – two platforms with identical platform services are interoperable. Two visibility platforms used by two logistics enterprises that can share events and milestones are an example of vertical interoperability.

- Horizontal interoperability – two platforms with adjacent functionality are able to share data, for instance a logistics marketplace integrates with a booking site.

The implementation of functional interoperability can be based on mechanisms like linked data (e.g. an order shared via a platform referring to a booking confirmation or framework contract specifying delivery conditions and payment terms), messaging (e.g. data or a link that is 'pushed' from one solution to another), or APIs (e.g. one solutions calls the APIs of another to post data). These mechanisms and the syntax for sharing the data will be analysed for their implementation.

5.2.4 Payment, clearing and settlement

The objective of this task is to identify any requirements on payment of data shared between any two platforms or between a platform and a peer-to-peer solution as a basis for payment and settlement. Each platform will have a particular business model with pricing and conditions. Since different users can be using different platforms, data is shared between those platforms. Structures like for instance used in the Internet by different Internet Service Providers or mobile operators in telecom might be applicable.

5.2.5 Configuration components

The objective of this task is to identify and analyse the required modelling – and configuration components for developing and extending the technology independent platform services, for creating platform interoperability, and to support plug and play. These components are a tool chain with interfaces that are required for end-users and IT service providers.

Most probably there is not a tool chain with the proper interfaces for seamless sharing of configuration files and models. Thus, interfaces have to be developed between these tools and can be proposed as standards to for instance W3C (World Wide Web Consortium, focussing on development of standards like OWL and SHACL).

5.3 Dependencies

$M_{TIS}2$ – platform services – needs to be completed to address functional interoperability. $M_{PP}3$ – data requirements – needs to be clearly specified for developing a tool chain.

Payment, clearing and settlement depend on and provide input to the governance procedures of BB Trusted, Safe and secure.

5.4 Resource requirements

There is a requirement for the following skills and expertise:

- IT platform expertise – expertise on the potential integration of platforms for data sharing and their business models is required.
- IT architecture skills – expertise for drafting a (high level) IT architecture of federated platforms.
- IT technical skills – skills for analysing and evaluating technical protocols.
- IT modelling skills – skills for assessing a tool chain for configuration of platform services.

5.5 Challenges / Risks

The following challenges and risks are identified, additional to those mentioned in section 2:

- Lack of IT skills – DTLF SG2 does not have sufficient skills and expertise to specify the functional and technical protocols
- Lack of knowledge of platform providers – DTLF SG2 lacks knowledge of business models and functionality of the various platform providers.

6 Trust, safe and secure

This building block - trusted, safe and secure - will provide general mechanisms like identity and authentication that ensure trust into the federated platforms, and the technical, legal and organizational governance of the solution.

6.1 Objective

The objective of this activity is to establish a neutral governance structure ensuring trust, safety, and security for data sharing via multiple providers of platform services, including peer-to-peer solutions. This involves various aspects that will be developed during this activity (see deliverables and tasks).

6.2 Tasks

6.2.1 Analyse best practices in other sectors

The objective is to learn from governance structures implemented in other areas with similar characteristics. The most obvious one is the Internet, another one is that of mobile operators. One or more sectors are selected and analysed with respect to their governance structure. What lessons can be learned from other sectors that evolved to a similar proposed (to-be) situation envisaged for supply and logistics (federated platform)? Can we learn from how the Internet has been established (ICAN, IETF, W3C), how the financial markets evolved, etc.?

6.2.2 Identify stakeholder groups

The objective of this task is to identify the relevant stakeholder groups from a governance perspective in supply and logistics sector, including their willingness to adopt the proposed solution (SWOT – Strength, Weakness, Opportunity, Threat analysis, based on the results of all building blocks addressed in the document). First movers will have to be identified and their skills will have to be analysed with respect to the adoption of the proposed solution.

6.2.3 Governance structure and terms of reference

The objective of this task is to specify and establish the required governance structure, based on the stakeholder analysis and best practices analysed. Each body in the governance structure will have its terms of reference. Part of this task is also to identify the various objects that need coordinated governance, independent of any solution implementing the governance.

Based on the identification of governance objects, relations with standardization bodies and/or user groups representing a particular subdomain in supply and logistics will be established. One has for instance a user group representing traders in commodities, called FOSFA. These can become part of the community and will focus on their specific needs.

6.2.4 Identification and authentication

The objective of this task is to define identification and authentication requirements and solutions. It requires validation of an identity by an Identity provider and a Certification Authority providing authentication. Particular rules need to be established like identity validation against an independent (authority) organization like a chamber of commerce.

Various mechanisms and standards will be analysed and evaluated resulting in a concrete proposal for a solution, possibly an extension of existing standards. In addition, protocols/solutions for federation of identity and its authentication (e.g. eID) and the role of platforms in supporting a federated identity need to be analysed. It is unlikely that an identity accepted in one country will also be accepted by other countries on a global scale. This requires therefore the federation of identities and selection of protocols for authentication.

6.2.5 Procedures

The objective of this task is to specify procedures for the various standardization bodies and user groups to maintain and extend the specifications. It cannot be expected that DTLF SG2 develops a complete solution for all interoperability issues, since future requirements will evolve when users apply the models in their settings. These users require clearly specified procedures and have to refer to the relevant bodies to have their requirements addressed properly. These procedures involve 'version management'.

6.2.6 Define security requirements

The objective of this task is to specify any additional security requirements to the various components and interfaces identified in the architecture. These security requirements need to cater with all types of cyber security attacks and (temporary) storage conditions for data (including personal data according to GDPR). They may result in certification and validation procedures to assure that all components and interfaces implemented by different providers work according to the specification.

Additional requirements for the infrastructure relate to performance and availability of individual components, where providers of components might be required to install fall-back functionality and/or have the ability to switch (temporarily) to a component of another provider.

6.2.7 Adoption and implementation instruments

The main objective is to identify first movers (see stakeholder groups). However, there may be particular instruments like financial support or new legislation to stimulate the adoption and implementation. The governance structure may for instance become part of a new legislative act.

Potentially a proposal for a new legislative act (or other stimulation instruments) will be required, but this is not made a separate deliverable or milestone since it depends on the identification and choice of instruments to stimulate the adoption and implementation of the proposed solution.

6.3 Dependencies

The foreseen dependencies are in $M_{TIS}1$ – basic principles – and $M_{PI}1$ – architecture. Both are input for identifying the required governance objects.

6.4 Resource requirements

There is a requirement for the following skills and expertise:

- Policy and governance expertise – expertise to set up a governance structure with its terms of reference.
- IT skills and expertise – knowledge of the architecture, distributed maintenance and development.

6.5 Challenges and risks

The following challenges have to be addressed for this building block:

- Incentive must be strong enough – there have to be incentives for all relevant stakeholders to migrate and adopt the proposed solution.
- Reluctance to share data because of commercial sensitivity – there will be a reluctance by organizations (enterprises and authorities) to share data, since it may imply they become liable if others use that data in decision-making. There have to be mechanisms that a user is in control of its data (data sovereignty).