Eemsgolaan 3
9727 DW Groningen
P.O. Box 1416
9701 BK Groningen
The Netherlands

www.tno.nl

T +31 88 866 70 00
F +31 88 866 77 57

TNO report

Considerations on data space connectors and connectivity protocols

To support the Basic Data Infrastructure (BDI) in view of the emerging Common European Data Space

Date June 2023
Report number TNO 2023 R10610

Author	H.J.M. (Harrie) Bastiaansen, PhD	TNO
	E.D.K. (Eliza) Hobo, MA	TNO

Report nr	TNO 2023 R10610
Number of pages	37
Project number	060.56621

Management summary

Federative data sharing is becoming increasingly prominent, which is evident from the numerous data sharing initiatives emerging across sectors in Europe. The National Growth Fund project Digital Infrastructure Logistics (NGF DIL, or simply DIL) pursues to realize a federative data sharing infrastructure adhering to the architectural concepts as developed by EU CEF FEDeRATED project.

In developing the BDI, the question has arisen what data space connectors and connectivity protocols are suitable to support the BDI-architecture. Although this may at first seem merely a ‘technical’ question, there are also clearly more strategical aspects involved. This especially applies to the considerations on a data space connector, as a data space connector is a pivotal component in the overarching data sharing environment being developed. Therefore, the considerations on data space connectors and connectivity protocols as presented in this report are positioned in the broader context of the federative data sharing developments in the EU.

Federative data sharing is clearly on the radar of the European Commission. Its release of the European Data Strategy, its associated acts and regulations and the support of both reference architecture development initiatives and (cross-)sectoral deployment initiatives illustrate the importance the EC attributes to (federative) data sharing for society and the economy.

There are many commonalities among these various initiatives, such as the European values of autonomy, data sovereignty and a level playing field. However, in the tangible choices these initiatives make differences emerge: in the type of data sharing that is pursued, the different (reference) architectures being developed and the various deployment initiatives that are supported. Moreover, EU regulations prescribing data sharing guidelines for specific application areas further complicate the picture and provide limitations to the freedom to develop and deploy new and overarching architectures for federative data sharing.

These observations are also very much applicable to the logistics sector. Organizations operating in logistics potentially have interactions with organizations operating in almost any other sector that in turn are part of data sharing initiatives borne out of their specific needs. Seen from the individual organizations, this creates a meshed network of data sharing initiatives that becomes more complicated to connect and work with every time a data sharing environment is created with a different set of unaligned architectural solutions.

The EC’s response to the risk of an unworkable inconsistency of federative data sharing reference architectures development initiatives and (cross-)sectoral deployment initiatives is the European Data Strategy with the ambition of the ‘Common European Data Space’ under the supervision of DG Connect. The current European Commission under President Ursula von der Leyen concluded in 2020 that for Europe to keep a sovereign position in the digital space, action was needed to counter the large centralized data platforms. The vision is a European model where data get unlocked from their silo’s and will be used to the benefit of companies and people, based on a system where the owners control sharing of their data with guarantees, built on fair and balanced agreements. The European Data Strategy that followed out of this vision in 2020 has been translated into legislation, regulations, investments in governance mechanisms and even a procurement action to build relevant software.

The concept of federative data sharing was not a new invention and many other initiatives including from other EC DG’s preceded this European Data Strategy.

Concrete examples are the CEF FEDeRATED and FENIX Actions commissioned by DG Move with the objective to provide input to and validate the architecture developed by the Digital Transport and Logistics Forum (DTLF), an expert group raised and chaired by DG Move. DTLF has been responsible for the architecture of FEDeRATED. On its turn, the FEDeRATED architecture forms the basis for development of the Basic Data sharing Infrastructure (BDI) by the DIL project.

In addition, other (and adjacent to logistics) federative data sharing initiatives have started on a regional, national or multi-national level. These initiatives, borne out of similar design criteria as the EC stipulated, have taken various directions. This is no surprise, given that each of them saw their own sectoral, market and practical needs as the starting point, without having to cope with the larger vision of an interoperable cross sectoral Common European Data Space.

The strategic issue at hand is therefore how these various initiatives can be aligned with the overarching European Data Strategy. The answer from the EC on this question is procedural and organizational by nature. In effect, the responsibility for the general system that guarantees interoperability between sectors is with DG Connect. The responsibility for the sectoral data spaces is with the DG's that cover their sector. This means that the data spaces in logistics and mobility are in the remit of DG Move. A governance is in place where the DG's meet to discuss the necessary alignment, in the so-called Interservice Steering Group, chaired by DG Connect. The EC governance is relevant and important, but ultimately an architecture is needed that determines all other practical arrangements that ensure interoperability such as standards, processes, etc..

As such, and in practical terms, the current challenge for the development of the BDI by the NGF DIL project is whether, how and when to align with the EC's development and deployment initiatives on the Common European Data Space. More specifically, this translates into the considerations on the selection of suitable data space connectors and connectivity protocols for the BDI architecture as addressed in this report.

From the considerations on data space connectors and connectivity protocols to support the BDI in view of the emerging Common European Data Space, the main conclusions are:

- From the data space connectors and connectivity protocols as considered in this report, there is not a specific one that currently fits all of the requirements as defined for the development of the BDI (as based on the FEDeRATED architecture).
- Instead of selecting a specific solution for the data space connectors and connectivity protocols it is recommended that the development of the BDI adopts the architecture framework for data space connectors as pursued by the Eclipse Dataspace Connector (EDC) initiative. Various (main and adjacent) European data space initiatives already have adopted the EDC. It is to be realized that adopting the EDC by different data spaces does not automatically mean interoperability between these data spaces. However, it will provide the flexibility to develop and migrate to a common approach interoperable across data spaces.
- The blueprint for federative data sharing and data spaces as currently being developed by the EU Data Spaces Support Centre (DSSC) initiative in combination with the upcoming EU SIMPL procurement initiative will provide the formalized EU architecture and open-source building blocks for the Common European Data Space. The DSSC and SIMPL operate under the overarching

governance of the European Data Innovation Board (EDIB). These initiatives are geared to solve the interoperability and scaling challenges.

However, the DSSC blueprint is currently (i.e. medio 2023) in development. DSSC Expert Groups are starting to the define common building blocks based on the requirements provided by a broad variety of EC-sponsored data space Collaboration and Support Activities (CSAs), e.g. the European Mobility Data Space CSA which also includes logistics. Therefore it is recommended:

- To include the specifics of the requirements of the BDI as input for the current European Mobility Data Space Collaboration and Support Activity (EMDS CSA) providing mobility (including logistics) specific inputs for the development of the the EU DSSC blueprint and its building blocks. The blueprint needs to accommodate the business requirements and consider architectures and solutions from the various sectoral data spaces.
- To take care that the BDI requirements are adequately taken into account in the further work on the DSSC blueprint. The CSA's input will be collected through the Communities of Practice of the DSSC in which the sectors are represented. Active involvement of DIL in the development of the DSSC blueprint should be considered. The most important topics seem to be inclusion of the FEDeRATED Index and Service Registry.

The observations and recommendations may pose the NGF DIL with a challenge. DIL's short-term goals with respect to the BDI development and deployment may not align with the timelines for adopting the EDC as data space connector and for aligning with the DSSC blueprint and the SIMPL building blocks development. A strategy may be needed that minimizes the risks associated with migration and evolution in adopting a data space connector approach. As part of this risk mitigation strategy it is recommended for the NGF DIL:

- to get actively involved (on the short term) in and influence the work on the EU DSSC blueprint and the SIMPL building blocks,
- to get familiarized with the approach and concepts of the EDC framework for data space connectors, including its architectural approach for the separation of the control plane and data plane and interoperability as defined by the emerging Dataspace Protocol,
- to assess how the approach of adopting the EDC and adhering to the EU DSSC blueprint and SIMPL initiatives is impacted by (and vice versa may / should impact) the existing regulations as applicable to logistics data sharing areas, e.g. on EFTi, EBSI, eDelivery and eIDAS (theses regulatory constraints have been out-of-scope for this report), and
- to highlight the associated risk upwards in the governance chain to make sure that changes down the line and potential additional efforts and costs will not come as a surprise.

Finally, it is recommended to mutually align on the data space connector and connectivity protocol approaches with the NGF DMI and the NGF DITM. These NGFs have been initiated in the context of the Dutch MinI&W and are adjacent to the NGF DIL. Common interest and benefits may be explored in aligning the data space connector and connectivity protocol approaches.

Table of contents

1 Introduction

1.1 Background

The Digital Transport Strategy for freight transport is the long-term strategy of the Ministry of Infrastructure and Water Management (MinI&W) to realize full digitization of freight transport data [1]. The development of a Basic Data Infrastructure (BDI) is one of the three milestones that is identified in the Digital Transport Strategy.

The Digital Transport Strategy defines the BDI as a federated network of platforms and IT systems that offers companies and authorities the procedural and technical capabilities to securely share data with each other in a decentralized, open, and neutral manner. It adheres to the vision as developed by the CEF funded FEDeRATED Action. Currently, this is more generically referred to as ‘federative data sharing’. Federative data sharing is considered as an attractive option to address the challenges for fully exploiting the business potential for the emerging data economy: it enables the (sharing of) ubiquitous available data, whilst adhering to the European values of data sovereignty.

The Dutch National Growth Fund (NGF) project ‘Digital Infrastructure Logistics’ (DIL) aims to develop the BDI, taking the architecture as being developed in the EU FEDeRATED project [2][3] as reference. The key FEDeRATED principles that are adopted are

(1) to keep the (potential sensitive) data at the source by means of

(2) a pull-based mechanism through the sharing of links.

These principles of the EU FEDeRATED project represent a type of data sharing that currently is also referred to as ‘federative data sharing’. Federative data sharing is a core element in the European Data Strategy [4]. As such, both the development of reference architectures and a deployment strategy have been defined by the EC, as will be further described in chapter 2.

1.2 DIL, BDI and FEDeRATED

The approach as pursued by the NGF DIL project in developing the BDI adheres to the principles for the FEDeRATED architectural principles [3], as highlighted in the BDI Framework Key Requirements document [5] [1]. The (ultimate) ambition is a distributed implementation of ‘FEDeRATED Nodes’ [2]. At a high-level, the connectivity

[1] A key element in the FEDeRATED architecture is the concept of 'events'. Events are defined in the ontology. Data providers implement a publish-subscribe mechanism for events. Data receivers can subscribe to events. Published events incorporate a link to the resource where additional data about the event can be accessed, under the condition that the data receiver is authorized to do so [5].

[2] In [3] (section 3.4), the FEDeRATED (data sharing) node is described as the actual component for findability of service providers and data and the sharing of (linked) data. The main aspects of the nodes are to identify the data distribution algorithm, i.e. who receives which links, and how can data quality be assured (event logic, correctness/completeness of data, etc.). A node, which fully supports the language, must also be able to support one or multiple options of the presentation -, security -, and connectivity protocols. This requires a so-called 'semantic adapter', taking care of the transformations between various presentation protocols via the semantic model. The concept of a ‘node’ can be implemented by a stakeholder, a platform, as a (cloud) solution or by existing IT systems of stakeholders.

architecture to support interactions between the FEDeRATED Nodes is depicted in Figure 1 [3].

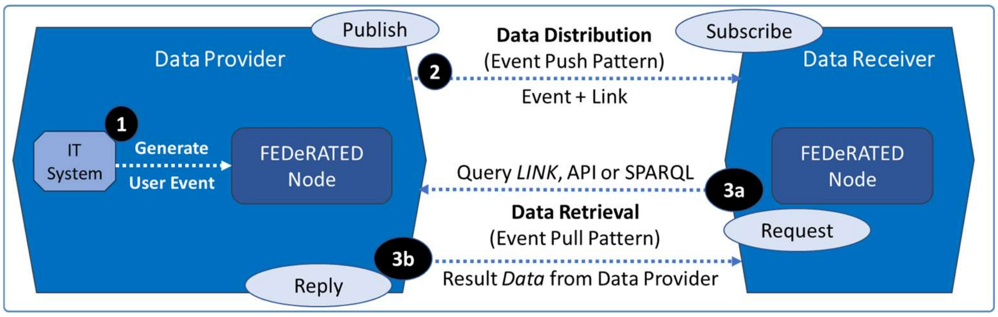


Figure 1: High-level connectivity architecture between FEDeRATED Nodes [3].

As the figure shows: three main parts are identified in the FEDeRATED architecture where data space connectors and connectivity protocols may be applicable [3]:

1. The connection between an existing IT system of a data provider and the FEDeRATED node of the data provider to transfer a ‘generate user event’ to start the flow of data sharing actions. As this applies to an internal process of the data provider, this part is further out-of-scope for this report.
2. The connection between the (FEDeRATED nodes at the) data provider and the data receiver to distribute links to all relevant data receivers. This is referred to as ‘data distribution’. Data distribution is done by means of a (publish / subscribe) ‘push’ mechanism.
3. The connection between the (FEDeRATED nodes at the) data receivers and the data providers to retrieve the (potentially sensitive) data at the source. This is referred to as ‘data retrieval’. Data retrieval is done by means of a (request/reply) ‘pull’ mechanism, in which the data receiver queries the data provider using the obtained link (step 3a in the figure) after which, when authorized, the results are provided by the data provider to the data receiver (step 3b in the figure).

In the trajectory towards the BDI implementation conforming to the FEDeRATED architecture, the NGF DIL project considers adopting a gradual development approach for the BDI to allow participants to create value quickly with minimal dependence on wide-scale adoption.

[3] It is to be noted that in this report the terminology for roles is applied as provided by the DSSC Glossary [11], distinguishing the following roles:

- *Data rights holder*: A transaction participant that has the legal right to use, grant access to or share certain data.
- *Data provider:* A transaction participant that, in the context of a specific data transaction, technically provides data to the data receivers that have a right or duty (granted by the data rights holder) to access and/or receive that data.
- *Data receiver*: A transaction participant to whom data is, or is to be technically supplied by a data provider in the context of a specific data transaction.
- *Data user:* A transaction participant that has been granted (lawful) access and the right to use data as the result of a specific data transaction. Also known as data rights receiver.

1.3 Considerations and scope

Based on the observation that various reference architectures are being developed that support a (seemingly) similar goal of federative data sharing, the considerations in this report address the question:

In view of the emerging Common European Data Space and the various reference architectures development and deployment initiatives for federative data sharing and data spaces, which data space connectors (and connectivity protocols) could / should be used for the BDI target architecture?

As indicated in the previous sections, the NGF DIL project develops the BDI based on the FEDeRATED architecture with the high-level connectivity architecture as described in the previous section. The scope of the considerations are on the 'data distribution' and the 'data retrieval' activity as described in the previous section, i.e. for the connectivity between the FEDeRATED Nodes for the second and third type of connection as depicted in Figure 1.

1.4 Approach

As basis for the considerations, the various data space connectors and connectivity protocols that are developed in the relevant reference architecture development initiatives for federative data sharing and data spaces are identified. They are considered on their suitability to support the BDI in view of the emerging Common European Data Space.

Logistics is cross-border and cross-sector by nature, requiring both interoperability between geographical logistics data space initiatives and with other sectoral data space initiatives. Hence, to be futureproof, to minimize the risks of (complex and costly) migration and to strive for convergence towards the ambition of a Common European Data Space, the approaches on data space connectors as adopted by adjacent data space initiatives are taken into account.

Furthermore, the considerations in this report are based on broad TNO-expertise and experience in both the development of federative data sharing and data spaces (reference) architecture initiatives and the deployment thereof, the FEDeRATED architectural approach and the basic knowledge of data space connectors and connectivity protocols.

1.5 Structure of the report

The report has the following structure: Chapter 2 describes the broader EU perspective on federative data sharing and data spaces as expressed by the EU Data Strategy with the ambition of a Common European Data Space, providing the context for the considerations on data space connectors and connectivity protocols the development of the BDI. The following chapter 3 and chapter 4 present the considerations on the data space connectors and the connectivity protocols, respectively. The final chapter 5 provides the overarching conclusions.

2 The EU perspective on federative data sharing

Goods flows and logistics are international. Therefore, EU developments and EC directives are important to take into account. As such, the Digital Transport Strategy (as described in section 1.1) refers to the European Communication on a Common European Data Space (as defined in the European Data Strategy [4]) as a way forward for the MinI&W to realize full digitization of freight transport.

Therefore, this chapter addresses the broader EU perspective on federative data sharing and data spaces [4] as context for the considerations on the data space connectors and the connectivity protocols in the follow-up chapters.

The subsequent sections in this chapter address the European Data Strategy, the EU Reference architecture initiatives on federative data sharing and the EC's role in supporting the deployment of data spaces, respectively.

2.1 European Data Strategy: data spaces

Federative data sharing is clearly on the radar of the European Commission. Its release of the European Data Strategy [4], the Data Governance Act [6] and the additional input sought on data spaces through the OPEN DEI initiative [7][8] illustrate the importance the EU attributes to data sharing for society and the economy. Moreover, various (European and national) initiatives are exploring the potential, reference architectures, and deployment for federative data sharing. An extensive overview on federative data sharing initiatives is given in [9].

The ambition on federative data sharing in the EU Data Strategy is expressed as a '*Common European Data Space'*. Alternatively, this may be phrased as: *'Towards a Federation of Interoperable Data Spaces'.*

The individual concepts in this EU ambition spaces need clarification:

- *Data space*

  The EU Data Spaces Support Centre (DSSC) initiative [10] is working towards a blueprint for the emerging (federation of) data spaces in Europe. It has defined a data space [11] as '*an infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. Data spaces should be generic enough to support the implementation of multiple use case*'.

  Moreover, the EU OPEN DEI initiative [7] has identified three types of building blocks that a data space should provide [8]: (1) building blocks such as *data platforms*, (2) building blocks such as data *marketplaces* and (3) building blocks ensuring *data sovereignty*.[5]

[4]. Although the broader perspective on federative data sharing as described in this chapter has the focus on the EU, there are also global producers (and customers) to be taken into account who must also be able to supply and consume data in a manner acceptable to them.

[5] The EU OPEN DEI initiative has defined a data space as "a decentralized infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed upon principles", [5] providing three types of building blocks: (1) building blocks such as *data platforms*, providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities, (2) building blocks such as *data marketplaces*, where data providers can offer and data receivers can request data, as well as data processing

- *Federation*

  There will be a multitude of European data spaces, e.g., for individual sectors, application areas or geographical regions. Being able to seamlessly share data over these data spaces yields clear advantages: It extends the reach and scope of accessible data and allows new business models and solutions to be developed across sectors and regions. Hence, jointly, the European data spaces pursue the common goal of being able to share data in a trusted manner between participants in different data space instances, whilst each individual data space instance has a high degree of autonomy in developing and deploying its own internal agreements and ICT landscape [12].

- *Interoperability*

  For data spaces to seamlessly interconnect in a federation, an interoperability framework is needed to manage and co-ordinate trusted and controlled data sharing between participants in multiple data space instances. An approach to systematically address the interoperability challenges is provided by the new European Interoperability Framework as developed by the European Commission [13]. It shows that data space interoperability is more than only the interoperability of its technical components. It distinguishes four interoperability levels (technical, semantic, organizational, and legal interoperability) under an overarching integrated governance approach. Each of these interoperability levels needs to be addressed.

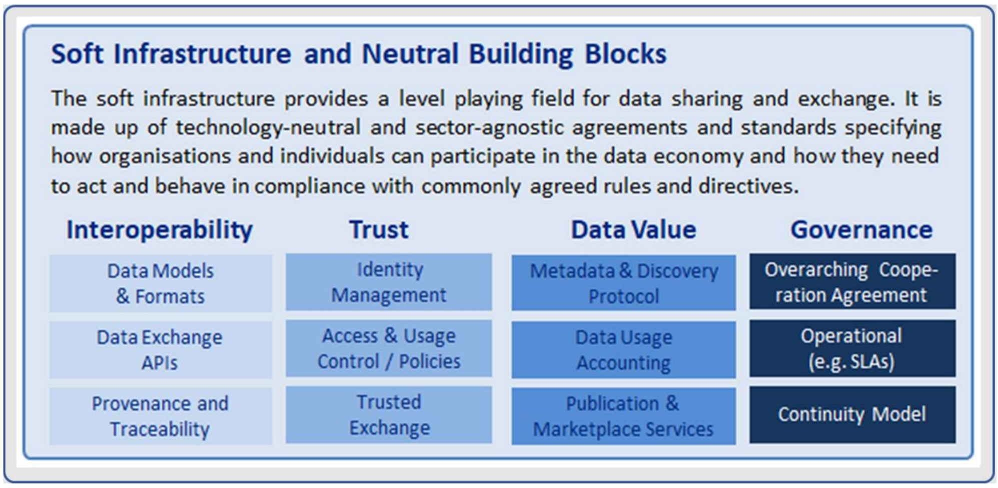
2.2 EU Reference architecture initiatives on federative data sharing

Various EU initiatives work on defining and aligning federative data sharing and data space reference architectures and developing reference implementations for their enabling building blocks. A main initiative defining the policy, approach and building blocks is the EU OPEN DEI initiative [8]. It aims at supporting the creation of a common data space (in the context of the ambition as expressed in the European Data Strategy, see section 2.2) based on a unified architecture and an established standard.

The OPEN DEI initiative has elaborated the data space concept in terms of a soft infrastructure consisting of 12 building blocks [8] as depicted in Figure 2 [6].

applications, and (3) building blocks ensuring *data sovereignty*, i.e. the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

[6] It is to be noted that the DSSC is building upon the OPEN DEI soft infrastructure and its building blocks to create an updated data space taxonomy, which will be formally released on short notice. The DSSC data space taxonomy is to a large extend similar to the OPEN DEI soft infrastructure and its building blocks.



Soft Infrastructure and Neutral Building Blocks

The soft infrastructure provides a level playing field for data sharing and exchange. It is made up of technology-neutral and sector-agnostic agreements and standards specifying how organisations and individuals can participate in the data economy and how they need to act and behave in compliance with commonly agreed rules and directives.

Interoperability	Trust	Data Value	Governance
Data Models & Formats	Identity Management	Metadata & Discovery Protocol	Overarching Coope-ration Agreement
Data Exchange APIs	Access & Usage Control / Policies	Data Usage Accounting	Operational (e.g. SLAs)
Provenance and Traceability	Trusted Exchange	Publication & Marketplace Services	Continuity Model

Figure 2 The OPEN DEI soft infrastructure and neutral building blocks [10].

As the figure shows, the OPEN DEI soft infrastructure distinguishes between technical building blocks (in the verticals ‘Interoperability’, ‘Trust’ and ‘Data Value’) and governance building blocks (in the vertical ‘Governance’), with trust and its associated building blocks being a key and integral part of the data space concept. OPEN DEI defines a trust framework as ‘a structure that lets people and organizations perform business securely and reliably online’.

The OPEN DEI soft infrastructure and its building blocks have been identified and described at a high abstraction level. Technical specification and elaboration of the building blocks are done by various European initiatives on reference architectures and building block implementations. The most noteworthy of these EU initiatives are:

- The *International Data Spaces Association (IDSA) initiative*, having developed a reference architecture model for data spaces [14]. The IDS data space architecture leverages existing standards and technologies as well as governance models for the emerging data economy. It facilitates secure and standardized data exchange and data linkage in a trusted (business) ecosystem, thereby providing a basis for creating smart service scenarios, while at the same time guaranteeing data sovereignty for data owners. The IDSA GitHub pages provide both a repository with the specifications for the IDS components [15] and an overview of repositories with IDS open-source components [16].

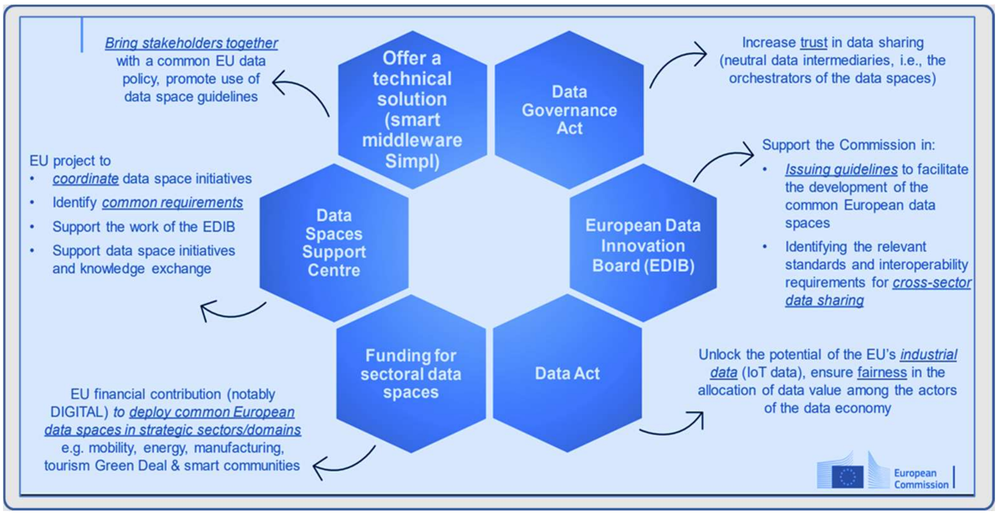
- The *Gaia-X initiative* has the goal to establish an ecosystem in which data is made available, collated and shared in a trustworthy environment in which entitled parties always retain sovereignty over their data [17]. It develops a software framework of control and governance and implements a common set of policies and rules that can be applied to existing cloud / edge technology stacks to obtain transparency, controllability, portability and interoperability across data and services. The Gaia-X architecture aims at a set of interconnected data and infrastructure ecosystems, enabled by a set of Gaia-X Federation Services (GXFS) [18]. The Gaia-X Federation Services are services used for the operational implementation of a Gaia-X Data Ecosystem. They are categorized into four groups: Identity & Trust, Data Sovereignty Services, Federated Catalogue and Compliance.

- The *FIWARE initiative* brings a curated framework of open-source software platform modules, building around the FIWARE Context Broker. A suite of complementary open-source FIWARE Generic Enablers is available, dealing with (amongst others) the building blocks for ‘Context Data/API management, publication, and monetization’ for the support of usage control and the publication and monetization part of managed context data. An overview of FIWARE open-source modules (i.e. the FIWARE Generic Enablers) can be found at [19].

- The *iSHARE initiative* provides a trust framework for data spaces. iSHARE originates from the logistics sector in the Netherlands [20] and is expanding towards other sectors and application areas as well. Moreover, iSHARE provides trust framework capabilities for sharing data both within a single data space and across multiple data spaces, i.e. for both ‘intra’ data space interoperability and for ‘inter’ data space interoperability, as addressed in the following chapters, respectively. For enabling data spaces iSHARE currently provides a legal framework, trust registration and administration, discovery and inter data space interoperability capabilities [21].
- The *Data Space Business Alliance (DSBA) initiative* [22] in which the International Data Spaces Association (IDSA), Gaia-X, the Big Data Value Association (BDVA) and the FIWARE Foundation have worked together on an aligned and coherent architecture for data spaces [23].
- The *Data Spaces Support Centre program* aims to facilitate common data spaces that collectively create an interoperable data sharing environment in Europe [10]. Therefore, it is working towards the DSSC Blueprint. The DSSC blueprint is currently under development, the first version is expected to be realized by the end of 2023.

2.3 The EC’s role in supporting the deployment of data spaces

To work towards the ambition of a Common European Data Space as expressed by the EU Data Strategy [4], the EC has initiated as set of initiatives as part of its Digital Europe program to address the development and the deployment of the Common European Data Space, including both interoperability within individual data space instances (i.e. intra data space interoperability) and interoperability between multiple data space instances (i.e. inter data space interoperability) and encompassing both the legal and technical aspects as depicted in Figure 3.



Offer a technical solution (smart middleware Simpl)

Bring stakeholders together with a common EU data policy, promote use of data space guidelines

Data Governance Act

Increase trust in data sharing (neutral data intermediaries, i.e., the orchestrators of the data spaces)

Data Spaces Support Centre

EU project to
- coordinate data space initiatives
- Identify common requirements
- Support the work of the EDIB
- Support data space initiatives and knowledge exchange

European Data Innovation Board (EDIB)

Support the Commission in:
- Issuing guidelines to facilitate the development of the common European data spaces
- Identifying the relevant standards and interoperability requirements for cross-sector data sharing

Funding for sectoral data spaces

EU financial contribution (notably DIGITAL) to deploy common European data spaces in strategic sectors/domains e.g. mobility, energy, manufacturing, tourism Green Deal & smart communities

Data Act

Unlock the potential of the EU’s industrial data (IoT data), ensure fairness in the allocation of data value among the actors of the data economy

Figure 3: The EC’s role in supporting the creation and deployment of data spaces [24].

The main initiatives as depicted in the figure include:

- The sectoral data spaces, encompassing both the preparatory *European Mobility Data Space Collaboration and Support Activity (*PrepDSpace4Mobility or EMDS CSA) and its follow-up EMDS deployment initiative, expected to start in October 2023.
- The *Data Spaces Support Centre program* [10] aimed to facilitate common data spaces that collectively create an interoperable data sharing environment in Europe, executing from October 2022 until March 2026.
- The *EU SIMPL procurement initiative* [25][26] aimed at procuring the open-source development of the smart middleware building blocks that will enable cloud-to-edge federations and support all major data initiatives funded by the European Commission, such as the Common European Data Space.
- The *European Data Innovation Board (EDIB) initiative* [27] advises the EC with regards to the practical implementation of amongst others the Data Act, the Data Governance Act and the Data Services Act. The scope of the EDIB includes data intermediation, data altruism and the use of public data that cannot be made available as open data, as well as on the prioritization of cross-sectoral interoperability standards. The EDIB will propose guidelines for the Common European Data Space. In practice, the EDIB will set guidelines for the DSSC through its advising role to the EC. The EC will remain the ultimate decision making authority.

3 Data space connectors

A data space connector (sometimes also referred to as a '*security gateway*') is a key data space component within data space architectures and, as such, also in realizing the overarching goal of a Common European Data Space as expressed in the EU Data Strategy. It connects an organization to the data space infrastructure.

The following sections in this chapter describe the functionality of a data space connector, identify various data space connectors and consider the data space connectors in view of their suitability for the BDI.

3.1 Data space connectors: functionality

The paragraphs in this section subsequently address the functionality of a data space connector and its relevance for interoperability and a converged and aligned data space approach.

3.1.1 Role in data spaces

A data space connector provides the interconnection between an organization and a data space. The main functionality of a data space connector includes [28][29]:

- it knows about the ICT assets a company / organization wants to share and under what conditions (usage policies),
- it handles contract negotiations and stores contract agreements,
- it facilitates the transfer of data,
- it offers an API to the internal IT-backend of a connected organization (which may be connector-specific and implemented by means of a '*data app*'), and
- it talks to the data space using well defined protocols.

Figure 4 depicts these main functionalities of a data space connector.

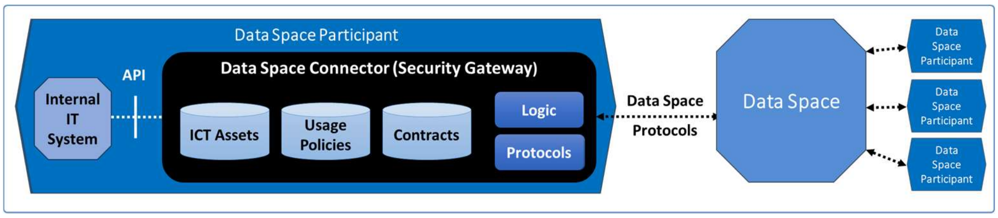


Figure 4: Data space connector: high-level functionality [28][29].

As the figure shows, data space connectors can be associated with data apps. Data apps can be used by a data space connector for connecting to the back-end systems of data space participants (through a well-defined '*data exchange API*') and to perform specific data processing or transformation tasks. They can perform tasks of different complexity, ranging from simple data transformation to complex data analytics.

3.1.2 Relevance for interoperability and convergence

Many EU initiatives on federative data sharing and data spaces have been / are being undertaken. This holds for both development of reference architectures and for sectoral deployments. It is clear that a fragmented approach may be contra-productive with respect to the EU Data Strategy of a Common European Data Space and convergence is to be preferred. The data space connector is pivotal and a key element for convergence at the technological level and, as such, for realizing the EU Data Strategy.

For the logistics sector convergence and a common approach (and as such the choice for an agreed upon data space connector) are essential as:

- Various types of data sharing are (and will increasingly become) of interest to the logistics sector, in addition to event driven data sharing as addressed in this report, for which a common and generic data sharing infrastructure will provide major advantages in both efficiency and effectivity.
- Logistics is cross-border and cross-sector by nature, requiring both interoperability between geographical logistics data space initiatives (e.g. cross-border) and requiring interoperability with other sectoral data space initiatives (i.e. cross-sector, e.g. with personal mobility, tourism, smart industry, ….).

The functions that an aligned definition of / choice for a data space connector should address have been enumerated in paragraph 3.1.1.

3.2 Data space connectors: identification

Multiple reference architecture initiatives have emerged over the last decade pursuing a similar goal on federative data sharing and data space. Hence, also multiple (types of) data space connectors have been developed. These include:

- The IDSA's Reference Architecture Model for data spaces (IDSA RAM [14]). Its IDS-connector uses standardized IDS protocols for data sharing, based on the IDS Information Model (a RDFS/OWL-ontology for describing ICT-resources such as data sets, data apps and data sharing policies). An overview of available IDS connectors and their usage in various data space initiatives has been provided by the IDSA [28]. The FIWARE TRUE (TRUsted Engineering) Connector [30] and the TNO Security Gateway (TSG) [31] are specific instances of the IDS-connector. Also the FENIX connector (see below) adheres to the IDS approach.
- Within the Gaia-X initiative, there is no concept of a connector. Nevertheless, it builds upon the so called Trust Services as part of the Gaia-X Federation Services [32]. Its Trust Services perform similar capabilities as provided by a data space connector. The most relevant is the Policy Decision Engine of Gaia-X that matches the policy enforcement framework as used within IDS.
- In the Coherence Architecture for Data Spaces [23] as developed by the Data Space Business Alliance (DSBA) initiative [22] a connector has a prominent role to fulfil, referring to the functions of the IDS-connector to be incorporated. In the DSBA, the IDSA, Gaia-X, the Big Data Value Association (BDVA) and the FIWARE Foundation cooperate on an aligned and coherent architecture for data spaces.
- The iSHARE initiative [20] provides a trust framework capability for data spaces [21]. It includes capabilities for legal agreements between participants in a data space, for transaction specific data sharing agreements and for data sovereignty management. ISHARE has its origins for B2B data sharing in the logistics sector [33]. It has potential to be broader applicable as trust framework, both for other sectors, application areas and various types of data sharing. Moreover, it provide functions for data sharing both within a specific data space and between multiple data spaces. The software component to connect an organization to iSHARE is sometimes referred to as an iSHARE-connector. Its scope is mainly on the trust

framework capabilities. It has limited capabilities for metadata discovery, transfer of data and semantics. Nevertheless, iSHARE can be used as trust framework in conjunction with (the connectors of) other data space initiatives [7].

- Currently, the Eclipse Dataspace Components (EDC) attracts major attention in various major and leading data space initiatives in Europe, as will be described in paragraph 3.3.3. The EDC adopts the architectural approach of the control plane and the data plane [34], in which the control plane handles the metadata interactions between connectors and the data plane handles the actual transfer of shared data. As such, no (potentially sensitive) primary data is shared between the EDC connectors, only the associated metadata. This architectural approach and the EDC are separately addressed in section 3.3.2.2 and in section 3.3.2.4, respectively.
- *The EU SIMPL procurement initiative* (as described in section 2.3 [25]) is aimed at procuring the open-source development of the smart middleware building blocks that will enable cloud-to-edge federations and support all major data initiatives funded by the European Commission, such as the Common European Data Space (as part of the EU Data Strategy). A data space connector has (preliminary) been identified to be part of the SIMPL architecture as described in its preparatory work [26]. It is to be expected that is definition will be in accordance with the developments of the reference architecture as jointly collaboratively pursued by the IDSA, GAIA-X and DSBA initiatives (as described in section 2.2) in combination with the emerging Dataspace Protocol (as described in paragraph 3.3.2.3). Based on the inputs of these reference architectures initiatives, the DSSC blueprint (as described in in section 2.2).
- The eDelivery e-SENSE building block [35] is part of the EU Connecting Europe Facility (CEF) suit of building blocks supported by EU DG Digit. It is a generic building block as it has been developed to establish a common transport infrastructure suited to the requirements of cross-border communication between eGovernment applications in different domains and for business to government. It is based on AS4 Access Points (‘connectors’) and the underlying AS4 messaging protocol, an OASIS standard [36]. It supports options for accessing metadata in service registries. The e-SENSE building block are mandatory unless there are reasons not to use them (comply or explain). For the PEPPOL procurement network for e-invoicing, the support of eDelivery e-SENSE is mandatory [37].
- The new European Interoperability Framework (EIF) [13] provides a set of extensive guidelines for developing interoperable digital infrastructures. It distinguishes four interoperability levels (technical, semantic, organizational and legal) under an overarching integrated governance approach. The associated European Interoperability Reference Architecture (EIRA) [38] provides a generic architecture, comprising a set of principles and guidelines. The EIRA is derived from the EIF. Its architectural elaboration defines a set for Architectural Building Blocks (ABBs) to build interoperable e-Government systems, including capabilities such as can be supported by connector implementations. However,

[7] As stated in a recent assessment of the iSHARE initiative [60], the main European initiatives on federative data sharing and data spaces (IDSA, GAIA-X, DSBA, DSSC….) are evolving to ever more distributed architectures, also in providing trust framework capabilities. It is to be expected that iSHARE will further develop its capabilities in alignment with these reference architectures and evolve to support these features accordingly.

providing (reference) implementations thereof is beyond the scope of the work of the EIF and the EIRA

- The FENIX Connector is developed as part of the CEF FENIX Action [39], which is based on the work and the recommendations of the DTLF. Its aim is to interconnect the different digital platform and harmonize their services and enable interoperability. FENIX builds upon the IDSA architecture, with the FENIX connector being an implementation of the IDS-connector.
- The Solid (Social Linked Data) project develops a platform for linked-data applications that are completely decentralized and fully under users' control [40]. Solid provides capabilities for identity, authentication, and authorization, metadata brokering and connectivity. Solid is based on RDF and Semantic Web technologies. Users store their data in an online storage space is referred to as a Personal Online Datastore (POD), which could as such be referred to as the SOLID Connector.
- The Context Broker (CEF [41] or FIWARE [42]) is part of a suite of components (developed by the FIWARE Community) for enabling data sharing, The scope of the Context Broker is on meta data brokering capabilities and it provides the NGSI (Next Generation Service Interface) API [43] enabling applications to provide updates and get access to context information. The Context Broker can be part of the broader set of capabilities as to be provided by a connector.

It is to be noted that this overview distinguishes the various types of data space connectors stemming from the various EU reference architecture development initiatives. For the various types of data space connectors, multiple instances may have been developed, each adhering to the basic standards as specified by the associated reference architecture initiative, but possible being extended with value adding capabilities or tailored to the specifics of a sector or application area. For example, the IDS-connector is a type of data space connector for which a multitude of instances have been developed, which may be open-source available, as listed in [28].

3.3 Criteria

The data space connectors as described in the previous section each build upon a similar ambition of federative data sharing as also pursued by the EU Data Strategy. As such, they each have functions to contribute to a federative decentralized data sharing infrastructure, providing data sovereignty to the entitled parties and using a secure and modular architecture.

The suitability of the various types of data space connectors in view of the BDI and in the context of the ambition as expressed in the EU Data Strategy as a Common European Data Space is considered in the following paragraphs of this section from various perspectives, i.e.:

- supporting the (short and longer term) BDI requirements,
- choosing for a solution or a strategic direction, and
- aligning with adjacent data sharing initiatives.

3.3.1 Supporting the (short and longer term) BDI requirements

The key requirements on the BDI have been defined in [5]. For the the various types of data space connectors, both the functional fit and the development status are to be considered.

3.3.1.1 Functional fit

The functional fit of a data space connector to support the key requirements on the BDI [5] strongly depends on the level at which the BDI functions will be implemented as part of the data space connector. For instance, should the functions for Identification and Authentication of participants, for Authorization of participants and for Findability of resources be part of the data space and provided as generic capabilities by the data space connector or should they be (remain) part of the BDI as value adding service.

The first option for applying the data space connectors and the connectivity protocols must be applicable for the bilateral transfer of data over the connection between the data receivers and the data providers to retrieve the data at the source, i.e. the 'data retrieval' activity within the main scope of this report as described in section 1.3.

However, additional benefits in terms of efficiency, interoperability and a single point of access for data providers may be gained when the alignment of the BDI and the data space approach goes beyond this basic connectivity, e.g. by considering:

- the option to integrate the functions for identification and authentication of participants in the BDI and the data space,
- the option to integrate the functions for authorization of data transfer transactions in the BDI and the data space, and
- the option to extend the functions of the metadata brokers in the data space architectures with the functions for the BDI Service Registry.

These options address a complex topic which needs an in-depth analysis, which is clearly beyond the scope of this report.

Additional functional fit aspects for a data space connector are its extensibility and flexibility in supporting multiple and additional connectivity protocols and in being able to migrate and evolve towards (compliance with) the upcoming SIMPL Connector as part of the EC's deployment approach as described in section 2.3.

3.3.1.2 Development status

For being used in (further developed and tailored for) BDI, a data space connectors should have a sufficient maturity level. This includes that it is well-documented, there is support available, there is an adequate User Interface (UI) available for both developers and administrators and that it should be at a technology readiness level of at least 5 (i.e. the technology is validated in a relevant environment).

3.3.2 Choosing for a solution or a strategic direction

Considering the overview of data space connectors as described in section 3.2, a strategic consideration for selecting a data space connectors has to be made. The criteria for the strategic considerations are addressed in the following subparagraphs.

3.3.2.1 Strategic choice: adopt and adapt the EC deployment approach

The strategic direction and the associated development and deployment initiatives taken by the EC in its ambition of a Common European Data Space have been described in chapter 2. As described, its building blocks will be defined and specified as part of the DSSC blueprint and will be open-source developed by the EU SIMPL procurement initiative. They will be deployed by a multitude of sectoral data spaces, including the preparatory European Mobility Data Space Collaboration and Support Activity (PrepDSpace4Mobility or EMDS CSA) and its follow-up deployment initiative.

This process of development and deployment will be governed by the overarching European Data Innovation Board (EDIB).

However, the DSSC blueprint is still in development and (therefore) also the building blocks to be developed by the SIMPL project are not fully specified yet. Hence, it will be clear that it is not possible yet to develop a compliant data space connector. Nevertheless, it is to be expected that the DSSC blueprint and the SIMPL project will build upon the ongoing technical developments for (interoperability of) data space connectors as are described in the following subparagraphs.

With these EC approach on the development and deployment of data spaces in mind, a main criterion in currently selecting a data space connector is on whether to choose for a specific data space connector solution that suits the current requirements for the BDI or to adopt an evolution strategy according to the EC development and deployment approach for the Common European Data Space and take care that the fulfilment of the BDI requirements are aligned with that or that they even will be included as part of the EC development and deployment approach.

3.3.2.2 Separation between control plane and data plane

Some of the data space connectors as listed in the previous section adhere to a specific protocol and/or semantic model that has to be implemented to be compliant with the specifications of the associated reference architecture. For example, IDS-connectors have to adhere to the IDSA specifications to be compliant. In this case, that holds for both the exchange of metadata being intertwined with the connectivity protocol for sharing of the primary data itself (referred to as 'in-band' control).

Currently however, a different architectural approach is also being developed and adopted. It is based on the basic architectural principle of separation of control plane and data plane. This development allows for a strategic consideration on the extent to which you must choose a specific type of data space connector (as described in section 3.2) or a data space connector framework approach allowing for more flexibility in including multiple connectivity protocols and variations in data space internal control processes.

The separation between the control plane and the data plane is depicted in Figure 5. It is also referred to as ' out-band' control for federative data sharing.

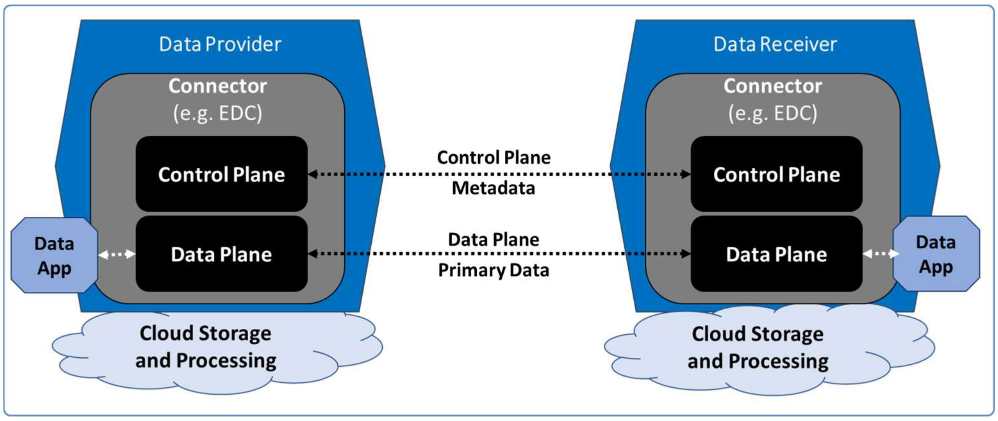


Figure 5: Out-band control for federative data sharing by means of separation of the control plane (for metadata exchange) from the data plane (for primary data transfer).

The *control plane* handles the discovery of the ICT assets offered by connectors and the associated policies. It also handles the contract negotiations. For this, it exchanges metadata with the control plane of other data space connectors.

The *data plane* handles the actual transfer of the shared data with the data plane of other data space connectors. This is referred to as the primary data and can be potentially sensitive data.

It is to be noted that this out-band control is different from the approach as originally taken by the IDS-connector in which the exchange of control information (metadata) is part of the data sharing protocol also containing the primary data to be transferred. This is also referred to as 'in-band control'. For the IDS-connector and its associated IDS-protocol and IDSCP protocol, this is depicted in Figure 6.

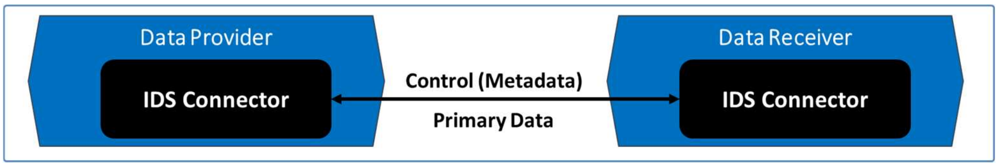


Figure 6: The IDS-connector with in-band control by means of the IDSCP protocol.

The advantages of using an out-band control mechanism with separation of the control plane and the data plane as depicted in Figure 5 as compared to an in-band control mechanism as depicted in Figure 6 are:

- It gives more flexibility in allowing multiple connectivity protocols at the data plane can simultaneously be enabled, e.g.:
  - to support multiple types of data sharing, e.g. for data streaming,
  - to serve different connectivity needs within a single data space, e.g. different for control metadata exchange from the primary data transfer,

  Whilst this on the one hand may lead to new interoperability challenges as it allows for differentiation in choices of connectivity protocols to be supported, it is on the other hand expected that only a limited set of connectivity protocols are needed and will be adopted to serve the majority of the connectivity needs to support the various types of data sharing. These will include the HTTP, MQTT and Kafka protocols (as will be addressed in chapter 4). Also the (Amazon) Simple Storage Service S3 may be expected to be included, providing object storage for Internet applications, backups, disaster recovery, data archives, data lakes for analytics, and hybrid cloud applications.
- It allows for a flexible and gradual evolution trajectory,

3.3.2.3 Interoperability: the Dataspace Protocol

Sharing data between autonomous entities (participants, data space connectors) requires the provision of metadata to facilitate the transfer of assets by making use of a data transfer protocol. The emerging Dataspace Protocol [33] defines how this metadata is provisioned. It is a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate usage agreements and access data as part of a federative data sharing architecture or data space, see Figure 7.

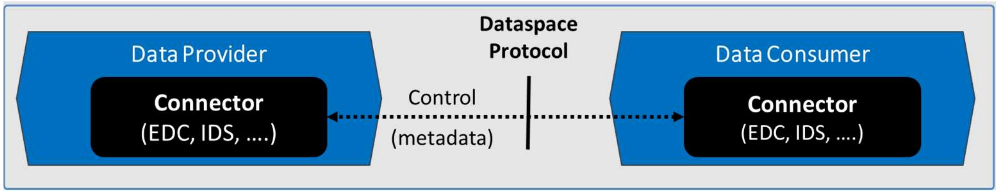


Figure 7: The Dataspace Protocol defining the control interface (metadata) between data space instances.

The Dataspace Protocols define how data assets are deployed (as DCAT Catalogs), how usage control is expressed (as ODRL Policies), how contract agreements that govern data usage are syntactically expressed and electronically negotiated and how data assets are accessed using data transfer protocols.

The Dataspace Protocol specification does not cover the data transfer process itself. While the data transfer is controlled by the Transfer Process Protocol, the data transfer itself (and especially the handling of technical exceptions) is an obligation to the Transport Protocol that will be used.

The fact that the Dataspace Protocol specifications address the processes of metadata exchange to enable data sharing but not the data transfer itself corresponds to the basic design assumption of separating the control plane (with metadata exchange to enable data sharing) from the data-plane (with the actual transfer of the (potentially sensitive) primary data.

3.3.2.4 The EDC connector

Currently, the Eclipse Dataspace Components (EDC) attracts major attention for implementing the data space connector according to the separation of the control plane and the data plane (as described in subparagraph 3.3.2.2) and for enabling the Dataspace Protocol for interoperability (as described in subparagraph 3.3.2.3).

However, it is to be realized that the EDC is more a software framework for developing data space connectors and less specifying (the architecture and protocols of the) data space connector itself. As such, the EDC leaves open several design choices still to be made on the protocol and data space connector level. This implies that adopting the EDC doesn’t automatically imply interoperability with other data spaces that adopt the EDC.

Moreover, it is to be realized that the EDC does not yet meet all the requirements of the BDI (yet). Adopting the EDC will require an in-depth assessment on including the BDI requirements.

The EDC is supported by major organization and companies (such as Amadeus, BMW, Fraunhofer, Microsoft T-Systems, ….) and already being used in several major European data space initiatives as will be described in the following section.

3.3.3 Aligning with adjacent data sharing initiatives

The importance of the choice of a data space connector for convergence of the various data sharing initiatives and the ambition of the EU Data Strategy of a Common European Data Space has been described in section 2.1. The following subparagraphs respectively address the adjacent EU and Dutch data sharing initiatives that should be taken into account when selecting a data space connector strategy for BDI.

3.3.3.1 Data space connectors adopted by leading data space initiatives

Table 1 provides an non-exhaustive overview of the main (adjacent) data space initiatives and their current selection for a data space connector type.

Table 1: Data space initiatives and their current selection for a data space connector type

Initiative	Type of Data Space Connector
German Mobility Data Space	The German Mobility Data Space is an operational data space originating from Germany, Its main focus is currently personal mobility. The German Mobility Data Space uses the EDC [44]
European Mobility Data Space	The European Mobility Data Space (EMDS) will be developed as part of the EU EMDS Deployment project, expected to start at the end of 2023. The choice and definition of the required data space connector is expected to be based on the input from (1) the current European Mobility Data Space Collaboration and Support Activity (EMDS CSA, or PrepDSpace4Mobility) [24] and (2) the DSSC blueprint. For bot, the architecture and specifications have not been provided (yet).
Smart Connected Supplier Network	The Smart Connected Supplier Network (SCSN) has been operational as data space for the high-tech manufacturing sector in the Netherlands since several years [45]. SCSN is based on the IDS architecture and, as such, uses the IDS-Connector. Currently there are no plans (yet) to migrate to EDC. The emerging Dataspace Protocol (see also paragraph 3.3.2.3) is foreseen to be used for interoperability with other data spaces.
Catena-X	Catena-X has recently been operationally launched as data space for the automotive industry. Catena-X uses the EDC [46] and foresees the use of the Dataspace Protocol (see also paragraph 3.3.2.3 for interoperability with other data spaces).
EONA-X	EONA-X is a data space for mobility, transport and tourism [47]. It is based on the GAIA-X reference architecture and it uses the EDC connector.
SIMPL	In the SIMPL architecture vision [26] as used for input to the EU SMPL procurement call, the need for a data space connector has been identified (referred to as a 'data store connector'). Its architecture and specifications are not provided. For that, it is expected that the SIMPL data space connector building block will be developed on the basis of the DSSC blueprint.
DSGO	The DSGO (Digitaal Stelsel Gebouwde Omgeving) aiming at a set of uniform agreements that ensure safe, reliable and controlled access to data in the construction / building sector [48]. DSGO has selected iSHARE for developing the trust framework.
DVU	The DVU (Datastelsel Verduurzaming Utiliteit) allowing companies and organizations to share their energy and building data more easily and more securely as key enabler for sustainability [49]. DVU has selected iSHARE for developing the trust framework.

3.3.3.2 Alignment with adjacent Dutch data sharing initiatives

Closely related to the NGF DIL addressing the topic of data sharing for logistics, several adjacent Dutch NGF's are running that may require an aligned and agreed upon strategy for using connectivity protocols and data space connectors. From the MinI&W perspective these NGF's include:

- the NGF Dutch Metropolitan Innovations (DMI) addressing the topic of data sharing for personal mobility, and
- the NGF Digital Infrastructure for Future-Proof Mobility (DITM - Digitale Infrastructuur voor Toekomstbestendige Mobiliteit) addressing the topic of data sharing for the roadside e.g. to support Cooperative, Connected and Automated Mobility (CCAM).

Reasons to align the choice for a specific data space connector with these adjacent Dutch data sharing initiatives include:

- participants of the various data spaces being able to access each other's data services with minimal integration efforts and through a single point of connection, i.e. without having to subscribe to multiple data spaces with potentially varying identification, authentication and authorization protocols,
- data providers and data receivers being able to support multiple types of data sharing without having to implement a separate data space connectors tailored for of the specific type of data sharing, and
- efficiency and effectiveness in jointly developing, deploying and operating aligned and interoperable data space instances across multiple and adjacent sectors or application areas.

At the time of writing of this report, it is not clear yet whether a specific data space connector choice has been made (and if so, which) by these adjacent Dutch data sharing initiatives.

3.4 Considerations and recommendations

Based on the observations in the previous sections, several considerations can be made with respect to a data space connector to support the BDI in view of the emerging Common European Data Space.

From the data space connectors as described in section 3.2, there is not a specific data space connector that currently is a perfect match with the requirements of the BDI for each of the parts of the BDI connectivity architecture (as described in section 1.2 and depicted in Figure 1) and can therefore be used 'as is'. A specific data space connector solution might serve the connectivity needs for a specific part of the BDI connectivity architecture. However, multiple and differing data space connector solutions for various parts of the BDI architecture should not be aimed at as coherence in deploying data space connectors across the BDI architecture will enable improved exploitation of the potential functional benefits a data space connector may offer (as listed in paragraph 3.1.1), will contribute to operational efficiency and may prevent minimization of future integration and migration efforts.

The development towards a data space connector that may coherently be deployed across the overarching BDI architecture should be the goal of the EU initiatives supporting the deployment of the Common European Data Space as described in section 2.3. Therefore, instead of currently selecting various data space connector solution for the various connectivity parts in the BDI architecture it is recommended to define for the BDI an evolutionary approach for developing and deploying a data space connector approach that (where necessary and possible) aligns with the EC's approach in developing and deploying it in the context of the Common European Data Space. This evolutionary approach should include a strategy to align with and contribute to the DSSC blueprint for federative data sharing and data space building blocks and to the open-source development thereof in the SIMPL initiative. Currently (i.e. medio 2023) the DSSC Expert Groups are starting to develop the blueprint specifications based on the requirements provided by a broad variety of sectoral Data Space Collaboration and Support Activities (CSAs), including the European Mobility Data Space CSA which also encompasses logistics. Therefore, it is recommended to include the specific requirements of the BDI as input for the EMDS CSA projects, and monitor and / or contribute that the BDI requirements are adequately taken into account by the DSSC Expert Groups.

Awaiting the results of the DSSC blueprint and the SIMPL open-source building blocks, it may be anticipated that they will build and extend upon the reference architectures for federative data sharing and data spaces as described in section 2.2, technically converging on the developments for data space connectors as described in subparagraph 3.3.2.2 (i.e. separation of control plane and data plane) and in subparagraph 3.3.2.3 (i.e. interoperability as specified in the emerging Dataspace Protocol).

For the practical development and implementation of these concepts, the Eclipse Dataspace Connector (EDC connector) as described in subparagraph 3.3.2.4 is currently paving the way. As part of this risk mitigation strategy it is therefore recommended for the NGF DIL to get familiarized with the approach and concepts of the EDC framework for data space connectors, including its architectural approach for the separation of the control plane and data plane and interoperability as defined by the emerging Dataspace Protocol. Both the applicability thereof for the connectivity part for the request / reply 'data retrieval' activity and for the publish / subscribe 'data distribution' activity (see section 1.2, Figure 1) should be included. It is to be realized that adopting the EDC by different data spaces does not automatically mean interoperability between these data spaces. However, it will provide the flexibility to develop and migrate to a common approach interoperable across data spaces.

In view of the broad overarching scope of architecture of the BDI, both in the alignment with the EU DSSC and SIMPL initiatives and in the development of the EDC, a step-wise approach may be considered in aligning (integrating) the various capabilities required to support the BDI architecture into the data space connector architecture:

- The Identification and Authentication capabilities and the capability for Authorization (sometimes jointly referred to as IAA). Re-using the IAA capabilities of the data space connector over various data spaces (including the BDI) may prevent data providers and other participants from having to separately register multiple times in different data spaces, e.g. for different types of data sharing. This 'harmonization' of the IAA capabilities may prevent data space participants from having multiple implementations of similar IAA capabilities whilst enabling interoperability with adjacent data space initiatives.
- The meta-data brokering capabilities of the data space connector to provide the Service Registry and the Index functions of the BDI and the semantic management and flow control functions that they provide. These capabilities

can be considered as ‘core’ to the BDI architecture. By including the Service Registry and the Index functions in the meta-data brokering capabilities of the data space connector allows them to be more easily available for and across various data spaces.

To enable such a step-wise approach, a functional break-down analysis of the Service Registry and the Index functions may provide additional insight on:

- how its individual functions can be taken into account by the related DSSC Expert Groups, and
- what protocols are needed to be able to implement them in an interoperable distributed manner reflecting the distributed FEDeRATED nodes approach as described in section 1.2 as input for the further development of the Dataspace Protocol.

Additional topics to be taken into account to support the BDI requirements could / should be to support the functions that enable the deployment of data apps and OpenAPI interfaces within the (security) domain of data space participants (e.g. through the roles and functions similar to the app store and the IDS-connector as part of the IDSA Reference Architecture Model [14]) and the support for usage control mechanisms to enforce data sovereignty.

4 Connectivity protocols

A connectivity protocol is a system of rules that allows IT-systems to exchange data. The term ‘connectivity protocol’ is overarching as it may contain aspects of both communications, messaging and security as will be described in this chapter.

In this chapter, connectivity protocols are considered that may be used for the BDI.

4.1 Connectivity protocols: functionality

As described in the sections 1.2, 1.3 and depicted in Figure 1, the main parts where connectivity protocols are to be considered in the FEDeRATED architecture are:

- for the ‘data distribution’ activity of links to (the FEDeRATED node of) all relevant data receivers, and
- for the ‘data retrieval’ activity to retrieve (potentially sensitive) data at the source, i.e. at the data provider.

There can and will be many / multiple types of (meta-)data sharing interactions as part of the workflows for both the ‘data distribution’ activity and the ‘data retrieval’ activity, Moreover, each can have its own specific needs for and requirements on the connectivity protocols. Therefore, they will not be individually addressed. Instead, a generic approach will be described.

The term ‘connectivity protocol’ is overarching It may contain aspects of both communications, messaging and security. Moreover, it may encompass functions from multiple layers of the well-known, traditional, 7-layer OSI model [50], i.e. from the transport layer, the session layer and the presentation layer. As such, functions they may be distinctive between the various connectivity protocols may be more generically referred to as the ‘*routing functions’* and *the ‘context functions’.*

The ‘*routing functions’* allow two or more IT-system to exchange data defining the rules, syntax, semantics, and synchronization of communication and possible error recovery methods. The routing functions are payload agnostic. Distinguishing features of the routing functions include:

- *Synchronous or asynchronous communication:* In synchronous communication between IT-systems, the initiating system sends a message to a receiving system and waits for the response to arrive within some expected timespan. In asynchronous communication, the initiating system sends a message and continues with its other tasks not waiting for a reply.
- *Uni-directional or bi-directional communication:* Uni-directional communication refers to a one-way data transfer, where information flows in only one direction. This means that data can only be sent or received, but not both. On the other hand, bi-directional communication refers to a two-way data transfer, where information can flow in both directions. This means that data can be sent and received simultaneously.
- *Messaging pattern:* For the messaging patterns, a distinction can be made between the request / reply messaging pattern and he publish / subscribe messaging pattern.

  The request / reply messaging pattern is a message exchange pattern in which a requestor sends a request message to a replier system, which receives and processes the request, ultimately returning a message in response. For simplicity, this pattern is typically implemented in a purely synchronous fashion (e.g. over HTTP) which holds a connection open and waits until the response is delivered or the timeout period expires. However, request–response may also be implemented asynchronously with a response being returned at some unknown later time [51].

The publish / subscribe messaging pattern can be used when senders of messages (the 'publishers') do not program the messages to be sent directly to specific receivers (the subscribers'), but instead categorize published messages into classes without knowledge of whether and which subscribers there may be. Subscribers express interest in classes and only receive messages that are of interest without knowledge of which publishers, The main representatives of the publish / subscribe messaging protocols are AMQP [52], MQTT [53] and Kafka [54].

The *'context functions'* including additional information on the type of data being exchanged, to be used by the applications for further processing.

The (positioning) of the routing and context functions is depicted in Figure 8.

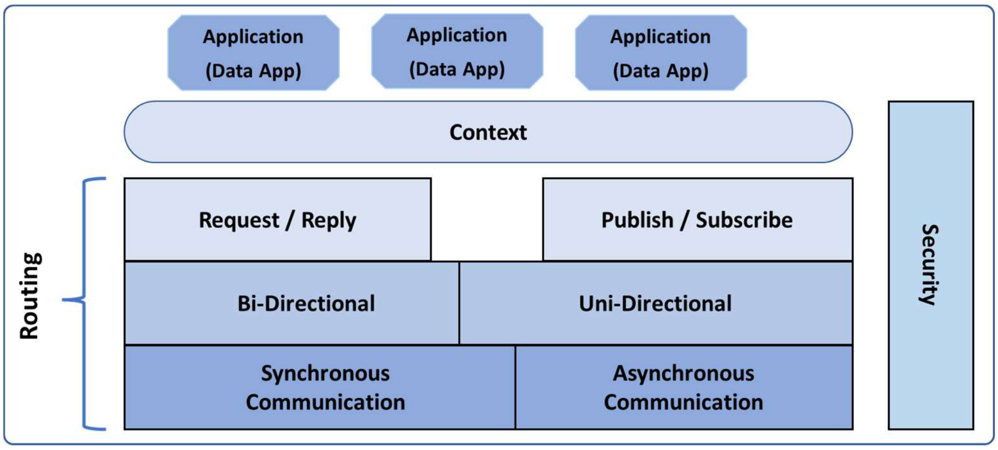


Figure 8: High-level positioning of the routing (with the various distinguishing features) and the context functions.

In addition, as the figure shows, security protocols may apply across the (various features of) the routing and context functions.

4.2 Connectivity protocols: identification

This section identifies the main connectivity protocols to be considered for the BDI, without the goal to be exhaustive.

It is to be noted that the mapping of the various protocols on the (various features of the) routing functions and the context functions as depicted in Figure 8 is not unambiguously. The protocols may have capabilities that span over multiple of these functions, as also reflected in the mapping on the connectivity protocols on the routing and the context functions as depicted in Figure 9.

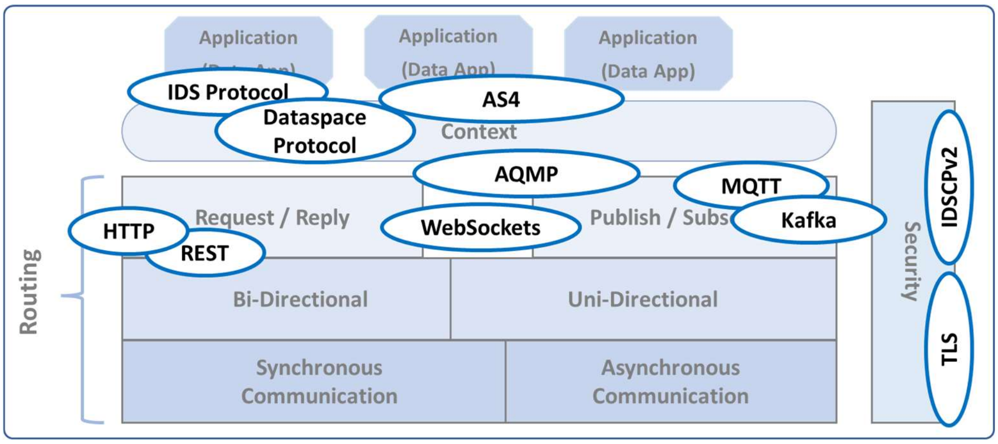


Figure 9: Mapping the connectivity protocols on the routing and the context functions.

In the listing of the connectivity protocols, an ordering from 'left-to-right' according to the figure is used.

- *HyperText Transfer Protocol (HTTP)* is a communication protocol for computer networks. HTTP is a bi-directional communication protocol for short-living connections to support request / reply messaging patterns.

  HyperText Transfer Protocol Secure (HTTPs) is an extension of the Hypertext Transfer Protocol (HTTP). It uses encryption for secure communication using TLS (or, formerly, SSL).
- *REpresentational State Transfer (REST)* is a (widely accepted) so set of guidelines for creating stateless, reliable web APIs. A web API that obeys the REST constraints is informally described as RESTful. RESTful web APIs are loosely based on HTTP methods to access resources via URL-encoded parameters and the use of JSON or XML to transmit data.
- The *IDS Protocol* is a messaging protocol developed as part of the International Data Spaces (IDS) initiative. In the evolution and alignment of the various reference architecture initiatives for federative data sharing and data spaces (as described in section 1.3), it is the expectation that the IDS protocol will soon become deprecated and superseded by the emerging Dataspace Protocol.
- The *Dataspace Protocol* [33] defines how this metadata is provisioned. It is a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate usage agreements, and access data as part of a federation of technical systems termed a data space. In view of its expected importance, the Dataspace Protocol has already been more extensively elaborated in subparagraph 3.3.2.3.
- *WebSockets* is a bidirectional protocol. A WebSocket connection lasts as long as any of the participating parties lays it off and the connection breaks automatically. WebSockets uses HTTP to initiate the connection.
- *Applicability Statement (AS4)* is an open standard for the secure and payload-agnostic exchange of Business-to-business documents using Web services. AS4 is a Conformance Profile of the OASIS eBMS specification [55]. The AS4 protocol has advanced security capabilities and the possibilities with 'pull' and 'push' notifications. It provides a

guarantee that sent messages will always be delivered and is based on the SOAP / XML standards.

- The *Advanced Message Queuing Protocol* (AMQP [52]) AMQP enables publish / subscribe message patterns with various types of message-delivery guarantees (such as at-most-once, at-least-once and exactly-once), together with authentication and/or encryption. It can support both point-to-point and publish / subscribe routing.
- The *Message Queuing Telemetry Transport Protocol* (MQTT [53]) is a publish / subscribe messaging protocol. It is 'lightweight' by design, to be used for connections with devices with resource constraints, e.g. as part of the Internet-of-Things (IoT). The MQTT protocol distinguishes between a message broker and a (number of) message clients.
- The *Kafka Protocol* [54] is a distributed event store and stream-processing platform for handling real-time data feeds with low latency. It is an open-source system developed by the Apache Software Foundation. It allows data providers to publish data to any number of systems or real-time applications and it allows data receivers to subscribe to these data streams.

In addition, Figure 9 depicts the security protocols in the ‘right’ part of the figure, i.e.:

- *Transport Layer Security (TLS*) is a cryptographic protocol that describes communication security for computer networks. TLS is an improved and more secure encryption protocol compared to SSL, which has recently been deprecated [56]. The most recent version of the TLS specification is defined in RFC 5246 [57].

  Mutual TLS (mTLS) is a type of authentication in which the two parties in a connection authenticate each other using the TLS protocol [58].

  Applying a (TLS) security protocol on the communication or messaging protocols generically leads to a ‘secure’ version thereof, e.g. HTTPS, Secure WebSockets, MQTTS,…
- The *IDS Communication Protocol version 2* (IDSCPv2) is a TLS -based protocol that establishes a bidirectional connection between connectors and allows to send any payloads [59]. It is developed to support the request / reply messaging pattern. It employs remote attestation to ensure integrity, authenticity and trustworthiness of the communication peers. It is used to send user data together with custom data usage policies and other arbitrary metadata.

  With the advent of the Dataspace Protocol [33] (as described above and elaborated in subparagraph 3.3.2.3), the expectance is that an updated protocol will be developed to support similar capabilities within the Dataspace Protocol architectural framework.

Furthermore, it is to be noted that the various messaging protocols can have (different) build in security features. For instance, as indicated in above, the AMQP provides options for message-delivery guarantees, which are different from the options as provided by the other protocols. Similarly, the AS4 protocol supports options for encryption at the message level.

4.3 Criteria

The considerations on the various connectivity protocols on suitability for the ‘data distribution’ activity and the ‘data retrieval’ activity in the FEDeRATED architecture (as described in section 1.2 and depicted in Figure 1) should take both qualitative and quantitative criteria into account.

The qualitative criteria include:

- the need for uni-directional or bi-directional connections,
- the need for short-living connections (e.g. to support request / reply interactions) or long-living connections (e.g. to support multiple, related, interactions),
- the required security level, including the need for remote attestation.

Furthermore, the outcome of the assessment on the connectivity protocols may depend on a performance analysis based on more quantitative dimensioning and scalability requirements. The scalability and dimensioning requirements determine to which extend the chosen connectivity protocol is able to efficiently and cost-effectively scale with respect to:

- the number of stakeholders being part of the data sharing infrastructure,
- the intensity with which the connectivity protocols are initiated, and
- the frequency of actual data sharing interactions.

For assessing the various connectivity protocols on these dimensioning and scalability requirements, reliable quantitative information is key. At the writing of this report, it was indicated that these numbers haven’t been specified yet for the development of the BDI.

Which connectivity protocol is most suitable may vary per part of the BDI environment to which it applies. Moreover, a functional breakdown of the Index and the Service Registry functions as core components of the BDI (as proposed in section 3.4) may give a more detailed view on the various connections and links in the BDI architecture and their associated requirements on connectivity protocols.

4.4 Considerations and recommendations

It is to be noted that (level of relevance of) an assessment of the connectivity protocols also is related to the considerations and the recommendations on the data space connector as described in chapter 3. More specific, a choice for the Eclipse Dataspace Connector (as proposed in section 3.4) provides flexibility in supporting various connectivity protocols in the data plane. So, the choice for the EDC gives extensibility and flexibility in updating connectivity and messaging protocols, under a common control plane architecture.

Furthermore interoperability is key in developing the BDI. Interoperability for data spaces is addressed by the emerging Dataspace Protocol as also has been described in subparagraph 3.3.2.3, in which the architecture and control for connectivity protocols and bindings are defined. Controlling and limiting the number of connectivity protocols to be supported improves manageability within and across data spaces.

5 In conclusion

It is expected that the role of the BDI as implementation for federative data sharing according to the architectural concepts as developed in the EU FEDeRATED project will become ever more related to and intertwined with the overarching EU ambition of a Common European Data Space (as expressed in the European Data Strategy) and, as such, also with the associated European reference architecture development initiatives and (cross-) sectoral deployment initiatives. Hence, as these initiatives develop data space connectors and connectivity protocols, this report has addressed the considerations on which data space connectors (and connectivity protocols) could / should be used for the BDI target architecture in view of the emerging Common European Data Space.

In this report, the data space connectors and connectivity protocols have been addressed in chapter 3 and in chapter 4, respectively. For the main considerations on each of these topics the reader is referred to the corresponding section 3.4 and section 4.4, respectively.

Main considerations are (1) to adopt the Eclipse Dataspace Connector (EDC) initiative (instead of selecting a specific solution for the data space connector) and (2) to provide input to current European Mobility Data Space Collaboration and Support Activity (EMDS CSA) and to align with the EU Data Spaces Support Centre (DSSC) initiative and the upcoming EU SIMPL procurement initiative to take care that the BDI requirements are adequately taken into account in the further development and deployment of the EU reference architectures for federative data sharing and data spaces.

These considerations may pose the NGF DIL with a challenge as their (longer term) timelines may not align DIL's short-term goals with respect to the BDI development. Hence, a strategy may be needed that minimizes the risks associated with migration and evolution in adopting the proposed data space connector approach. As part of this risk mitigation strategy it is recommended for the NGF DIL:

- to get actively involved (on the short term) in and influence the work on the EU DSSC blueprint and the SIMPL building blocks,
- to get familiarized with the approach and concepts of the EDC framework for data space connectors, including its architectural approach for the separation of the control plane and data plane and interoperability as defined by the emerging Dataspace Protocol,
- to assess how the approach of adopting the EDC and adhering to the EU DSSC blueprint and SIMPL initiatives is impacted by (and vice versa may / should impact) the existing regulations as applicable to logistics data sharing areas, e.g. on EFTi, EBSI, eDelivery and eIDAS (theses regulatory constraints have been out-of-scope for this report), and
- to highlight the associated risk upwards in the governance chain to make sure that changes down the line and potential additional efforts and costs will not come as a surprise.

In addition, it is noted that several adjacent Dutch National Growth Funds (NGFs) have started within the context of the MinI&W, especially the NGF Dutch Metropolitan Innovations (DMI) addressing the topic of data sharing for personal mobility and the NGF Digital Infrastructure for Future-Proof Mobility (DITM - Digitale Infrastructuur voor Toekomstbestendige Mobiliteit) addressing the topic of data sharing for the roadside e.g. to support Cooperative, Connected and Automated Mobility (CCAM). At the time of writing of this report, it is not clear (yet) whether these NGF projects have already defined their data space connector strategy. As these projects are adjacent to the DIL project and the development of the BDI, it is recommended to mutually align on the data space connector and connectivity protocol approaches.

6 References

[1] Dutch Ministry of Infrastructure and Environment. “Digitale Transport Strategie – Goederenvervoer”, December 2018, URL: https://www.tweedekamer.nl/kamerstukken/detail?id=2018Z22747&did=2018D57686.

[2] EU FEDeRATED project. “EU-project for digital cooperation”. URL: http://www.federatedplatforms.eu/.

[3] EU FEDeRATED project. "FEDeRATED Reference Data Sharing Architecture", Version Under Development, June 2022. URL: http://www.federatedplatforms.eu/index.php/library/item/draft-federated-reference-architecture-document-june-2022.

[4] European Commission. “A European strategy for data”, 2020, URL: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

[5] Topsector Logistics (2023). "Basic Data Infrastructure Framework - Key requirements". *Will be made available on-line on the short term*.

[6] European Commission (2022). “European Data Governance Act”. URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

[7] EU OPEN DEI project. “Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry”, URL: https://www.opendei.eu/.

[8] EU OPEN DEI project. “Design Principles for Data Spaces – Position Paper”, 2021, URL: https://design-principles-for-data-spaces.org/.

[9] Protium. “Overzicht Internationale Ontwikkelingen – Federatief Zakelijk Data Delen”. *Available on request*.

[10] EU Digital Europe Programme. “Data Spaces Support Centre (DSSC)”. URL: https://dssc.eu.

[11] Data Spaces Support Centre (DSSC, 2023). "DSSC Glossary". URL: https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf.

[12] N. Lindström, B. Nyström and J. Zdravkovic. "An Analysis of Enterprise Architecture for Federated Environments"; The Practice of Enterprise Modeling, Springer International Publishing, pp. 156-170, 2017

[13] European Union. “New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations”, 2017, URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[14] International Data Spaces Association (IDSA). “International Data Spaces: Reference Architecture Model Version 3”, 2019, URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.

[15] International Data Spaces Association (IDSA). ‘IDS-G on GitHub”. URL: https://github.com/International-Data-Spaces-Association/IDS-G.

[16] International Data Spaces Association (IDSA). ‘Overview on the IDS Repositories on GitHub”. URL: https://github.com/International-Data-Spaces-Association/idsa/blob/main/overview_repositories.md.

[17] EU GAIA-X Initiative. “A Federated and Secure Data Infrastructure”, URL: https://www.gaia-x.eu/.

[18] EU GAIA-X Initiative. “GAIA-X Federation Services - FXFS”, URL: https://www.gxfs.eu/specifications/.

[19] FIWARE. “Components”. URL: https://www.fiware.org/catalogue.

[20] iSHARE Foundation. “Trust & Foundation Governance”, URL: https://ishare.eu/ishare/the-foundation/governance/.

[21] ISHARE Foundation. “(Benefits) For Data Spaces”, URL: https://ishare.eu/ishare/benefits/for-data-spaces.

[22] Data Space Business Alliance (DSBA). “Unleashing the European Data Economy”, URL: https://data-spaces-business-alliance.eu.

[23] Data Space Business Alliance (DSBA). “Technical Convergence – Discussion Document”, URL: https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf.

[24] EU PrepDSpace4Mobility (European Mobility Data Space) Coordination and Support Action (EMDS CSA, PrepDSpace4Mobility). "First Public Stakeholder Forum". URL: https://mobilitydataspace-csa.eu/wp-content/uploads/2023/03/psf-28february.pdf.

[25] EU Digital Europe Programme. “SIMPL: cloud-to-edge federations and data spaces made simple”. URL: https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple.

[26] EU Digital Europe Programme. “SIMPL: Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform - Architecture Vision Document”. Version 4.00, March 2022. URL: https://ec.europa.eu/newsroom/dae/redirection/document/86241.

[27] EC -European Commission. "Data Governance Act explained". URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

[28] International Data Spaces Association (IDSA) (2022). “Data Connector Report”. URL: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/International-Data-Spaces-Data-Connector-Report-November-2022.pdf.

[29] NTT DATA (2022). "Dataspace Connector Survey Report - Overview of IDS-RAM and Eclipse Dataspace Connector". URL: https://www.nttdata.com/global/en/-/media/nttdataglobal/1_files/technology/dataspaceconnectorsurvery_sep2022.pdf.

[30] FIWARE FTC."FIWARE TRUE (TRUsted Engineering) Connector". URL: https://fiware-true-connector.readthedocs.io/en/latest.

[31] GitHub. "TNO Security Gateway - Architecture & Documentation". URL: https://tno-tsg.gitlab.io.

[32] EU Gaia-X Initiative. “Gaia-X Federation Services - GXFS”, URL: https://www.gxfs.eu/specifications.

[33] GitHub. "Dataspace Protocol - Version 0.8". URL: https://github.com/International-Data-Spaces-Association/ids-specification/tree/main.

[34] Eclipse Foundation. "Eclipse Dataspace Components". URL:https://projects.eclipse.org/projects/technology.edc.

[35] EU Digital Europe Programme. “eDelivery - Exchange documents and data securely and reliably “. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

[36] OASIS (2013). "AS4 Profile of ebMS 3.0 Version 1.0". URL: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf.

[37] EU Digital Europe Programme. “Support for the PEPPOL AS4 profile mandatory in the PEPPOL eDelivery Network from 1 February 2020". URL: https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/2019/02/19/Support+for+the+PEPPOL+AS4+profile+mandatory+in+the+PEPPOL+eDelivery+Network+from+1+February+2020.

[38] EC ISA2 Programme. "European Interoperability Reference Architecture (EIRA)". URL: https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira.

[39] FENIX Network. “A European FEderated Network of Information eXchange in LogistiX - To support the transition to seamless data sharing”. URL: https://fenix-network.eu.

[40] Wikipedia. "Solid (web decentralization project)". URL: https://en.wikipedia.org/wiki/Solid_(web_decentralization_project).

[41] EU CEF. "Context Broker Documentation". URL: https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=82773700.

[42] FIWARE Foundation. "FIWARE Components". URL: https://www.fiware.org/catalogue.

[43] GitHub. "FIWARE-NGSI v2 Specification". URL: https://fiware.github.io/specifications/ngsiv2/stable.

[44] Mobility Data Space (Germany). "Mobility Data Space: The data marketplace for the mobility sector". URL: https://mobility-dataspace.eu/solutions-features.

[45] Smart Connected Supplier Network (SCSN). “SCSN - Smart Connected Supplier Network”. URL: https://smart-connected.nl.

[46] Catena-X. "EDC - The Central Component". URL: https://catena-x.net/en/offers/edc-the-central-component.

[47] EONA-X. "EONA-X - Data space for Mobility, Transport and Tourism”. URL: https://eona-x.eu.

[48] Platform Duurzame Huisvesting. "Project Datastelsel Verduurzaming Utiliteit (DVU)". URL: https://www.platformduurzamehuisvesting.nl/projecten/datastelsel-verduurzaming-utiliteit.

[49] Nederland Digitaal. "Richtinggevende principes Digitaal Stelsel Gebouwde Omgeving (DSGO) vastgesteld". URL: https://www.nederlanddigitaal.nl/actueel/nieuws/2022/05/10/richtinggevende-principes-digitaal-stelsel-gebouwde-omgeving-vastgesteld.

[50] Wikipedia. "OSI-Model". URL: https://en.wikipedia.org/wiki/OSI_model.

[51] Wikipedia. "Request–response". URL: https://en.wikipedia.org/wiki/Request%E2%80%93response.

[52] OASIS. "AMQP (Advanced Message Queuing Protocol) Version 1.0". URL: http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf.

[53] OASIS. "MQTT (Message Queuing Telemetry Transport) Version 3.1.1". URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html.

[54] Apache. "Kafka Protocol Guide". URL: https://kafka.apache.org/protocol.html.

[55] OASIS. "AS4 Profile of ebMS 3.0 - Version 1.0". URL:http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf.

[56] Internet Engineering Task Force (IETF). "RFC 7568 - Deprecating Secure Sockets Layer Version 3.0". URL: https://datatracker.ietf.org/doc/html/rfc7568.txt.

[57] Internet Engineering Task Force (IETF). "RFC 5246 - The Transport Layer Security (TLS) Protocol - Version 1.2". URL: https://www.ietf.org/rfc/rfc5246.txt.

[58] Internet Engineering Task Force (IETF). "RFC 8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens". URL: https://datatracker.ietf.org/doc/html/rfc8705.

[59] International Data Spaces Association (IDSA). ‘IDS Communication Protocol version 2 (IDSCPv2) on GitHub”. URL: https://github.com/industrial-data-space/idscp2-jvm.

[60] Topsector Logistiek. "ISHARE as generic trust framework capability". URL: https://topsectorlogistiek.nl/wp-content/uploads/2022/07/TNO-2022-R11094-Report-iSHARE-as-generic-capability-1.pdf.

Signature

Groningen, June 2023 TNO

M. (Marieke) van Milligen-Versluis
Head of department Data Ecosystems

H.J.M. (Harrie) Bastiaansen, PhD
Lead Author