CENTRE OF EXCELLENCE
DATA SHARING & CLOUD

Towards a Common Carrier Layer

A First Step for a Participant-Driven Data Sharing Approach for Data Spaces

Concept DSSC Book Chapter

July 2026

www.coe-dsc.nl
info@coe-dsc.nl

Title:	Towards a Common Carrier Layer - A First Step for a Participant-Driven Data Sharing Approach for Data Spaces	
Author(s):	S. Pretzsch	Fraunhofer
	H. Bastiaansen, B. Farias Loscio, G. Kruithof	TNO
	K. Chawla, P. Mulder, S. Udayan	TNO
Date:	July 2026	
Number of pages:	24	

www.coe-dsc.nl
info@coe-dsc.nl

Summary

This paper is a concept of a DSSC book chapter. It has been accepted for publication and is expected to be published in the fourth quarter of 2026.

The goal of this DSSC book chapter is to disseminate the results of the CoE-DSC work on a participation-driven model based on a Common Carrier Layer as enabler for large-scale interoperability and federation of data spaces. The audience is the broader (applied) research community, aiming to foster the discussion on its applicability, development and deployment.

The participation-driven model based on a Common Carrier Layer may become a key success factor for broad adoption of data space architectures and concepts and realizing the EU ambition of the Common European Data Spaces, as expressed in the EU Data Strategy.

Abstract of the book chapter

This chapter introduces the concept of the Common Carrier Layer (CCL), a novel approach to enable cross data space participation. We reflect on the evolution from current “community-driven” data spaces towards cross data space use cases and the need for a “participant-driven” data space approach, where individual participants control and manage their dynamic data sharing relationships with others. The participant-driven model is enabled by the CCL, whose onboarding provides participants with a single point of entry to access data across community and data space boundaries. This approach builds on data space standards and integrates an easy-to-use trust framework based on eSignatures/eSeals, which is part of the EU eIDAS regulations and enables participants to easily create secure, legally binding data sharing agreements. The CCL extends the Interlinking Layer concept, a key part of the European Mobility Data Space initiative to build a cross-data space “horizontal” infrastructure. The participant-driven data sharing model, together with the CCL, forms the foundation for a layered data space architecture, enabling clear separation of roles and supporting cross-domain use cases, large-scale federation, and interoperability. Further, this chapter presents a proof of concept, demonstrating a representative mobility use case with potential applicability to other domains. The findings of this work provide key contributions to cross-data space interoperability.

Keywords

Data Space, Community-Driven Data Sharing, Participant-Driven Data Sharing, Common Carrier Layer, Cross-Data Space Interoperability.

1 Introduction

The concept of data spaces is central to Europe's Data Strategy [1], which expresses the ambition to create "Common European Data Spaces" [2], while aiming for a single market for data to ensure Europe's global competitiveness and data sovereignty. Data spaces are created to provide a scalable mechanism for sharing data among numerous participants and stakeholders. They include mechanisms for data governance, metadata management, and access control, allowing stakeholders to maintain control over their data while benefiting from shared resources and insights.

Presently, the data sharing landscape includes both the emerging sectoral data spaces as part of the broader Common European Data Spaces initiative, and a plethora of individual Data Sharing Initiatives (DSIs) and communities [3]. In the mobility and logistics domain for example, there are already several national data spaces in operation, such as the German MDS [4], the French Eona-X [5], the Belgian FSDS [6], and the Dutch BDI [7].

However, these DSIs and data spaces are organizationally and technically not interoperable with each other. This limits the full exploitation of the potential value of data sharing, as data sharing use cases and the needs of their participants generally extend beyond the boundaries of a single DSI or data space. For example, mobility and logistics data sharing use cases often span regional or national borders and will involve data stemming from other sectors such as energy, tourism, and urban infrastructure.

The need for cross-community data sharing becomes even more pronounced with the rise of new data sharing application areas such as Digital Product Passports (DPPs) as mandated by the European Commission's ESPR Regulation [8], collaborative Digital Twins (DTs) to create comprehensive simulation environments [9], and Privacy Enhancing Technologies (PETs), which allow access to and processing of sensitive data without requiring the data itself to be shared between participants for privacy, legal, or ethical concerns [10]. These emerging application areas integrate data from various sectors and therefore operate across sectoral or regional data sharing communities.

In the context of the common European Mobility Data Space (EMDS), the European Commission (EC) already reacted by proposing an Interlinking Layer [11] as a core part of the EMDS to enable cross-data space data discovery by collecting metadata in a federated catalogue.

Considering the increasing relevance and growing interest in cross-community data sharing, this chapter introduces a novel data sharing model for data spaces, which enables participants to access data across data space boundaries: the participant-driven approach, which is enabled by a Common Carrier Layer (CCL). The CCL supports the dynamic establishment of bilateral trusted data sharing relationships and enables the secure sharing of (potentially sensitive) data. Participants in these relationships are not required to belong to the same data space or be part of any data space at all. The CCL provides an implementation of Article 33.1 of the EU Data Act [12], which specifies the essential requirements for interoperability of data, data sharing mechanisms, and data sharing services.

The participant-driven approach builds upon recently developed data space standards, such as the Data Space Protocol, in combination with a simple, low-barrier, electronic trust framework. Together, these elements enable legally binding data transaction contracts, i.e. an enforceable agreement governing data access and use between data space participants. Such contracts are aligned with the EU Data Act and can be implemented by means of existing eIDAS-compliant trust services to ensure legal validity and accountability.

To validate the feasibility of the participant-driven approach, a Proof of Concept (PoC) focused on a mobility data sharing scenario was implemented. The PoC demonstrates how a data provider and a data consumer can share (potentially) sensitive data in a trusted manner, even when they do not belong to the same DSI or data space.

This chapter has the following structure. Section 2 presents a motivational example of a use case across data spaces, after which Section 3 describes the basic concepts required for trusted sharing of sensitive data. Subsequently, Section 4 addresses the community-driven approach as currently being used for data sharing in data spaces, together with its limitations in supporting cross-cutting use cases in a largely scalable manner. Section 5 introduces the participant-driven approach as an alternative, together with its enabling CCL. Section 6 elaborates on the PoC. The participant-driven approach and the CCL can provide the foundation of a layered business and technical system architecture, which is elaborated in Section 7. The next steps for further developing, deploying and adopting the participant-driven approach and the CCL are described in Section 8, after which Section 9 presents the overarching conclusions.

2 Motivational Examples: Data Sharing across Data Spaces

It is particularly important to share data across data spaces in scenarios where combining diverse data sets is necessary to address complex challenges. For example, in healthcare, the combination of patient records, research data, and clinical trial results from different institutions can enable more effective disease management. Similarly, in smart cities, the integration of data from transportation systems, energy grids, and environmental sensors may optimize urban planning and resource management. Overall, cross-cutting data sharing enables significant advances in data management, promoting a more connected and data-driven world.

In the mobility sector, there is already a plethora of data ecosystems in place, some of which are already based on data space concepts and technologies, such as Eona-X and the German MDS. These data spaces are managed by regional private or public organizations responsible for their governance and technical infrastructure. To access data and services from these ecosystems, an organization must become part of these ecosystems, and it is still necessary to sign individual participant contracts with the respective data space governance authorities and undergo organizational and technical onboarding procedures. This current setup does not support the ambition of mobility stakeholders on the European and international level that need to access (potentially sensitive) data from a multitude of these DSIs and data spaces. For example, globally operating service providers that broker connected journeys and tickets to end-users want to combine long distance (train and air) and “first- and last-mile” local transport options. Therefore, they need to access the data of long-distance operators as well as local transport operators.

However, these local operators are currently structured within regional data ecosystems. This means that globally operating service providers currently need to become participants in each regional data sharing ecosystem to gain access to only a limited number of local operators. This situation does not scale, because the globally operating service providers need to sign contracts with each individual DSI or data space authority to get access to their participants’ data offerings.

3 Data Sharing: Basic Concepts

For participants to be willing to share sensitive data, trustworthy data sharing infrastructures are needed, in which legally binding data transaction contracts are established. In the following paragraphs, we present the following basic concepts: the fundamental capabilities for trusted data sharing (Paragraph 3.1), the role of trust frameworks (Paragraph 3.2) and data transaction contracts (Paragraph 3.3) therein.

3.1 Fundamental Capabilities for Trusted Data Sharing

Two fundamental capabilities are indispensable for ensuring that (potentially sensitive) data can be shared:

i) *Data Sovereignty*, providing data holders and data owners with the means to define and enforce the conditions under which its (potentially sensitive) data is shared. This may be done by specifying access and usage terms, thereby protecting sensitive information and upholding compliance requirements;

ii) *Trust,* establishing governance, legal and technical agreements together with mechanisms to ensure their compliance in order to build trust among the participants, and ensure that shared data adheres to agreed-upon terms and is not misused.

In addition, a third capability that may be considered as fundamental is *Discoverability*, enabling the registration, exposure, and searching for entities such as data, participants and data sharing initiatives, preferably across sectors, borders, and application areas. Although not a strict prerequisite for providing the holders with sufficient confidence to share their data, discoverability does make the plethora of available data findable and accessible.

Figure 1 depicts how these three fundamental capabilities are provided by means of data space participant agents. Each participant agent consists of a Control Plane and a Data Plane, facilitating federated data sharing in a flexible manner. The Control Plane implements the Data Space Protocol (DSP) [13], which consists of the discoverability protocol (based on the DCAT [14]), the definition of usage policies (expressed in the ODRL [15]) and the contract negotiation protocol. Moreover, the participant agents of the data provider and data consumer are both linked to the trust framework of their associated data space, which are generally different and non-interoperable when they are developed for different data spaces.

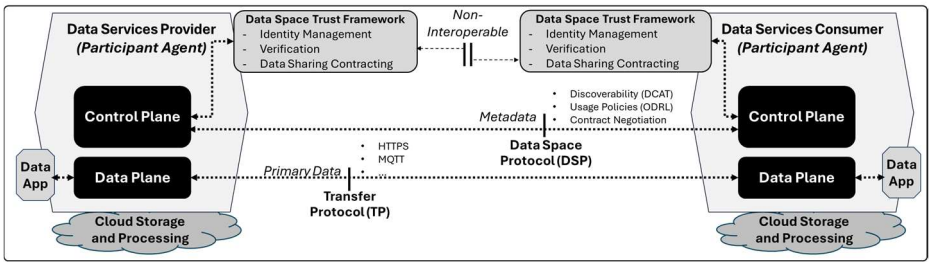

Fig. 1. Data sharing between participant agents enabled by the Data Space Protocol (DSP).

In addition, the figure shows the transfer protocols as supported by the Data Plane, which are managed by the control plane. The Eclipse Data Space Components (EDC) framework [16] and the FIWARE Data Space Connector [17] are initial (open source) data space agent implementations.

3.2 Trust Frameworks

As Figure 1 shows, the participant agents of the data provider and data consumer are associated with the trust framework of their data space, which may differ in terms of implementation, configuration, or

trust anchor. However, interoperability between trust frameworks is key when sensitive data needs to be shared.

Multiple architectures for realizing the required interoperability between trust frameworks are feasible, may coexist and can be complementary [18]. In a data space, the data space governance authority governs the trust framework on behalf of its participants. As such, data space governance authorities need to address (the challenges of) trust framework interoperability across data spaces at design time to support cross-community data sharing use cases involving sensitive data. Two main architectures can be distinguished for enabling trust framework interoperability between data spaces: the Federated Trust Framework and the Spanning Trust Framework [18]. These architectures are shown in Figure 2.

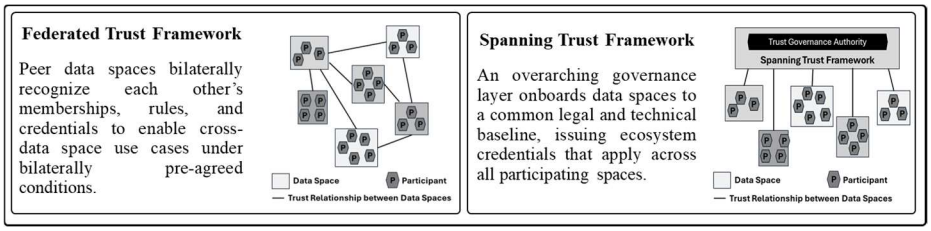

Fig. 2. Trust framework interoperability architectures: Federated Trust Framework and Spanning Trust Framework.

Both trust framework interoperability architectures have their specific types of use cases for which they are suitable. Nevertheless, they also have their limitations:

- The *Federated Trust Framework* architecture requires minimal organization and control. However, due to complexity in having to make bilateral or multi-lateral legally binding conditions and agreements on joint rules across each of the four interoperability layers of the European Interoperability Framework (EIF) [19], scalability issues may arise in the number of participating data spaces in the federation.
- The *Spanning Trust Framework* architecture needs each participating data space to join the overarching or spanning ecosystem of data spaces. Large-scale adoption therefore needs broad acceptance of both the overarching framework (spanning across the data spaces) of legal conditions and agreements, and the separate governance authority responsible for the overarching or spanning ecosystem of data spaces.

Protocols and solutions are available to implement these trust framework architectures, including the Gaia-X Digital Clearing House (GXDCH) [20] and the iSHARE Trust Framework [21]. Alternatively, recent advancements in distributed identity and claims architectures provide fundamental capabilities for dynamically establishing trust relationships as part of the participant agent architecture, i.e. independently of specific trust frameworks. This includes the Decentralized Claims Protocol (DCP) [22], the OpenID for VC (OID4VC) [23] and the EU Digital Identity wallets (EUDI-wallet) [24] being mandated under the eIDAS Regulation [25].

3.3 Data Transaction Contracts

Agreement negotiation protocols, such as provided by the DSP, yield dynamically established technical data sharing agreements. However, from a legal perspective, they do not represent legally binding contracts in their current form.

While the EU currently lacks a harmonized Civil Code that can harmonize private law across the Member States directly, in EU law, Article 9 of the eCommerce Directive (Directive 2000/31/EC) [26] requires all Member States to ensure that their legal system allows contracts to be concluded by electronic means. This is, for instance, implemented in Dutch law in the Burgerlijk Wetboek [27] in Art. 6:227a. Looking at the implementation of this into Dutch law further, the important features of an 'agreement' under the Dutch Civil Code are that it must be a statement of consensus, as a multilateral legal act intended to bring about legal consequences, at the expense of one (or more) parties and to the benefit of others [28 – 29]. This agreement may be free of form, unless required otherwise by law. Concretely, this also requires an offer to be made and an acceptance (Art. 6:217, 6:218, Burgerlijk Wetboek). While there are many variations between jurisdictions, these requirements reflect the broad,

basic requirements for validity of a contract as well: offer, acceptance, consideration in common law or 'cause' in civil law, paired with the legal capacity to contract and non-violation of existing (more specific) legal requirements [29 – 30].

Hence, for data sharing agreements to become legally binding contracts, agreement by both the data provider and consumer, with the *intention* of creating a *binding* agreement and clarity regarding the steps that create the same (Art. 10, eCommerce Directive), is needed. The act of attaching a signature to agreed-upon terms is crucial evidence that there has been a meeting of the minds between the parties, and that there is an intention to create a legally binding agreement. This is also reflected in Art. 6:227a (1) (b, c, d) of the Burgerlijk Wetboek. For this, Art. 25 of the eIDAS establishes the validity of electronic signatures in general, and Art. 3 (10, 11, 12) establishes the three 'levels' of such signatures, going from simple 'electronic signatures' to 'advanced electronic signatures' and 'qualified electronic signatures'. Critically, as established in Art. 25 eIDAS, qualified electronic signatures are the only types of electronic signatures that are directly presumed to have the same legal effect as a handwritten signature.

The reliable and trustworthy creation of a digital contract requires a qualified electronic signature as mandated by the recent EU eIDAS regulation [25], with electronic seals (or eSeals) serving to establish the origin and integrity of a document as per Art. 35 [31]. It should be noted that qualified eIDAS eSeals and eSignatures service offerings are already becoming broadly available in EU member states, provided by eIDAS Qualified Trust Service Providers (QTSPs).

It is important to clarify at this point that we discuss here the procedural rules for the 'formation' or 'conclusion' of a valid contract, without going too deeply into the requirements regarding the completeness of the content of such an agreement. In addition to conditions for creating a legally binding agreement as listed above, data-transaction agreements can include clauses and components such as intellectual property rights, liability terms, and dispute resolution mechanisms. Given the context of the data usage contract, such components may be necessary, desirable or even mandatory. These components may be electronically negotiated by means of the DSP, defined within specific data spaces as overarching agreements, or covered in a natural language contract to which a machine-readable policy is an addendum (both of which would together form the 'electronic contract'). Similarly, contract law often includes requirements for fair contracts, as also reflected in the Data Act [32]. However, evaluating the fairness of such terms is outside the scope of the technical framework tested and validated here. An additional core requirement is likely that the parties can show what terms were agreed upon in terms of electronic contracts. The eCommerce Directive requires that contract terms are made available to a recipient 'in a way that allows to store and reproduce them'. In parallel, Art. 6:227(1)(a) requires the agreement to be 'accessible' to both parties. This may also be part of the requirements in EU consumer law to provide contracts in a 'durable medium', i.e., a medium that allows them to store the information for future reference for as long as necessary [33]. This requirement can likely be complied with by providing each party with a copy of the final, electronically signed contract, for their own storage [34]. To this end, being able to mutually access the signed contract via a shared resource is useful, but not a necessary requirement. For this shared storage capability, an 'observability service' can be developed and included as part of the CCL, as for example proposed in the "Logging House" chapter of this book. It should be noted that digital identities and signing (such as provided by eIDAS) may also be integrated in the bilateral contract negotiation process to provide participants with more advanced trust levels in the early phases of contract development. For a minimal implementation of the participant-driven approach that supports a broad range of basic data sharing use cases, this may, however, not be required, and digital signing of the resulting sharing agreements may suffice to yield a legally binding contract.

4 The Community-Driven Approach: Limitations in Supporting Cross-Cutting Data Sharing Use Cases

In the current landscape of data spaces, we observe that ecosystems are “community-driven”. This means that a community of stakeholders, organized around a specific domain, use case, or region, constitutes a data space for a specific purpose, which is then operated and used by this community under the control of a data space governance authority.

For use cases within well-defined (“closed”) communities of participants that have strong similarities in data sharing requirements, such a static top-down community-driven approach may be appropriate. This approach is helpful within the boundaries of a data space and is supported by community-specific agreements that are managed by the data space authority, at each of the four interoperability levels of the European Interoperability Framework (EIF), i.e. to ensure technical, semantic, organizational, and legal interoperability. These agreements are tailored to meet the specific needs of the community and their use cases.

However, participants wanting to use data from different data spaces for their products and services face the challenge of having to become participants in every relevant data space. For every data space, such a participant needs to conclude an accession contract with the data space authority, follow an individual onboarding process and undergo cumbersome trust-enabling procedures. The software components required for participating in a data space, referred to as a data space connector or participant agent, are tailored to the specific requirements of a particular data space and cannot be used for participation in another data space. Hence, such a participant needs a dedicated software connector for each data space. This approach does not scale from a participant perspective, especially for participants acting across regions and sectors and therefore depend on a variety of different data sources.

The community-driven approach faces challenges in supporting use cases that extend beyond data space borders. Federation between data spaces requires bilateral agreements at each of the four EIF interoperability levels, which involves significant alignment complexities. These are particularly prominent in governance, legal, and trust relationships. Furthermore, as the number of data spaces to be federated is expected to grow significantly, reaching complex interoperability and federation agreements on a bilateral basis among multiple data spaces will not be scalable.

Hence, from both the participant perspective and the data space federation perspective, an alternative data sharing approach becomes necessary. Such an alternative is possible by enabling the dynamic establishment of trusted data sharing relationships between participants, without being restricted to participants within a single data space. This is referred to as the participant-driven approach, which is introduced and further elaborated in the remainder of this book chapter.

5 The Participant-Driven Approach Enabled by a Common Carrier Layer

Participant-driven data sharing implies that participants (e.g. data providers and consumers) are individually responsible for establishing trustworthy data sharing relationships, i.e. without relying on onboarding to an overarching community by dedicated governance authority. It requires a participant-driven trust framework, which is managed by individual participants. They can (dynamically) establish bilateral, legally binding, trust relationships between individual participants at runtime, even when these participants are members of different DSIs or data spaces. The participant-driven approach is enabled by a Common Carrier Layer (CCL) with the capabilities to bilaterally establish these legally-binding, trust relationships, bypassing the role that is taken by the data space governance authority in the community-driven approach.

The following paragraphs elaborate on the capabilities of the CCL (Paragraph 5.1) and its deployment aspects (Paragraph 5.2), respectively.

5.1 Common Carrier Layer

The Common Carrier Layer (CCL) consists of a set of services that enable individual participants to manage trusted data sharing relationships on a bilateral basis without dependence on a 'community' governance authority. Hence, the CCL is the enabler of the 'participant-driven approach'. The CCL itself is a distributed system, comprising layers of services that specify and facilitate interactions between participants. As depicted in Figure 3, the CCL consists of three layers: the Trust Layer, the Interoperability Layer and the Discoverability Layer.

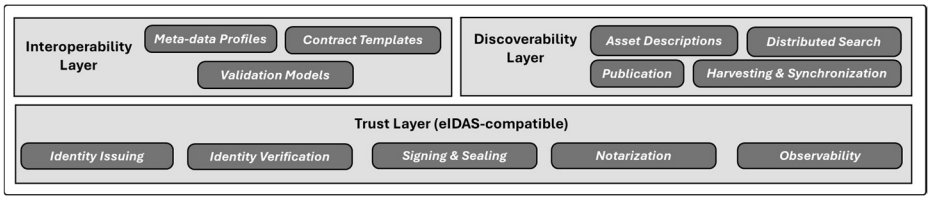

Fig. 3. Common Carrier Layer.

The *Trust Layer* enables participants to use eIDAS trust services to: (1) obtain a trusted identity (eID) from a QTSP, (2) verify the eIDs of other participants via an QTSP, (3) electronically sign and seal documents, and (4) optionally connect to notarization services that act as "witnesses" to the contract agreements, and which store log information about the signing steps taken by the participants (see also the book chapter on Logging).

The *Discoverability Layer* consists of interconnected catalogue services that are partially synchronized and able to forward search queries to other catalogue services. These mechanisms work like DNS servers. Data product descriptions from data space participant agents are published to a catalogue, which in turn gets distributed among other catalogue services within the Discoverability Layer.

The *Interoperability Layer* consists of repositories that provide interoperability-enabling assets. They may comprise (1) data interoperability and semantics services such as provided by vocabulary hubs, e.g. as developed as building block for the data space blueprint of the EU DSSC initiative [35], (2) ODRL contract template services as the basis for the contract negotiation process, covered by the DSP

protocol, (3) meta-data profile services to describe data and service offerings with meaningful attributes, and (4) validation model services, such as SHACL shapes.

5.2 Deployment Aspects

For deploying the participant-driven approach based on the CCL services only minimal effort is needed, as the CCL services are already emerging as offerings of multiple independent service providers.

Participants require a data space participant agent. The data space participant agent can either be obtained as open source and deployed by the participant or may be acquired from a Connector-as-a-Service (CaaS) provider. The latter has the advantages of ease of use and ensured compatibility of data space participant agents between participants. The data space participant agent must support the following capabilities:

- The DSP for contract negotiation, allowing participants to bilaterally establish data sharing relationships and control the policies and conditions under which they share their (potentially sensitive) data.
- Connection to the Discoverability Layer for publication and discovery of data products. Participants can optionally publish asset-describing metadata to the Discoverability Layer. Technically, the participant agents connect to one or more catalogue services that constitute the Discoverability Layer and register the agent. Subsequently, these catalogue services harvest the agent's local catalogue and distribute the data product descriptions among other catalogue services within the Discoverability Layer. Similarly, search queries from a data consumer are directed towards a connected catalogue and distributed within the Discoverability Layer, returning all relevant results back to the participant agent of the data consumer. The EMDS Interlinking Layer [11] is already being developed and deployed by the European Commission (EC) to provide such federated cataloguing services as a core part of the EMDS, which may be extended to serve other sectors as well. In addition, assets such as ODRL contract templates and validation models (such as SHACL shapes) should be available from the Interoperability Layer.
- Integration functions with an eIDAS QTSP for: (1) Obtaining an eID from a QTSP as the basis for further eIDAS processes; (2) Providing eIDAS signing and sealing functions to make data sharing contracts legally binding. In combination with the contract negotiation protocol of the DSP, an agreement proposal (or subsequently a counteroffer) will always already be electronically signed by the participant when sending it to the other participant. If the agreement is accepted by the other participant, it gets countersigned as well and sent back, so that both participants have the mutually signed agreement as legally binding contract; (3) Getting eIDAS Qualified Website Authentication Certificates (QWACs) [36 – 37] to encrypt HTTP traffic. This already reduces complexity compared to most community-driven approaches, where HTTP encryption and identity credentials require different technologies. With an eIDAS QWAC, the same private key as for signing can be used. Hence, the identity of a participant can already be verified with the first HTTP connection. Therefore, a dedicated protocol, such as DCP, is not required for identity verification.

  For convenience, the participant agent may already integrate a list of available QTSPs from which the participant (either the data provider or data consumer) can choose.

Based on these deployment aspects, the introduction of the participant-driven approach based on a CCL requires the implementation of the DSP and eIDAS protocols, but no additional legal commitments to be made (e.g. as prescribed to join data sharing communities or data spaces). Moreover, only low-level technical capabilities are needed to participate, while participants can still share sensitive data with other participants in the CCL. This provides the participant-driven approach based on the CCL with high scalability in terms of the number of participants, while also enabling it to serve a broad range of cross-cutting use cases. Moreover, it can provide an extensible foundation for more complex data space business role models, as described further in Section 7.

6 Proof-of-Concept

This section presents a Proof of Concept (PoC), demonstrating the feasibility of the participant-driven approach and the CCL in supporting data sharing. The PoC expands on the motivational data sharing example introduced in Section 2. It demonstrates how to dynamically establish legally binding contracts between participants using eIDAS-based electronic signing for bilaterally negotiated agreements.

For the implementation, we made the following assumptions: (1) the data consumer has already identified data providers who can supply the required data, (2) both the data consumer and data provider have a data space participant agent that supports the DSP, and (3) both the data provider and the data consumer use an eIDAS QTSP service to enable eSigning and eSealing data sharing contracts, resulting in legally binding data sharing contracts. Figure 4 shows the sequence of interactions implemented in the PoC.

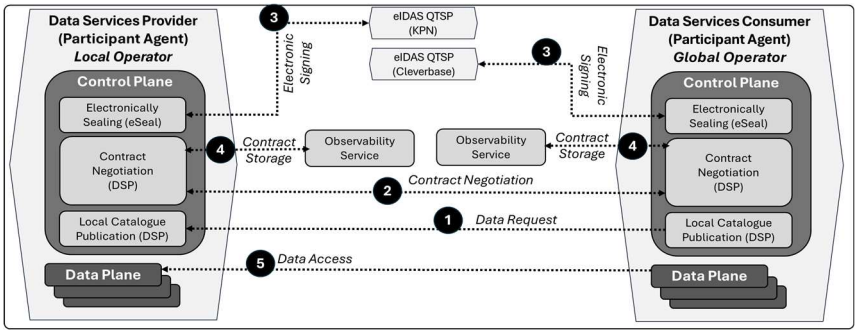

Fig. 4. Sequence of interactions in the PoC implementation.

1. *Data Request*: the globally operating service provider contacts one of the two local transport operators and sends a request for access to its data service API.
2. *Contract negotiation*: the local operator (as data provider) and the global operator (as data consumer) bilaterally run the contract negotiation protocol by means of the DSP until they reach mutual agreement on a usage policy. To facilitate this process, the participants use pre-defined contract templates.
3. *Electronic Signing*: Both participants electronically sign the agreed-upon contracts into legally binding data transaction contracts, using the identity and signing services of their qualified eIDAS service providers. As a first step, they use a qualified eIDAS eSignature, followed by a qualified eIDAS eSeal, both as provided by their eIDAS QTSP. The former expresses the participant's intention to create a legal agreement, the latter that its integrity and origin are confirmed by the participant's organization. Together, these mechanisms provide assurance that the participants' organizations are legally binding entities. When necessary (optionally), both participants can verify each other's eIDAS electronic signatures as part of these processes. The QTSP's electronic signatures can be validated by means of the EU Digital Signature Service (EU DSS).
4. *Contract Storage*: Participants may employ an observability service for prolonged contract storage. This ensures that contracts remain accessible and available even in the event of corruption of local data. Although not a strict condition for a data transaction contract to be legally binding, it is useful to have (see Paragraph 3.3).
5. *Data Access*: the data provider provides access tokens for the local ticketing APIs to the global data consumer. These tokens are valid for the period agreed upon in the data transaction contract. The globally operating data consumer can then access ticketing APIs to sell local transport tickets.

The PoC has been implemented using the TNO Secure Gateway (TSG) [38], an IDSA-certified data space participant agent, for both the data provider and consumer. It runs the DSP with the contract negotiation protocol for digital contracts with usage policies expressed by means of ODRL. For the PoC scenario, ODRL policies were negotiated on the applicable jurisdiction (country), and the period for

unrestricted data access. An eIDAS extension has been implemented in TSG for electronic signing (negotiated) data transaction contracts. This eIDAS extension integrates with the commercial eIDAS service offerings provided by two different Dutch EU-accredited eIDAS QTSPs [39]: Cleverbase as used by the data consumer and KPN as used by the data provider. Cleverbase is also developing a Qualified Electronic Storage (QES) service, which will be considered as an observability service in future development steps. Both eIDAS QTSPs implement the Cloud Signature Consortium API (CSC API) [40] for electronic signing. The CSC API is currently becoming a widely adopted standard and has therefore been implemented in the PoC in the TSG eIDAS extension. Specifically, the electronic signatures are created in the form of a JAdES-B-LT document in the eIDAS QTSP's digital signing service. By using eSigning and eSealing services of commercial eIDAS QTSPs, the current feasibility of compliance with EU regulations, accredited and ubiquitously available electronic signing services for bilaterally established, legally binding data transaction contracts have been demonstrated in the PoC.

7 Towards a Layered Business and Technical Data Space System Architecture

The integration of community-driven and participant-driven approaches to data sharing fosters the development of innovative business models. Sector-specific data spaces and application areas can benefit from the services provided by the Common Carrier Layer (CCL), while participants in the CCL, in turn, may leverage membership claims and credentials issued within these communities.

Figure 5 depicts a layered business and technical architecture that results from combining participant- and community-driven data sharing strategies, thereby enabling the realization of such business models. In the following paragraphs, the layered business model (Paragraph 7.1) and the hybrid model (Paragraph 7.2) are described. However, additional models may emerge from such a combination.

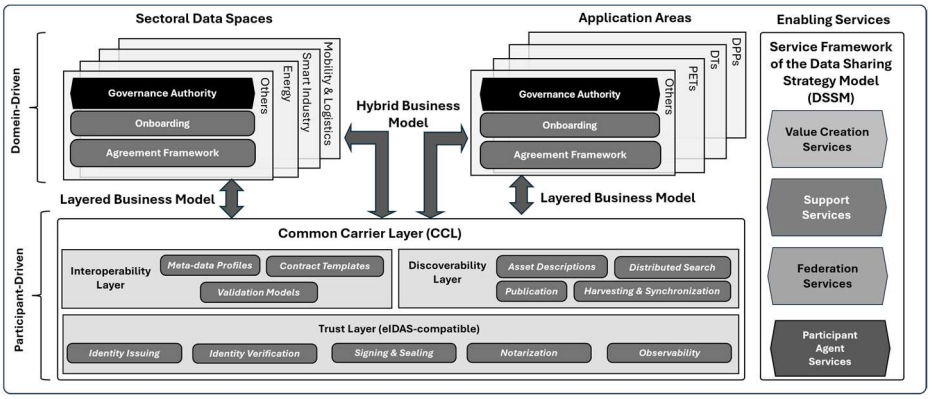

Fig. 5. Layered business and technical architecture resulting from the integration of the participant and community-driven approaches for data sharing.

It should be noted that Fig. 5 also includes the Data Sharing Strategy Model (DSSM) [41], which provides a framework for data sharing building blocks through third-party enabling services. The DSSM services framework is further addressed in Paragraph 8.1.

7.1 Layered Business Model: Enabling Services for Community-Driven Reuse

In the layered business model depicted in Figure 5, each community-driven data space operates at a higher layer and retains its own governance authority and governance framework. Despite this autonomy, the layered model enables higher-layer communities to reuse the processes, services, and infrastructure provided by the underlying CCL. This approach increases efficiency for data spaces in developing and deploying their data space environment and infrastructure, while also improving effectiveness for participants by simplifying onboarding processes in specific communities when CCL (eIDAS) identities can be reused. Moreover, participants also benefit from the ability to engage in cross-community data sharing use cases, which are inherently supported by the participant-driven approach and facilitated by the CCL.

Further efficiency is achieved through economies of scale and scope, as the CCL's trust interconnection and enabling services are harmonized and reused across multiple data spaces and application areas.

By leveraging the CCL's shared infrastructure capabilities, the layered business model reduces duplication of effort and maximizes resource utilization, thereby enabling cost-effective and scalable data sharing solutions.

Ultimately, the layered approach, combining participant- and community-driven approaches, brings together the strengths of both models by delivering a comprehensive set of data space capabilities and services that ensure robust and flexible data sharing across sectors and communities.

7.2 Hybrid Business Model: Integration of Community-Driven and Participant-Driven Approaches

The hybrid business model introduces another scenario in which community-driven and participant-driven approaches are combined in a complementary manner to reinforce each other's capabilities. In this model, claims and credentials associated with data space memberships, e.g., as implemented by means of Verifiable Credentials (VCs), are incorporated into the data sharing contracts that are bilaterally negotiated between participants, even when these interactions occur outside the formal boundaries of a data space. These membership claims and credentials can be verified during the contract negotiation and signing processes and may be used as prerequisites—expressed as policies—for engaging in data sharing transactions. As a result, the hybrid model provides additional trust and assurance regarding participant accreditation and their associated legal commitments.

CEN/CENELEC is currently developing the Trusted Data Transaction format [42 – 44], which defines a common structure for data sharing transactions. This format allows data space membership claims and credentials to be included alongside permissions, prohibitions, and obligations within the data product definition, where obligations may reference applicable claims and credentials.

By incorporating data space membership claims and credentials into the Trusted Data Transaction format, they become part of the dynamic establishment of bilateral data sharing relationships in the participant-driven approach. This enables hybrid data sharing scenarios in which participant-driven contract negotiation mechanisms are combined with community-driven claim and credential issuance and verification.

It should be noted, however, that such hybrid scenarios may still require a community-driven trust framework governance model to validate the meaning, scope, and accreditation under which membership claims and credentials have been issued. Consequently, the applicability of these hybrid scenarios remains subject to the characteristics and scalability limitations of the community-driven data space and trust framework federation approaches previously addressed in Section 4.

8 Next Steps toward Development, Deployment and Adoption

The previous sections have addressed the architectural fundamentals for introducing a participant-driven approach and the CCL to support large-scale interoperability and federation in an emerging and overarching ecosystem of data sharing initiatives and data spaces. The following paragraphs in this section address additional topics that are considered highly relevant for further developing, deploying, and adopting the participant-driven approach and the CCL, including enabling services, recently developed within the service framework of the Data Sharing Strategy Model (DSSM, Paragraph 8.1), service offerings and cost structures for digital signing services (Paragraph 8.2) and the (high-level) evolution and migration options for existing data sharing initiatives and data spaces (Paragraph 8.3).

8.1 Enabling Services: Service Framework

In addition to the fundamental capabilities of the CCL as described in the previous sections, a set of data space building blocks should be developed as re-usable enabling services. This is referred to as the service framework, which is part of the overarching Data Sharing Strategy Model (DSSM) [41] and is depicted in Table 1. The DSSM services framework is based and extends on the DSSC building block model [35], distinguishing four categories of services: Participant Agent Services, Federation Services, Support Services, and Value Creation Services, as described Table 1.

Table 1. Enabling services according to the DSSM services framework

Participant Agent Services These services support individual participants in connecting to, interacting with, and enforcing agreed rules. They typically sit close to the participant's systems and implement control plane and data plane functionality required for secure and governed data exchange.	**Support Services** They enable adoption, operation, and sustainability of participation. They focus on organizational, technical, and operational enablement rather than core federation or data exchange functionality.
Federation Services They provide capabilities that allow multiple participants, data spaces, ecosystems, and service providers to interoperate without centralizing control or data. They typically operate at ecosystem or infrastructure level and enable trust, discovery, observability, and semantic alignment.	**Value Creation Services** These services create business and regulatory value, by leveraging federation and participant services to enable domain-specific applications, regulatory use cases, and advanced data-driven services, such as Digital Product Passports (DPP), sustainability reporting, and trusted data sharing across value chains.

In the DSSM services framework, it is anticipated that these enabling services will be (commercially) offered by independent service providers. To be broadly re-usable for a multitude of data sharing use cases, either based on a participant-driven or community-driven approach, the enabling service offerings must:

- be offered and made accessible through well-defined APIs, adhering to the data spaces standards and protocols as currently being defined,
- be diversified and tailored to the varying needs of a broad and diverse spectrum of participants, with strong variations in IT-savviness and capabilities, and
- support mutual federation of the services offerings across the services providers, if relevant. It improves effectiveness (in scale and scope) for the service providers as their services are

deployed for a great reach of users. For instance, this may result in a federated catalogue of data sharing services that is perceived by participants as a single service although implemented as a federation of many interconnected individual catalogues of multiple providers.

The (DSSM) services framework is further elaborated in this book's chapter [45].

8.2 Digital Signing Services: Cost Structures and Service Differentiation

The participant-driven approach based on the CCL relies on electronic signatures for creating legally binding data sharing contracts, for example through commercially available eIDAS eSealing and eSigning services, as used in the PoC described in Section 6. Since electronic identities and eSigning are needed for each data sharing transaction and may also be implemented in the future as part of the bilateral contract negotiation process (see Paragraph 3.3) and for securing data exchanges (see Paragraph 5.2), the architecture may become highly dependent on eIDAS services.

Hence, a pricing scheme is needed for electronic identities and signing that reflects its use in data transaction services to be economically viable. Such a matching pricing scheme should find a balance between its components for:

- onboarding the electronic identity and signing services, obtaining the digital certificate and for managing it as part of an organization's (internal) electronic signing processes, and
- using the electronic identity and signing services, e.g. both for the signing of digital data transaction contracts and for the verification of identities and certificates.

Moreover, the electronic identity and signing service offerings must serve the needs of a broad and diverse spectrum of participants. Moreover, different management and usage mechanisms may be needed for electronic certificates and keys, e.g. by means of hardware tokens (such as USB- or smartcard-based) that are used by participants on their computers or by means of managed service solutions within a highly-secure environment of the service provider accessible for a participant with a mobile app.

8.3 Evolution and Migration of (Existing) Data Sharing Initiatives and Data Spaces

The previous sections have described the participant-driven approach based on a CCL for large-scale interoperability to support data sharing use cases across DSI and data space boundaries. It should be recognized that the deployment and adoption of this architecture must take place in an environment in which a multitude of community-driven data sharing initiatives and data spaces are already operational, as illustrated by an inventory for the mobility and logistics sector conducted by the European Mobility Data Space initiative [46]. This inventory identifies hundreds of such operational, community-driven, data sharing initiatives and data spaces. For the adoption of the new participant-driven approach, it is clear that a gradual evolution and migration process for these existing initiatives is required.

Current community-driven data sharing initiatives manage their trust mechanisms and data space building blocks on their own. This results in conceptual differences and the lack of cross-data space interoperability, even if the same technologies are being used, as described in Section 4. To support the participant-driven approach from an existing community-driven approach, the participants should be able to use and verify eIDAS identity credentials and electronic signing services. To implement this approach, participants need to take the following steps: (1) Their data space participant agents need to be extended to support eIDAS identities (presentation and verification), the DSP and an additional protocol that enables and validates eIDAS electronic signing (both eSignatures and eSeals). This can be done with a dedicated extension to existing data space participant agents as demonstrated by the PoC (Section 6). It remains possible that agents support both eIDAS and a community's own identity management system in parallel to implement different trust levels. (2) Make the use of the DCP protocol optional for the participant-driven approach, since identity verification already happens at HTTPS level.

(3) The data space participant agents need an extension to support publication of asset descriptions at the CCL's Discoverability Layer.

Optionally, community governance authorities can migrate to the CCL approach by contributing their data space service, such as catalogues, to the CCL: (1) by connecting the community's metadata catalogue to the CCL Discoverability Layer to make the community's data offers visible to external data consumers, and (2) by becoming an eIDAS QTSP to issue and manage eIDs for the community's participants. Furthermore, the communities' logging service can be extended to also support information that has been created during the negotiation and signing processes.

9 Conclusions

In this chapter, we introduced the participant-driven approach and the CCL as a vision for the future of large-scale interoperability in data sharing use cases across data space boundaries. Historically, discussions around the development of "Common European Data Spaces" have operated under the assumption that data spaces are *community-driven*, with sector-specific use cases forming the foundation. However, the need for a scalable approach to support use cases across data space boundaries is becoming increasingly important. Instead of participating individually in each data space or trying to establish bilateral agreements between data spaces to establish data space federations, we believe that the *participant-driven* model enabled by a CCL has the potential to support cross-community data sharing use cases on a large scale.

Moreover, the participant-driven approach can complement and may even provide a shared foundation for the more traditional community-driven approach. As such, introducing a layered business and technical data space architecture with a participant-driven CCL may lead to evolving business role models. This also contributes to opportunities for actors to focus on their specific added value through a clear separation of concerns. Individual data space participants can be part of the CCL and engage in participant-driven bilateral data sharing transactions. At the same time, they can be members of specific data sharing communities or data spaces with a minimal effort regarding onboarding process, legal commitments and adherence to agreements. Community-driven data sharing initiatives can concentrate on their community-specific added value without the burden of developing and deploying trust and legal frameworks or generic infrastructure building blocks.

Through commoditization, third-party service providers can achieve sufficient scale. This allows them to function as a shared foundation across multiple data-sharing initiatives and individual participants, offering a portfolio of trust interconnection and enabling services. Jointly, these developments may pave the way towards a sustainable and modular data space services market.

To further advance the participant-driven approach and the CCL, future work will focus on three main directions: (i) the technical validation of the CCL services, as described in Paragraph 5.1; (ii) the elaboration of the business potential of these services through integration into a layered business data space architecture, as outlined in Section 7; and (iii) the dissemination of the underlying concepts across European data space development and deployment initiatives.

Acknowledgements

The work presented in this chapter was conducted under the umbrella of the Dutch Centre of Excellence for Data Sharing and Cloud (CoE DSC, www.coe-dsc.nl), with valuable contributions from the TNO project "Future Proof Smart Logistics" and the EU-funded SM4RTENANCE project (https://sm4rtenance.eu). The described use case and the overarching interoperability requirements between data spaces were inspired by the deployEMDS (https://deployemds.eu/) and boostEDIC (https://edic-ml.eu) projects. We would like to thank these initiatives for providing the opportunity to conduct this highly relevant research within a stimulating and cooperative setting. We also would like to thank Cleverbase and KPN for supporting the topic and providing us with help in integrating their commercial eIDAS services into the proof of concept as EU recognized eIDAS QTSPs. Finally, our gratitude goes to Vera Irmak (TNO) for her thorough review of the legal aspects of data sharing contracting.

References

1. European Commission Homepage, https://digital-strategy.ec.europa.eu/en/policies/ strategy-data, last accessed 2026/03/19.
2. European Commission Homepage, https://digital-strategy.ec.europa.eu/en/policies/data-spaces, last accessed 2026/03/19.
3. S. Oliveira, M. I., Barros Lima, G. D. F., & Farias Lóscio, B.: Investigations into data ecosystems: a systematic mapping study. Knowledge and information systems, 61, 589-630 (2019).
4. German Mobility Data Space Homepage, https://mobility-dataspace.eu, last accessed 2026/03/19.
5. EONA-X Homepage, https://eona-x.eu, last accessed 2026/03/10.
6. Agency Digitaal Vlaanderen Homepage, https://www.vlaanderen.be/digitaal-vlaanderen/onze-diensten-en-platformen/vlaamse-smart-data-space, last accessed 2026/03/10.
7. Basic Data Infrastructure Homepage, https://bdinetwork.org, last accessed 2026/03/10.
8. European Commission Homepage, https://eur-lex.europa.eu/eli/reg/2024/1781/oj, last accessed 2026/03/19.
9. TNO. 'Reliable and Real-Time Digital Twin Systems'. https://www.tno.nl/en/digital/digital-innovations/data sharing/reliable-real-time-digital-twin-systems, last accessed 2026/06/29.
10. OECD: Emerging privacy-enhancing technologies: current regulatory and policy approaches. OECD Digital Economy Papers, No. 351. OECD Publishing, Paris (2023).
11. European Commission, https://transport.ec.europa.eu/transport-themes/smart-mobility/creating-common-european-mobility-data-space_en, last accessed 2026/03/10.
12. European Union, https://eur-lex.europa.eu/eli/reg/2023/2854/oj/, last accessed 2026/03/19.
13. International Data Spaces Association, https://internationaldataspaces.org/offers/dataspace-protocol, last accessed 2026/03/10.
14. World Wide Web Consortium, https://www.w3.org/TR/vocab-dcat-2, last accessed 2026/03/19.
15. World Wide Web Consortium, https://www.w3.org/TR/odrl-model, last accessed 2026/03/19.
16. Eclipse Foundation, https://projects.eclipse.org/projects/technology.edc, last accessed 2026/03/19.
17. FIWARE, https://github.com/FIWARE/data-space-connector, last accessed 2026/03/19.
18. Dutch Centre of Excellence for Data Sharing and Cloud, https://coe-dsc.nl/wp-content/uploads/2025/12/CoE-DSC-Cross-Cutting-Trust-Frameworks-to-support-Data-Sharing-across-Communities.pdf, last accessed 2026/03/19.
19. European Commission, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf, last accessed 2026/03/19.
20. Gaia-X, https://gaia-x.eu/services-deliverables/digital-clearing-house, last accessed 2026/03/19.
21. iShare. 'iSHARE Trust Framework'. https://framework.ishare.eu, last accessed 2026/03/19.
22. Eclipse Foundation, https://projects.eclipse.org/projects/technology.dataspace-dcp, last accessed 2026/03/10.
23. OpenID, https://openid.net/sg/openid4vc, last accessed 2026/03/10.
24. European Commission, https://ec.europa.eu/digital-building-blocks/sites/spaces/ eudigitalidentitywallet/overview, last accessed 2026/03/19.
25. European Commission, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation, last accessed 2026/03/19.
26. European Union, http://data.europa.eu/eli/dir/2019/770/oj, last accessed 2026/03/19.
27. Burgerlijk Wetboek, https://wetten.overheid.nl/BWBR0005289, last accessed 2026/03/19.
28. Sieburgh, C.H.: Asser 6-III. Algemeen overeenkomstenrecht, 16th ed. Wolters Kluwer, Deventer (2022).
29. Chawla, K.: Guarding the Digital Cookie Jar: An Interdisciplinary Study of Automated Privacy Preference Negotiation, Monitoring, and Enforcement. CentER Dissertation Series. Tilburg University, Tilburg (2024).
30. Lando, O., Beale, H. (eds.): Principles of European Contract Law. Kluwer Law International, The Hague (2000).
31. European Union, https://eur-lex.europa.eu/eli/reg/2024/1183/oj/, last accessed 2026/03/19.
32. European Union, https://eur-lex.europa.eu/eli/reg/2023/2854/oj/, last accessed 2026/03/19.
33. European Union, https://eur-lex.europa.eu/eli/dir/2019/770/oj/, last accessed 2026/03/19.
34. European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62011 CJ0049, last accessed 2026/03/19.
35. Data Spaces Support Centre (DSSC). https://blueprint.dssc.eu, last accessed 2026/07/21.
36. European Commission, https://digital-strategy.ec.europa.eu/en/policies/discover-eidas, last accessed 2026/03/19.
37. European Parliament, https://www.europarl.europa.eu/RegData/etudes/ATAG/ /739285/EPRS_ATA(2023)739285_EN.pdf, last accessed 2026/03/19.
38. TNO, https://tsg.dataspac.es, last accessed 2026/03/19.
39. European Commission, https://eidas.ec.europa.eu/efda/trust-services/browse/ eidas/tls/tl/NL, last accessed 2026/03/19.
40. Cloud Signature Consortium, https://cloudsignatureconsortium.org/resources, last accessed 2026/03/19.
41. Centre of Excellence for Data Sharing and Cloud (CoE-DSC). https://coe-dsc.nl. last accessed 2026/08/12.
42. CEN/CENELEC Standard. "EN 18235-1:2026 Trusted Data Transaction - Part 1: Terminology, concepts and mechanisms". Publication date 2026.03.25

43. CEN/CENELEC Standard. “prEN 18235-2 Trusted Data Transaction — Part 2: Trustworthiness Requirements”. Public consultation finished in Q2 2026, final vote expected in Q3 2026.
44. CEN/CENELEC Standard. “prEN 18235-3 Trusted Data Transaction — Part 3: Interoperability Requirements”. Under public consultation in Q3 2026.
45. Van Houwelingen, G., Punter, M., Berkers, F., Stolwijk, C., Stoter, A.: The Influence of the Emerging Service Provider Market on the Data Space Business Model. In: Developing and Deploying Data Spaces (in press).
46. European Commission, https://mobilitydataspace-csa.eu/wp-content/uploads/2024/03/ 2024-03-19-deliverable-d2.1-inventory-of-data-ecosystems-v3.pdf, last accessed 2026/03/19.

www.coe-dsc.nl
info@coe-dsc.nl

Colophon

This concept DSSC book chapter is a result of the work of the Dutch Centre of Excellence for Data Sharing and Cloud (CoE-DSC, www.coe-dsc.nl), specifically its work on interoperability, harmonization and federation of data spaces. It has been accepted for publication and is expected to be published in the fourth quarter of 2026.

The goal of this book chapter is to disseminate the results of the CoE-DSC to the broader (applied) research community and to foster the discussion on applicability, development and deployment of a participation-driven model based on a Common Carrier Layer as enabler for large-scale interoperability and federation of data spaces, a key success factor for broad adoption of data space architectures and concepts and realizing the EU ambition of the Common European Data Spaces, as expressed in the EU Data Strategy.

Authors

- S. Pretzsch — Fraunhofer
- H. Bastiaansen, B. Farias Loscio, G. Kruithof — TNO
- K. Chawla, P. Mulder, S. Udayan — TNO

Contact

- Centre of Excellence for Data Sharing and Cloud (CoE-DSC)
- E-mail — info@coe-dsc.nl
- Website — www.coe-dsc.nl

Augustus 2026

Towards a Common Carrier Layer
DSSC Book Chapter

July 2026

www.coe-dsc.nl
info@coe-dsc.nl