Deliverable D31.4
IDSA-compliant Connectors for secure, reliable, trusted data exchange in federated data space

Project acronym:	MOTIONAL
Starting date:	M7
Duration (in months):	46
Call (part) identifier:	HORIZON-ER-JU-2022-01
Grant agreement no:	101101973
Due date of deliverable:	M46
Actual submission date:	30.09.2026
Responsible/Author:	DLR
Dissemination level:	PU
Status:	Issued

Reviewed: yes
Reviewer: Michaela Haberler-Weber (ÖBB-Infrastructure)

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101101973.

Document history		
Revision	*Date*	*Description*
0.1	29.01.2025	First issue (50% Deliverable)
0.2	03.07.2025	Integration of contributions from partners
0.3	05.11.2025	Further integration of contributions from partners, consolidation of contents
0.4	08.05.2026	Consolidation and of document structure and input integration
0.5	29.07.2026	Consolidation and integration of comments and different text blocks provided by partners
0.6	07.08.2026	Annex and validation added
0.7	22.08.2026	Annex B added
0.8	25.08.2026	Annex C added and conclusion
0.9	29.09.2026	Incorporation and addressing of reviewer's feedback
1	23.10.2026	Addressing of D31.4 specific issue review

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Nicolás Ortiz	DLR	Author
Anthony J Bokolo	IFE	Author
Rossella Bisio	IFE	Author
Giuseppa Caruso	FST	Author
Luca Mariorenzi	FST	Author
James Bergisch	Wabtec	Author
Alexander Meierhofer	Virtual Vehicle	Author
Mario Schwaiger	Virtual Vehicle	Author
Meike van't Hoen	Knorr-Bremse	Author
Saikrishna Adapa	Hitachi	Author

Disclaimer
The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.
Funded by the European Union. Views and opinion expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them."

Table of Contents

1. Executive Summary 6
2. Abbreviations and acronyms 7
3. Background 9
4. Objective/Aim 13
5. Methodology 15
6. Connector Technologies for Federated Rail Data Spaces 18
6.1. Federated Architecture and Connector Component for Rail Data Space 18
6.2. Technical Connector Properties and Core Functions 20
6.2.1. Secure Data Exchange 21
6.2.2. Reliable Data Exchange 21
6.2.3. Trusted Data Exchange 21
6.3. IDSA-compliant Connectors 22
6.4. Application of the IDSA Architecture within MOTIONAL 25
7. Implementation: T-System / The EDC connectors at MotionRail-X 26
7.1. Connector deployment 27
7.2. Working with a connector 28
7.3. Execution of data transfer via connector 30
7.4. An example of application 34
7.5. Security, reliability, trust aspects 34
7.5.1. Secure Data Exchange 35
7.5.2. Reliable Data Exchange 36
7.5.3. Trusted Data Exchange 37
8. Validation of the Connector Implementation 40
8.1. Rail-specific Test Use Cases and Test Data Exchange Scenarios 41
8.2. Demonstrator 50
8.2.1. Demonstration Event 50
8.2.2. Validation of Demonstrator 52
8.3. Validation Results 53
8.4. Discussion 54
8.5. Limitations 54
8.6. Lessons Learned 55
9. Conclusions 57
10. References 59

ANNEX A: Use Cases 60
1. Monitoring of Track Settlement and Identification of Single Faults in Switches 60
1.1 Interface description and Data Model....62
1.2 Implementation Status 64
2. Maintenance Decision Tool 64
2.1 Implementation Status 66
3. Digital Twin of Point Machine....66
3.1 Implementation Status 67
4. Track and Positioning regional Lines and Data Yard Automation 68
4.1 Implementation Status 69
ANNEX B: Interaction with other Flagship Projects....72
5. Interaction with FP3 – IAM4RAIL (Integrated Asset Management for Rail) 72
6. Interaction with FP5 73
7. Interaction with FP6 – FutuRe (Innovative rail services for regional and capillary lines) ...73
ANNEX C: Validation Questionnaire 75

List of Figures

Figure 1. Overview on FP1 work packages associated with the TT....10
Figure 2. Full overview of the Rail Data Space 12
Figure 3. Data exchange within a data space extended from [4]....19
Figure 4. IDS Connector Architecture 23
Figure 5. LivingLab architecture, source T-System. 27
Figure 6. Dashboard associated to a connector for one of the organizations. 28
Figure 7. Tools for connector administration provided by T-System....29
Figure 8. Process for creating an offer 30
Figure 9. User Interface for managing assets, on the right the pop up window for creating an asset. 31
Figure 10. LivingLab interfaces for managing policies and offers/contract definitions. 32
Figure 11. Showing the catalogue of one of our partners....32
Figure 12 – Process from negotiation to data transfer 33
Figure 13. Successful negotiation of test asset 33
Figure 14. Resulting contract of negotiated data asset....33
Figure 15. A sketch for an application externalizing advanced computation based on data collected from a data space and providing back the results to the data space. 34
Figure 16. Overview of components involved in data exchange between two connectors. Source T-system....35
Figure 17. DIH Verification Building Blocks 39
Figure 18. Publishing of data offers to meta data broker 50
Figure 19. Secure data transfer through the connector....51

Figure 20. Screenshot of the LivingLab sandbox environment including a created data offer. 51
Figure 21. Screenshot of the App-Store including executed use-cases. 52
Figure 22. Overview of the use case “Monitoring of Track Settlement and Identification of Single Faults in Switches” 61
Figure 23. Overview of the use case: “Digital Twin of Point Machine” 67
Figure 24. High-level architecture of “Track and Positioning regional Lines and Data Yard Automation” use case 69

List of Tables

Table 1: Comparison between Data Space, B2B, and Data Lake approaches 10
Table 2. System Requirements and Coverage in MOTIONAL 15
Table 3. Technical Connector Properties 20
Table 4. Core functional capabilities of data space connectors 20
Table 5. KPIs for technical performance evaluation 42
Table 6. KPIs scenario 1, Test 1 43
Table 7. KPIs scenario 1, test 2 44
Table 8. KPIs scenario 1, test 3 44
Table 9. Data exchange scenario 2 45
Table 10. Data exchange scenario 3 47
Table 11. Data exchange scenario 4 48
Table 12. Connector capability validation 54
Table 13. Overview of Roles and Requirements 61
Table 14. User Inputs 62
Table 15. Dynamic Data 62
Table 16. Output 62
Table 17. Static Data Super-structure 63
Table 18. Static Data Vehicle 63
Table 19. Additional quantities 64
Table 20. Overview of Roles and Requirements 65
Table 21. Overview of Roles and Requirements 67
Table 22. Overview of Roles and Requirements 70
Table 23: Participant Profiles 75
Table 24: Strategic Relevance & Expected Impact 75
Table 25: Priority Use Cases for the Rail Data Space 76
Table 26: Technical Validation 76
Table 27: Governance & Trust Framework 76
Table 28: Business Model & Sustainability 77
Table 29: Risks & Critical Success Factors 77
Table 30: Final Feedback / overall Validation 77

1. Executive Summary

The establishment of a Federated Rail Data Space requires secure, reliable and trusted mechanisms for exchanging data across organisational boundaries while preserving data sovereignty and interoperability. This deliverable investigates the suitability of IDSA-compliant connector technologies as a technical foundation for such an environment. Rather than developing a proprietary connector solution, the work evaluates, configures, integrates and validates an existing EDC-based implementation within the MOTIONAL Federated Rail Data Space. The connector layer complements the metadata broker and application services developed in Deliverables D31.2 and D31.3 and provides the technical basis for interactions between participating organisations.

The work follows a structured implementation and evaluation methodology comprising requirements analysis, technology selection, configuration and integration, demonstration and validation, and evaluation and lessons learned. The requirements analysis considered representative railway use cases, data space principles, relevant regulations and existing reference architectures. Based on these requirements, existing connector technologies were assessed with respect to interoperability, maturity, extensibility and alignment with IDSA principles. EDC-based connectors deployed within the T-Systems LivingLab were selected and integrated with complementary data space services, including the metadata broker and App Store. The implementation was subsequently evaluated through representative railway use cases derived from WP26, covering participant authentication, metadata publication and discovery, contract negotiation, policy enforcement, secure data transfer and interoperability between federated participants.

The validation confirmed the successful deployment and operation of the connector technology and demonstrated the principal functions required for federated railway data exchange, including secure participant authentication, metadata publication and discovery, policy-controlled access, contract negotiation, trusted data transfer and interaction with complementary data space services. The results further indicate that mature, standards-based connector technologies can provide the required technical foundation without the need to develop proprietary connector middleware. At the same time, the validation identified limitations regarding real-time dynamic data transmission, while the controlled LivingLab setting limits the conclusions that can be drawn regarding large-scale operational performance, scalability and production readiness.

Overall, the work demonstrates that the further evolution of Federated Rail Data Spaces should focus not only on connector technology, but also on integration, governance, semantic interoperability and organisational onboarding. The deliverable therefore recommends continued use of open and interoperable connector technologies while directing future development efforts towards domain-specific interoperability, larger-scale deployments, automated onboarding and cross-data-space interoperability.

2. Abbreviations and acronyms

Abbreviation / Acronym	Description
API	Application Programming Interface
AWS	Amazon Web Services
B2B	Business-to-Business
CA	Certificate Authority
DAPS	Dynamic Attribute Provisioning Service
DCAT	Data Catalog Vocabulary
DCAT-AP	DCAT Application Profile
DCP	Decentralized Claims Protocol
DID	Decentralized Identifier
DIH	Data Intelligence Hub
DPF	Data Plane Framework
DSP	Dataspace Protocol
EDC	Eclipse Dataspace Components
EDI	Electronic Data Interchange
EU	European Union
FA	Flagship Area
FP	Flagship Project
GA	Grant Agreement
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
IATP	Identity and Trust Protocol
IDSA	International Data Spaces Association
IDSCP	IDS Connector Protocol
IoT	Internet of Things
JKS	Java KeyStore
JSON	JavaScript Object Notation
JSON-LD	JSON for Linked Data
JWS	JSON Web Signature
JWT	JSON Web Token
KPI	Key Performance Indicator
MAWP	Multi-Annual Work Programme
MQTT	Message Queuing Telemetry Transport
MVD	Minimum Viable Dataspace
OCI	Open Container Initiative
ODRL	Open Digital Rights Language
OPC-UA	Open Platform Communications Unified Architecture
PKCS#12	Public-Key Cryptography Standards #12
RAM	Reference Architecture Model
RDF	Resource Description Framework
REST	Representational State Transfer
SI-Token	Self-Issued OpenID Connect ID Token

SLA	Service Level Agreement
TLS	Transport Layer Security
TT	Transversal Topic
VC	Verifiable Credential
VP	Verifiable Presentation
WGS84	World Geodetic System 1984
WP	Work Package

3. Background

The European railway sector is a cornerstone of mobility across the continent, facilitating the movement of passengers and goods in an efficient, sustainable, and cost-effective manner. However, as the industry embraces digital transformation, the need for secure, interoperable, and governed data exchange has become increasingly evident.

The objective is to create a federated data ecosystem where different stakeholders—rail operators, infrastructure managers, and suppliers—can seamlessly exchange data on the basis of contracts while preserving data sovereignty, ensuring security, and maintaining a level playing field. The data itself remains sovereign to the provider at all times. This is guaranteed by the federated principle of the software architecture, creating a decentralised data ecosystem with distributed rights and obligations between all participants. The International Data Spaces Association (IDSA) provides a standardized approach to trusted, secure, and decentralized data sharing through its Gaia-X [1] and International Data Spaces (IDS) compliant architecture [2]. This framework ensures that all participants in a data ecosystem (e.g., the rail domain) can share digital resources while maintaining full control over their data. An IDSA-compliant Rail Data Space aims to implement this concept within the railway industry, fostering a more integrated and data-driven ecosystem. In this document, a demo version is presented that was developed in *WP 31 Federated Dataspaces*, which was part of the Digital Enabler Works Stream 2 of FP1 Motional or also called *Transversal Topic: Digital Enablers* (TT) as identified in Section 7.8 of the Multi-Annual Work Programme (MAWP).

Another work package of the TT was *WP26*, which focused on creating a repository of possible use-cases from all FAs. In *WP27*, *WP28* as well as *WP29*, selected use-cases were developed further, while *WP30* discussed and refined ontologies for the selected use-cases. An overview is contextualized in Figure 1.

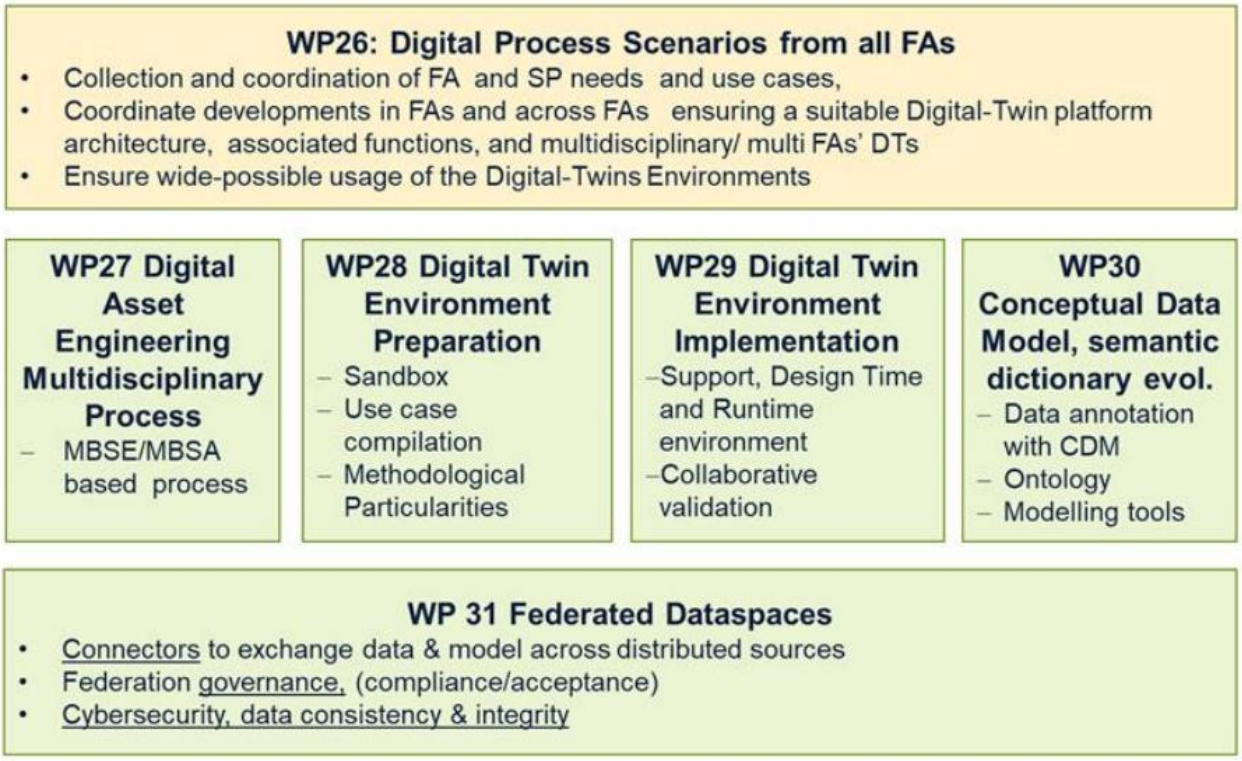


Figure 1. Overview on FP1 work packages associated with the TT

All these work packages are connected in the rail data space, which can deliver the data needed to run the use cases. Within this rail data space, the technologically secure and structurally sovereign networking of domain players - including operators, suppliers, maintenance companies and authorities - allows them to share and utilise their data and services based on contracts. The data itself always remains under the provider sovereignty. This is guaranteed by the federated principle of the software architecture, creating a decentralised data ecosystem with distributed rights and obligations between all participants. Thus, it will serve as basis for the implementation of use cases such as integrated ticketing, exchange of track and train diagnostic data, carbon footprint and emissions tracking, cross-company product lifecycle tracking, freight traceability and tracking.

Of course, a data space is not the only option of transferring data between participants. Table 1 shows a comparison between some commonly used methods: data space, Direct Business to Business (B2B) connections via EDI or API and a centralised platform, i.e. a data lake.

The data space combines the advantages of federated solutions and centralised approaches.

Table 1: Comparison between Data Space, B2B, and Data Lake approaches

Criterion	Data Space	Direct B2B	Data Lake
Data Storage	At each party	At each party	Centralized
Data Sovereignty	Distributed	Distributed	Centralized

Single point of failure	None inherent	None inherent	Yes
Lock-in risk	Low	Medium–High	High
Discovery	Federated catalogues	None ("who knows whom")	Centralized catalogue
Scalability	High	Low	High, but bottlenecks
Trust & identity	Centralized	Bilateral trust	Centralized
Standardization & Principles	Centralized	Fragmented and bilateral	Centralized
Governance	Centralized	Fragmented and bilateral	Centralized

To develop, update and extend all necessary software features as well as to implement and test use-cases, a data space sandbox was provided by T-Systems called the T-Systems LivingLab. Based on this implementation, there were the following key components for the IDSA-compliant rail data space identified:

- **Participants** can be either data provider or data consumer. Participants are connected to the data space via connectors.
- **Offers** consist of *Assets* and *Policies*. Assets contain the meta data and a link to the actual data (which can be any kind of file, including models, instructions or service orders), while policies manage access and usage of the data (e.g. time-restricted or project-restricted), as defined by the data provider.
- **Standardised connectors** are software components for secure and trusted data exchange across all participants in the federation – using IDSA-provided sample code, reference implementations, testbed services for interoperability compliance, technical specifications, starter-kit and co-creation platform. This is presented in the current document.
- **The Meta-data broker,** i.e. a comprehensive data catalogue, that contains machine-readable semantic descriptors of digital resources participating in the federation that are published by resource providers enabling resource discovery by resource consumers. This is presented in Deliverable *D31.2 IDSA-compliant meta-data broker and discovery services in federated data space*.
- **The App-Store** as searchable repository of packaged software-components, such as compiled Digital Twin Functional Mock-up Units, common domain ontology graph developed in work package CDM, and semantic automated cross-format converters according to the common domain ontology. This is presented in Deliverable *D31.3 IDSA-Compliant App Store in federated data space*.
- **The Governance Body** defines the standards and principles on which the data space operates. It is also responsible for the definition of the commercial framework and supervises qualification and performance of the operating company

- **The Operating Company** develops the core services of the data space, e.g. registration, connectors or meta data broker. They also offer onboarding services for future participants.

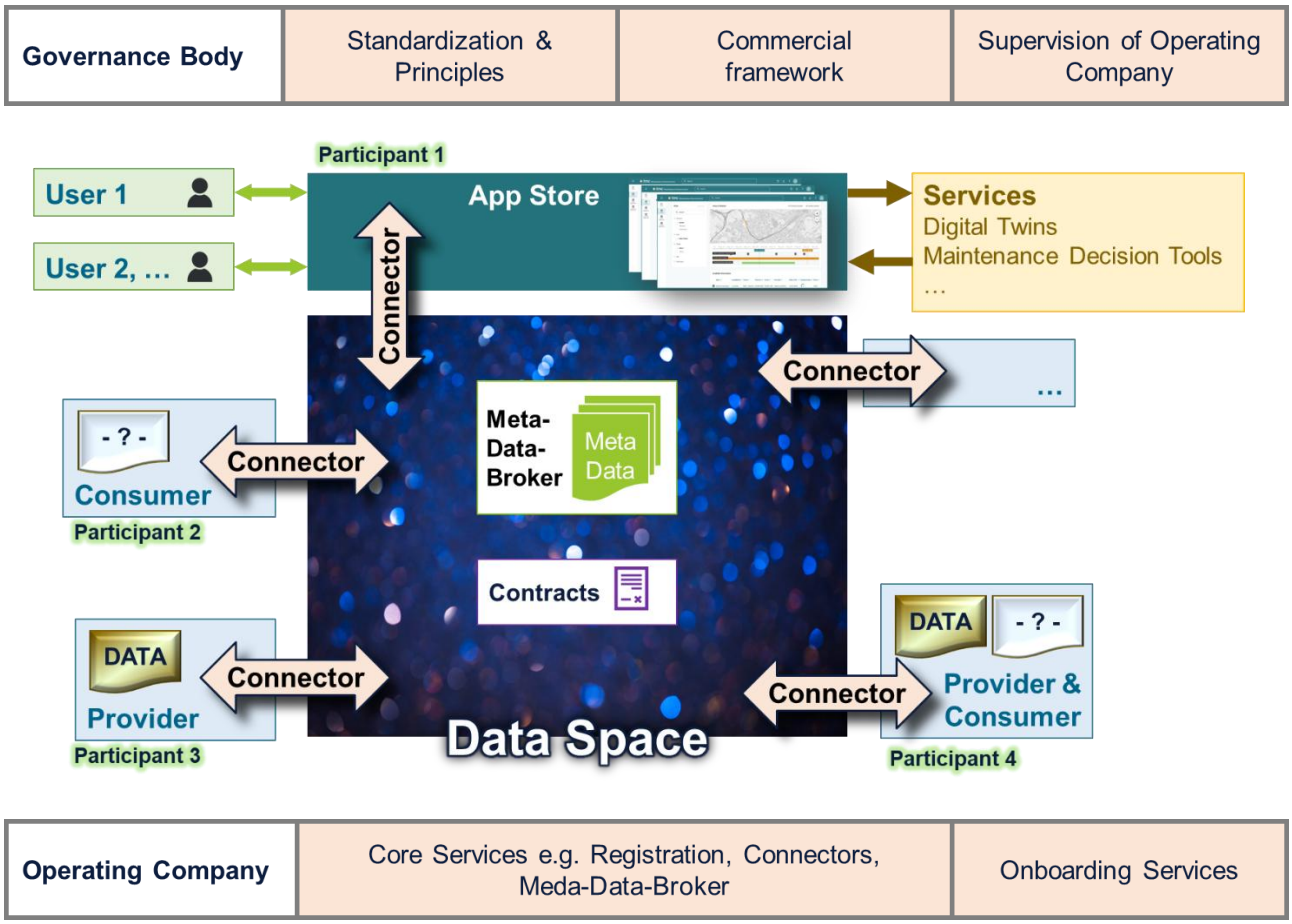


Figure 2. Full overview of the Rail Data Space

A full overview of the Federated Rail Data Space is given in Figure 2. It is envisioned as a federated and interoperable data ecosystem to address these challenges by facilitating a secure, transparent, and trusted data exchange. Adhering to IDSA principles and aligned with the European Data Act and EU Strategy for Data, it ensures that all participants can share data without compromising ownership rights or security.

4. Objective/Aim

This document describes Deliverable *D31.4 – IDSA-compliant Connectors for secure, reliable and trusted data exchange in federated data space*, as defined in the Grant Agreement *GA 101101973*, and explains its purpose, implementation approach and limitations within the context of the MOTIONAL project.

Within Work Package 31, data space connectors represent the fundamental technical building block enabling sovereign, secure and interoperable data exchange between participants of the Federated Rail Data Space. Rather than acting as simple communication interfaces, connectors implement the technical mechanisms required for participant identification, metadata publication, policy enforcement, contract negotiation and controlled data transfer while ensuring compliance with the principles of data sovereignty established by the European Data Strategy and the IDSA.

The objective of this deliverable is therefore not to present the development of a new connector technology. Instead, it documents the evaluation, selection, configuration, integration and validation of an IDSA-compliant connector implementation based on EDC within the MOTIONAL Federated Rail Data Space. The deliverable describes the technical rationale behind the selected implementation, the adopted architectural approach, the deployment within the T-Systems LivingLab environment and the practical experience gained during the implementation and validation of railway-related data exchange scenarios and use cases.

The connector implementation follows the architectural foundations established in *Deliverable D31.1 – Federated Data Space "Sandbox Environment" Description*, where the LivingLab environment was introduced as the common experimentation platform for Work Package 31. Rather than developing and maintaining an independent connector implementation, MOTIONAL also adopts an existing IDSA-compliant technology stack to ensure compatibility with the rapidly evolving European Data Space ecosystem while allowing the project to concentrate on the evaluation of connector technologies within railway-specific use cases.

Within the overall Rail Data Space architecture, the connector constitutes one of several complementary technical components. While Deliverable *D31.2* addresses metadata brokerage and discovery services and Deliverable *D31.3* focuses on the application layer represented by the App Store, the present deliverable concentrates on the connector layer that enables secure and trusted interaction between federated participants and provides the technological basis for all subsequent data exchange processes.

The implementation and deployment activities described in this document therefore focus on the following objectives:

- evaluating the suitability of IDSA-compliant connector technologies for railway data sharing scenarios;
- implementing and configuring EDC-based connectors within the MOTIONAL LivingLab environment;
- integrating connectors with complementary Rail Data Space services, including metadata brokerage and application services (see *D31.2* and *D31.3*);
- validating secure, reliable and trustworthy data exchange through representative railway use

cases;

- analysing the practical strengths, limitations and deployment considerations of connector technologies in the context of a Federated Rail Data Space; and
- deriving recommendations and lessons learned for the future evolution of interoperable European Rail Data Spaces.

Figure 1 places Deliverable *D31.4* within the overall Digital Enabler Work Stream and illustrates its relationship with the remaining TT. Building upon the architectural foundations established in *D31.1* and the complementary services described in *D31.2* and *D31.3*, the present deliverable documents how connector technologies were applied and evaluated as the central technical enabler for secure and sovereign data exchange throughout the MOTIONAL Federated Rail Data Space.

5. Methodology

The work presented in this deliverable follows a structured implementation and evaluation methodology reflecting the overall approach adopted in Work Package 31 for establishing a Federated Rail Data Space. Rather than developing a new connector technology, the methodology focuses on the assessment, configuration, integration and validation of an existing IDSA-compliant connector implementation within representative railway data sharing scenarios.
The methodological approach builds upon the architectural foundations established in Deliverable *D31.1* and complements the metadata broker (*D31.2*) and App Store (*D31.3*). It consists of five consecutive and partly integrated phases, progressing from requirements analysis towards practical validation and evaluation.

1. *Requirements Analysis*
   The first phase identified the functional and technical requirements for secure, trustworthy and interoperable data exchange within the railway domain. This included the analysis of representative railway use cases, European data space principles, relevant regulations and existing reference architectures in order to derive the capabilities required from the connector technology. The requirement analysis is linked to Section 8.1 and Annex A and Annex B on interactions with other Flagship Projects as well as the connection to WP26 and the use case repository where technical and functional requirements were extracted (see Use Case Annex).

   The following Table 2 provides a retrospective mapping of the system requirements identified from the MOTIONAL railway use cases (Annex A) and the system requirements matrix compiled during Wave 1 to the capabilities of the EDC-based connector implementation deployed in the T-Systems LivingLab:

Table 2. System Requirements and Coverage in MOTIONAL

No	System requirement	EDC coverage
1	Heterogeneous datasets support	EDC implementation supports several data planes for different types of data and heterogeneous sources (Azure Blob Storage, AWS S3 and HTTPS/API). D31.4 identifies real-time dynamic transfer as a limitation; not all transfer modes are validated (Section 8.1, 8.5).
2	Architecture framework (EDC)	EDC-based connectors were selected and configured in the T-Systems LivingLab (Section 5–7). D31.4 documents the selected implementation, not a comparative ranking of alternatives (*see also D31.1*).
3	Adaptability of Metadata Broker	EDC catalogue/discovery functions (federated catalogue) are used and demonstrated (Section 7, 8.3).
4	Connector CRUD via Azure, AWS, HTTPS (Agnostic data integration and aggregation functionality)	CRUD management via the EDC management API and Azure/AWS/HTTPS data planes are identified. D31.4 reports a selection of file-exchange tests (Section 8.1).
5	Catalogue services	EDC Connector provides a catalogue service. Offers can be published and partner catalogues browsed; metadata publication/discovery is shown (Section 7.2–7.3, 8.3).
6	Cyber security of	Security configuration and protected transfer are covered in Section 7.5.

	connectors	
7	Policy specification language (e.g Open Digital Rights Language (ODRL)	Offer policies and contract negotiation are covered in Section 7.2–7.3 (standard offered by EDC).
8	IoT devices integration and interoperability	Protocol-specific (e.g. AAS/OPC-UA over HTTPS or Kafka); EDC distinguishes between data and control plane, data planes can be added to the connector architecture.
9	User management	EDC fully supports user management. Keycloak is used for user- and group-based connector access (Section 7.2).
10	Standardized communication protocols with connectors and IoT devices	DSP and DCP/IATP are discussed in Section 6–7. Validation covers participants within the T-Systems LivingLab, not federation between separately operated data spaces.
11	Privacy-preserving measures (data access control, integrity verification, and user permissions-based SSI, privacy-preserving digital identity system)	Section 7.5 covers TLS/CA, DCP/IATP, DID/VC verification, ODRL policies and audit logs. Storage and credential-lifecycle patterns are described.
13	Transparency	Section 7.5 describes integrity-protected logs for access decisions, data access and configuration changes. Activity on the EDC is logged and made available to authorized users via dashboards.

It is intended to clarify the extent to which the selected implementation addresses the identified requirements, rather than to reconstruct an initial comparison of alternative connector technologies. The requirements cover supported data types, source and sink interfaces (Azure Blob Storage, AWS S3 and REST APIs), and different transfer modes, including on-demand, periodic and manually triggered transfers. Interoperability is specified primarily in terms of connecting heterogeneous sources and sinks. Support therefore depends on the compatibility and configuration of the corresponding data-plane interfaces. Security, reliability and trust requirements are discussed in Sections 6.2 and 7.5, while Section 8 provides the implementation and validation evidence.

2. *Technology Selection*
   Based on these requirements, existing connector technologies were evaluated with respect to interoperability, maturity, extensibility and alignment with the European Data Strategy and IDSA principles. The assessment resulted in the selection of EDCs deployed within the T-Systems LivingLab as the technological foundation for the MOTIONAL Rail Data Space (see *D31.1*). The technology selection grounds on D31.1 and the state-of-the-art connector and data space technology introduced in section 6.
3. *Configuration and Integration*
   The selected connector implementation was subsequently configured and integrated into the MOTIONAL Federated Rail Data Space. Activities focused on participant onboarding, connector configuration, policy definition and the integration with complementary data space services, including metadata brokerage and App Store developed within Work Package 31. The configuration

and integration activities done in WP31 are described in section 7 as well as further-leading explanations on usability aspects.

4. *Demonstration and Validation*
   The configured environment was evaluated through representative railway use cases derived from *WP26 - Digital Process Scenarios from all FAs* and executed within the LivingLab environment. The validation assessed the connector lifecycle, including participant authentication, metadata discovery, contract negotiation, policy enforcement and secure data transfer, while verifying interoperability between federated participants. Additionally, the results were presented at a Digital Foundation Demonstration event and were as well evaluated by external domain experts after a joint WP31 Validation Event. This methodology step is linked to section 8 which is about the validation of the results within this WP31 and the related tasks.

5. *Evaluation and Lessons Learned*
   The final phase consolidated the experience gained during implementation and validation. Besides technical observations, the evaluation considered interoperability, deployment effort, operational aspects (see use cases) and organisational challenges encountered during the application of connector technologies. The resulting lessons learned provide recommendations for future production-oriented Rail Data Spaces and form the basis of the conclusions.

6. Connector Technologies for Federated Rail Data Spaces

As introduced in the previous chapters, the Federated Rail Data Space established within Work Package 31 provides the technological foundation for connector-based secure, interoperable and sovereign data exchange between railway stakeholders. While Deliverable D31.1 defined the overall sandbox environment and Deliverables D31.2 and D31.3 address complementary services such as metadata brokerage and application provisioning, the present chapter focuses on the connector technology.

Within a federated data space, connectors constitute the primary technical interface between an organisation's internal information systems and the external federation. They enable data providers and consumers to discover digital resources, negotiate access conditions and exchange information while preserving data sovereignty and ensuring compliance with common governance principles. Consequently, connectors represent one of the core technical enablers of the Federated Rail Data Space and provide the foundation upon which all subsequent data exchange processes are built.

This chapter introduces the technological concepts underlying data space connectors and explains how these concepts are reflected in the IDSA-aligned architecture adopted within MOTIONAL. The objective is to establish the technical background for the requirement-based technology selection, connector implementation, and validation activities presented in the following chapters.

6.1. Federated Architecture and Connector Component for Rail Data Space

The federated infrastructure of data spaces refers to the decentralized approach to creating data ecosystems in which data is not brought together in a central location but remains in its original sources. The access, use and exchange of data is enabled by standardized protocols, metadata and security mechanisms. Data spaces follow the principle of decentralization, meaning only metadata describing the data (products) is used to provide match-making services for data providers and data consumers [1, 2]. This architecture forms the infrastructural basis that enables participating parties to exchange data in a secure, transparent and trustworthy manner. The focus here is on data sovereignty, which is implemented and ensured through the semantic and technical formalization of data usage conditions [3]. In this way, data is only transferred once a consensus has been reached on data usage and compensation [2].

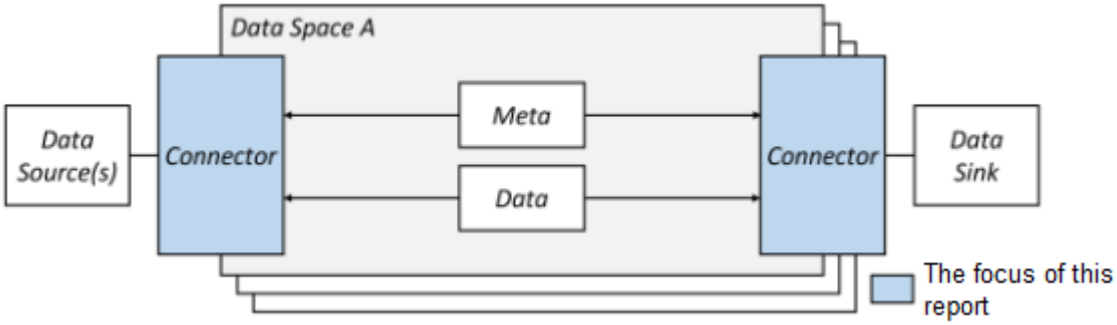


Figure 3. Data exchange within a data space extended from [4].

Federated systems give participants increased autonomy and self-determination [5], so that they have control over their own data and can define the conditions for its use. This contrasts with data integration models with central instances that could sell data to third parties without authorization as intermediaries [6]. In this context, federations can be defined as heterogeneous, loosely coupled associations of autonomous actors that form and share a virtual usage level in a data space through the provision of infrastructure services and the implementation of interoperability mechanisms [7, 8].

The connector (see Figure 3) is a software component of the federated infrastructure and serves the participants as a gateway to the data space in order to access data according to common rules [1, 4]. The connector automatically authenticates the connected entities and authorizes them by controlling and enforcing data exchange policies. By interfacing with a connector, many data endpoints can build a distributed network for data and metadata exchange, providing secure, interoperable, and sovereign data exchange [9]. In each connector are defined rules (i.e. policies) that the other connectors must fulfil to use its data. The connectors can be seen as the gatekeepers between data and internal infrastructure and the data space.
Furthermore, the connectors load and execute data applications that encapsulate data processing or transformation services. Thus, participants in a data space can technically control, at their connectors, to what extent and with what accuracy their datasets can be used by other participants [10], creating a very flexible mechanism for offering data. As the requirements for data exchange in a dataspace vary by regulatory area, business, and application, so do the requirements for the connector in terms of resource consumption, efficiency, and cybersecurity [9].

6.2. Technical Connector Properties and Core Functions

Table 3 represents technical connector properties:

Table 3. Technical Connector Properties

Property	Description
IDSA conformity	Compliance with the IDS Reference Architecture Model for secure data sharing
Decentralized architecture	Avoidance of centralized data storage; each participant manages its own data.
Semantic interoperability	Use of ontologies and data models (RDF, JSON, etc.) for the standardized description of data.
Extensibility	Support for services, APIs and platforms. Functionality can be extended by adding services for data processing before delivering it.
Compliance with EU regulations	GDPR, Data Act, etc. for data protection and cyber security.
Flexibility and scalability	Support for Docker, Kubernetes and cloud-native deployments.

The requirements introduced above are realised through a coherent set of functional capabilities integrated within data space connectors. Connectors orchestrate the complete lifecycle of sovereign data exchange, beginning with resource publication and ending with monitored and policy-compliant data transfer.

Table 4. Core functional capabilities of data space connectors

Core functions	Connector control plane	Connector data plane
Data provisioning	Catalog & Discovery	
Data access & usage control	Contract Negotiation, Policy Enforcement	
Trusted identity and certificate management	Identity Management	
Interoperability		Data Transfer
Security & encryption		Data Transfer
Decentralized data management	Data Flow Management	

While Table 3 describes the architectural and technical properties of data space connectors, Table 4 operationalizes these properties by mapping them to the core functional capabilities required throughout the data exchange lifecycle.

Connectors consist of a control plane and a date plane. The control plane is responsible for deciding how data is managed, routed, and processed. The data plane is responsible for the actual movement of data between participants after the control plane has negotiated a valid contract,

utilizing secure, often encrypted, protocols.

The following sections describe the fundamental characteristics that connector technologies must fulfil in order to support secure, reliable and trusted data exchange in a federated data space within the railway domain.

6.2.1. Secure Data Exchange

Security is a fundamental prerequisite for every federated data space. As operational, commercial and infrastructure-related information is exchanged between independent organizations, connector technologies must ensure that communication is protected against unauthorized access while preserving confidentiality, integrity and authenticity throughout the complete exchange process.

Within the Federated Rail Data Space, security extends beyond encrypted communication. Connectors provide the mechanisms required to authenticate participating organizations, verify digital identities, establish secure communication channels, and enforce access restrictions defined by data providers. These capabilities ensure that only authorized participants are able to discover and access digital resources.

These mechanisms form an integral part of the connector architecture and establish the technical basis for sovereign and policy-controlled data exchange. The implementation of these mechanisms within the MOTIONAL deployment is described in Chapter 7.

6.2.2. Reliable Data Exchange

Besides security, connectors must provide reliable and predictable operation under distributed conditions. Railway applications frequently require the continuous exchange of operational information across organisational boundaries, making reliability an essential requirement for practical deployment.

Reliability is achieved through the decentralised architecture of the Federated Rail Data Space, where each participant operates its own connector while remaining responsible for its local information systems. This approach eliminates central points of failure and allows individual participants to independently manage scalability, availability and operational maintenance.

Connector implementations further separate control-related functions, such as negotiation and policy management, from the transfer of digital assets. This architectural separation improves scalability, facilitates integration with heterogeneous enterprise systems and supports different communication and transfer mechanisms without affecting the overall interoperability of the federation.

6.2.3. Trusted Data Exchange

Trust distinguishes federated data spaces from conventional information exchange mechanisms. While security protects communication, trust establishes confidence that exchanged data are accessed and used exclusively under mutually agreed conditions.

Connector technologies establish trust by combining technical mechanisms with common governance principles. Through participant identification, policy enforcement, contract

negotiation and verifiable digital identities, connectors ensure that access permissions defined by data providers remain effective throughout the complete lifecycle of a data exchange.
For railway ecosystems involving numerous independent organisations, this trust model enables collaborative data sharing without requiring participants to relinquish ownership or control over their digital assets. Consequently, trusted data exchange forms the basis for sustainable interoperability within the Federated Rail Data Space.

6.3. IDSA-compliant Connectors

Following the introduction of the generic connector principles and capabilities, this section presents the architectural concepts adopted within the MOTIONAL Federated Rail Data Space. Here, MOTIONAL adopts IDSA-aligned concepts and relies on EDC as the technological basis for connector implementation within the T-Systems LivingLab environment. The adoption of an IDSA-aligned architecture ensures interoperability with the evolving European Data Space ecosystem while providing a mature and standardised foundation for secure, sovereign and trustworthy connector-based data exchange. This approach enables the project to concentrate on the practical deployment, configuration and validation of connector technologies instead of developing new middleware components.

The following subsections summarise only the architectural elements relevant to the MOTIONAL implementation and validation activities.

The connector architecture considered in MOTIONAL is aligned with the IDSs Reference Architecture Model and supports secure, controlled and sovereign data exchange.
The Connector Architecture (RAM) uses application container management to separate all components and deploy each of them in a secure and controlled environment. Furthermore, to ensure data privacy, any operation regarding data should proceed as close as possible to the data source. Thus, a connector should run on top of a Virtual Machine/Hardware and an Operating System. Moreover, as it comprises multiple containers, there is a need to create an Application Container Management, isolating components from one another and providing a more secure platform. Finally, a container can comprise a Connector Core Service, which is responsible for Data/Metadata management, Contract/Policy Management, etc. It can also comprise an IDS App, in case it is downloaded from the App Store, or a Custom App, if it is developed by the connector itself [11].

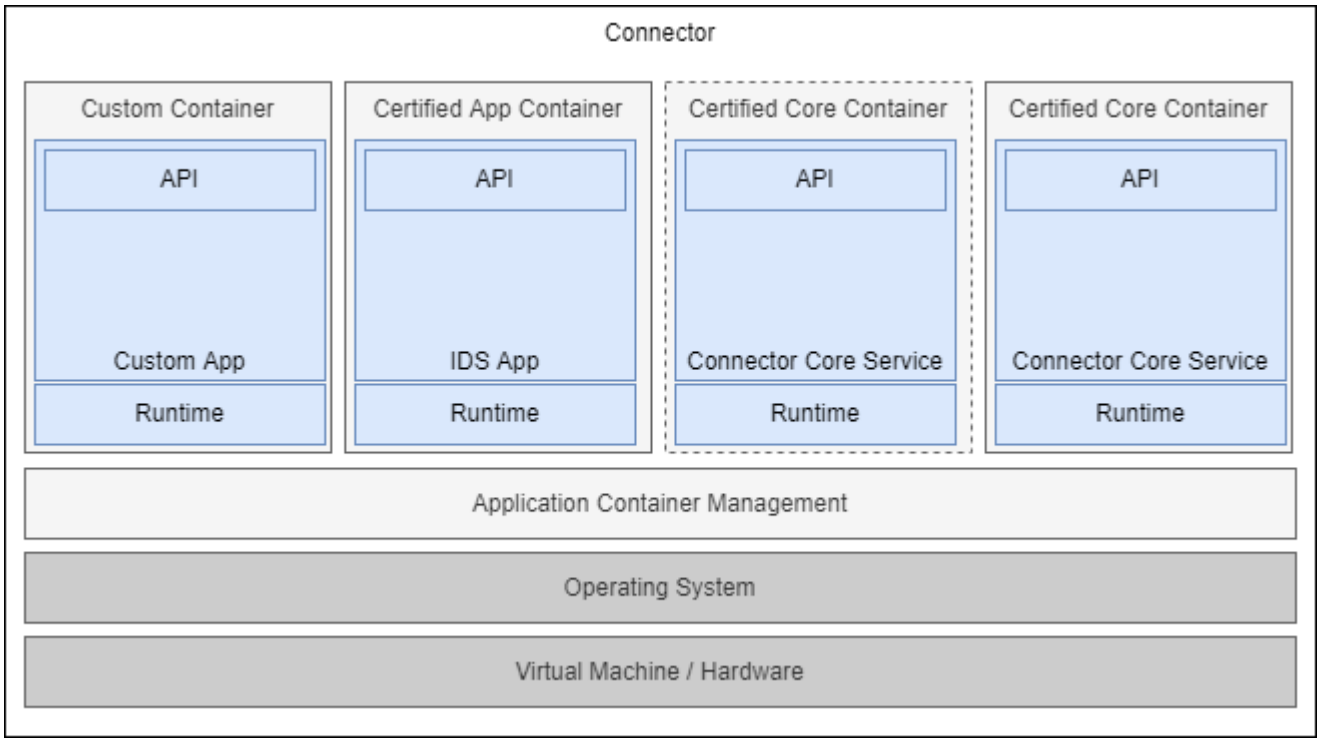


Figure 4. IDS Connector Architecture[1]

Figure 4 illustrates the architecture of a Connector within the IDS framework, highlighting its modular structure, interactions with underlying infrastructure, and support for both certified and custom applications.

This architectural model forms the conceptual foundation for data space connector implementations. While earlier IDS architectures relied on protocols such as IDSCP and centralized trust components such as DAPS, recent data space developments increasingly rely on the Dataspace Protocol (DSP) as a common interaction layer for catalogue exchange, contract negotiation and data transfer. This evolution supports more decentralized and flexible trust models, including the use of Decentralised Identifiers (DIDs) and Verifiable Credentials.

The Eclipse Dataspace Components (EDC) represents the at the time of the project state-of-the-art implementation of the data space connector concept, building upon the principles defined in the IDS-RAM while introducing significant architectural enhancements. EDC provides a modular and extensible framework composed of loosely coupled components, including the connector, federated catalog services, identity management components, and management interfaces[2]. A key architectural characteristic of EDC is the separation between control plane and data plane:

- The control plane manages metadata exchange, contract negotiation, and policy enforcement
- The data plane is responsible for the actual transfer of data between participants

[1] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_2_ids_connector
[2] https://internationaldataspaces.org/idsa-data-space-connector-report

Furthermore, EDC supports protocol-agnostic communication and integrates the Dataspace Protocol (DSP) as the primary mechanism for connector-to-connector interaction, enabling interoperability across different implementations and domains. EDC architectures are designed to support:

- decentralized identity management
- scalable cloud-native deployments
- integration with multiple trust frameworks (e.g. Gaia-X)

The DSP is protocol-agnostic and can be used over HTTPS, MQTT, WebSockets, OPC-UA, or other transport layers. This flexibility makes it suitable for heterogeneous infrastructures, including cloud, edge, IoT (Internet of Things), and OT environments.
A fundamental principle of the IDS is data sovereignty: participants retain full control over their data assets. Connectors enforce this principle by embedding usage policies and contractual agreements directly into the data exchange process. In this way, data providers can ensure that access conditions, obligations, and restrictions are technically enforced and transparently traceable. Connectors also support semantic interoperability through the Vocabulary Hub, allowing coherent interpretation of shared vocabularies and ontologies, such as DCAT, DCAT-AP, and RDF-based models. This ensures consistent understanding of metadata and data assets, even across heterogeneous environments. Furthermore, DSP requires traceable and auditable data exchanges across multiple participants.

Overall, this design enables secure, flexible, and traceable data exchange within the IDS ecosystem, providing the foundation for interoperable and governed data sharing in complex environments, including rail, manufacturing, and other industry sectors.

To integrate heterogeneous information systems into a common federation, connectors expose a set of standardised interfaces supporting both administrative and operational interactions.
Administrative interfaces enable connector configuration, participant onboarding and operational management. Operational interfaces support metadata publication, catalogue queries, contract negotiation and data transfer between participating organisations.
The interoperability of these interfaces is achieved through the adoption of common communication protocols and standardised information models defined within the European Data Space ecosystem. Consequently, organisations remain free to operate heterogeneous internal information systems while participating in a common interoperable federation.
The specific interfaces configured within the MOTIONAL are detailed in Chapter 7 together with the LivingLab environment.

6.4. Application of the IDSA Architecture within MOTIONAL

IDSA provides a standardized approach to trusted, secure, and decentralized data sharing through its IDS architecture[3]. This framework ensures that all participants in a data ecosystem (e.g., the rail domain) can share digital resources while maintaining full control over their data.

Building upon the concepts and principles introduced above, the MOTIONAL project adopted an implementation strategy based on existing IDSA-compliant technologies rather than developing a proprietary connector solution. In this context, EDC-based connectors deployed in the T-Systems LivingLab provided the practical basis for testing connector-based data exchange in railway scenarios.
Within the LivingLab environment, connectors were configured and deployed to interact with complementary data space services including the metadata broker, governance services, and the App Store developed within WP31. Together, these components supported the evaluation of a Rail Data Space. All connectors deployed in WP31 are IDSA-compliant and certified (see Task 31.6).

The following chapter describes the deployment, configuration, and use of connectors within the T-Systems LivingLab environment.

[3] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4

7. Implementation: T-System / The EDC connectors at MotionRail-X

The first version (MotionRail-X) of the Rail Data Space has been hosted in the DIH LivingLab. The LivingLab is part of the T-System "Data Intelligence Hub" (DIH)[4]. The DIH is a cloud-agnostic platform providing managed services for dataspaces and data sharing technology, enabling enterprises to share, process, and analyse data while retaining absolute data sovereignty.

The LivingLab is described by T-System, on their web site:

> "LivingLab is a sandbox with a dataspace, a software development environment to let you focus on use cases and prototyping of apps powered by dataspace capabilities, such as data sovereignty protection – without all the dataspace complexities. Build and enhance expertise in dataspace technology and have the benefits of a managed service. A trustful ecosystem with data sovereignty about shared data an additional trust level through T-Systems Digital.ID. LivingLab is the fast-track to the world of dataspace.
>
> LivingLab provides an end-to-end dataspace experience with a friendly User Interface and allows users to deploy & test various use cases or applications within dataspace environment. Delivered as a pre-configured product, LivingLab eliminates dataspace complexities and allowing users to focus on developing their business applications. Whether upgrading existing apps or creating new ones, LivingLab empowers businesses to benefit from better data."

All connectors used during this project have been hosted on the same platform. T-System provided the most mature and convenient platform to satisfy the general requirements for a rail data space emerged in the early phases of the project. At the same time, they offered a secure environment where the MOTIONAL participants could start the experimentation and exploration phase. Motivations behind the choice of this platform are detailed in D31.1.

The LivingLab architecture is reported in the following figure:

[4] https://dih.telekom.com/en

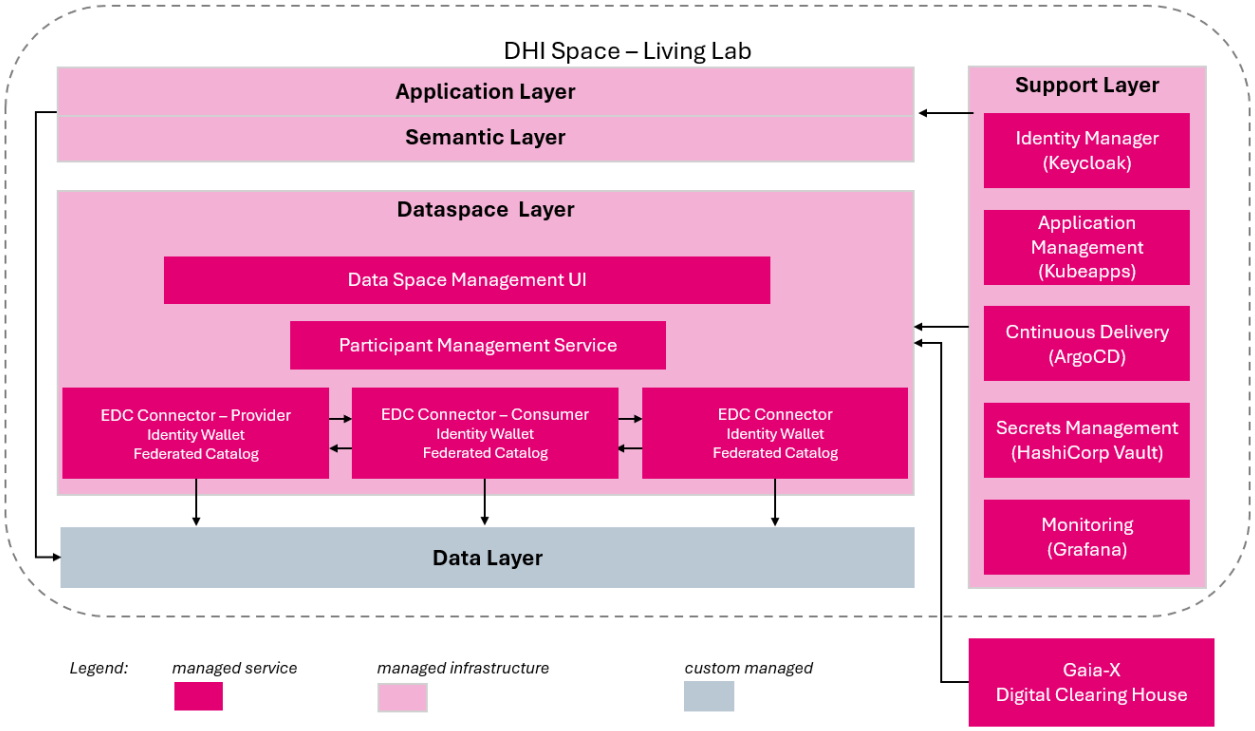


Figure 5. LivingLab architecture, source T-System.

7.1. Connector deployment

The first connector was deployed by T-System to the MotionRail-X data space's owner Knorr-Bremse. After this, the WP31 partners had the opportunity to independently deploy additional connectors; the data space owner would initially have to authorize the organizations as data space participants followed by an onboarding process. Additional connectors were deployed in the T-Systems data space, and after the user requested the data space owning company to activate to make it visible in the shared data space, the onboarding process started. All members of Motional project - Work Package 31 (extended by some cross-FP collaborations), could participate in MotionRail-X by onboarding to the data space. After onboarding, the owner/administrator of the connector can grant access to it to other persons from their respective organization as well as grant rights by defining roles, by assigning personal accounts associated to their e-mail addresses. For deployment and administration, we had access to:

- **Deployment Documentation:**
  T-Systems Connector Deployment Guide at the https://docs.dih.telekom.com/connect-for-livinglab/MVD-Connector-Deployment (restricted access to onboarded participants only)
- **Workshop Reference:**
  Deployment details and application setup were covered in a dedicated workshop by T-Systems. Refer to the T-Systems Workshop documentation for further insights.
- **Kubeapps Portal:**
  All deployed connectors and UI apps (including those from other companies) can be viewed in the Kubeapp portal, there are also visible other companies' applications which are in the same data space. In the next section there are more details on the tools available for managing the connector.

7.2. Working with a connector

The members of a company use their connector in MotionalRail-X to exchange data with the other companies of the same data space.
The access to the connector can take place via web interface or via Rest APIs. The following figure shows the web interface (provided by T-System) associated to the connector for one of our organizations. The access to the web interface requires previous login with the personal account. Access via APIs requires the API-key associated to the organization owner of the connector.

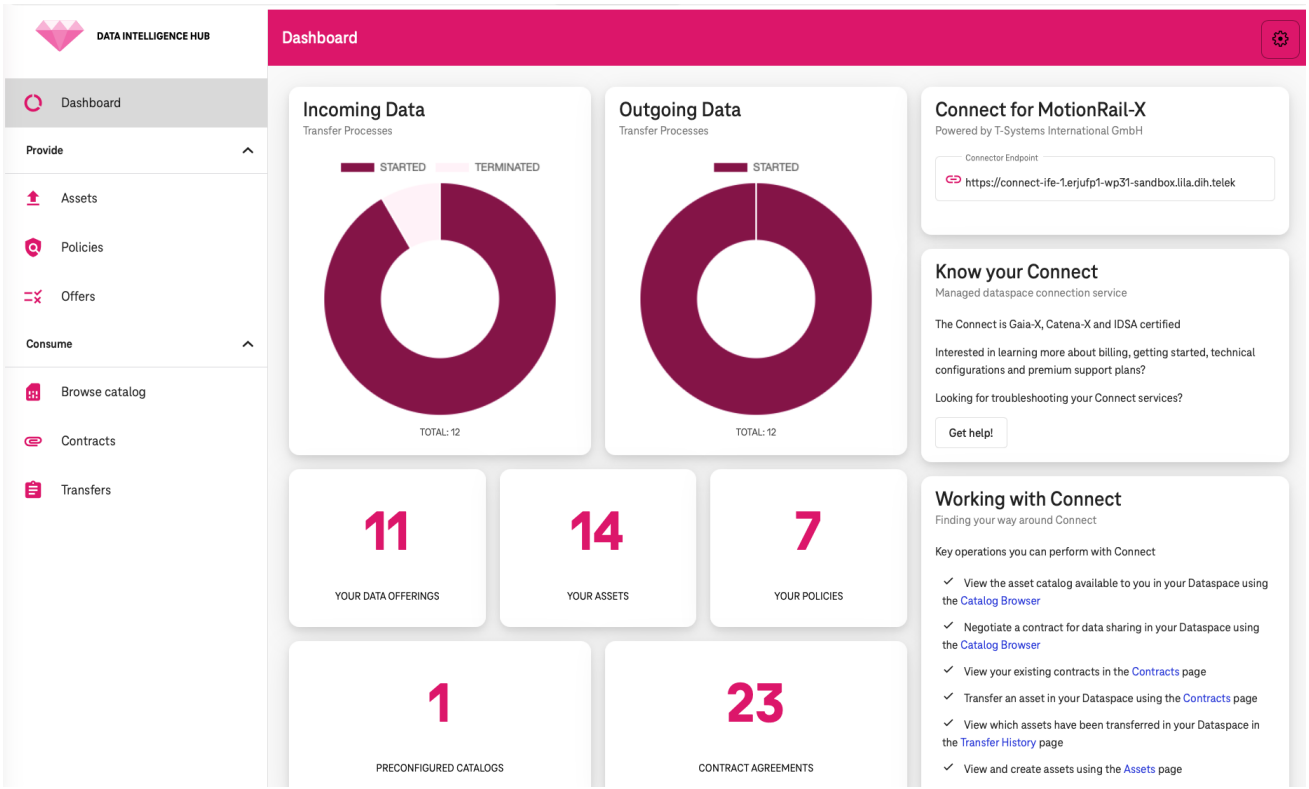


Figure 6. Dashboard associated to a connector for one of the organizations.

On the left of the dashboard are visible the main commands for the provider role: providing assets, defining policies, accessing and using them, for creating offers by associating assets to policies; and for the consumer role: consuming other participants offer. This is done in three steps: browsing other participants' catalogues; select an offer from the catalogue; start the negotiation of a contract and, on the basis of this contract start the data transfer. Section 7.3 presents the process and some of the steps as they appear in the user interface.

Beside the web interface, the connector is available via APIs at the connector endpoint shown on top right of Figure 6. For example, via curl, Participant1 could ask Participant2 for all the currently available offers related to assets containing the string "test", with the following call:

```
curl --request POST \
  --url
https://<Participant1_Connector_Enpoint>/api/management/v2/catalog/request\
  --header 'content-type: application/json' \
  --header 'x-api-key: xxxxxx \
  --data '{
  "@context": {},
  "protocol": "dataspace-protocol-http",
  "counterPartyAddress": "https://<Participant2_Connector_Enpoint>/api/dsp",
  "querySpec": {
    "offset": 0,
    "limit": 500,
    "filterExpression": [
      {
        "operandLeft": "https://w3id.org/edc/v0.0.1/ns/id",
        "operator": "like",
        "operandRight": "%test%"
      }
    ]
  }
}'
```

Administrators of a connector have access to extra tools, summarised in the following figure:

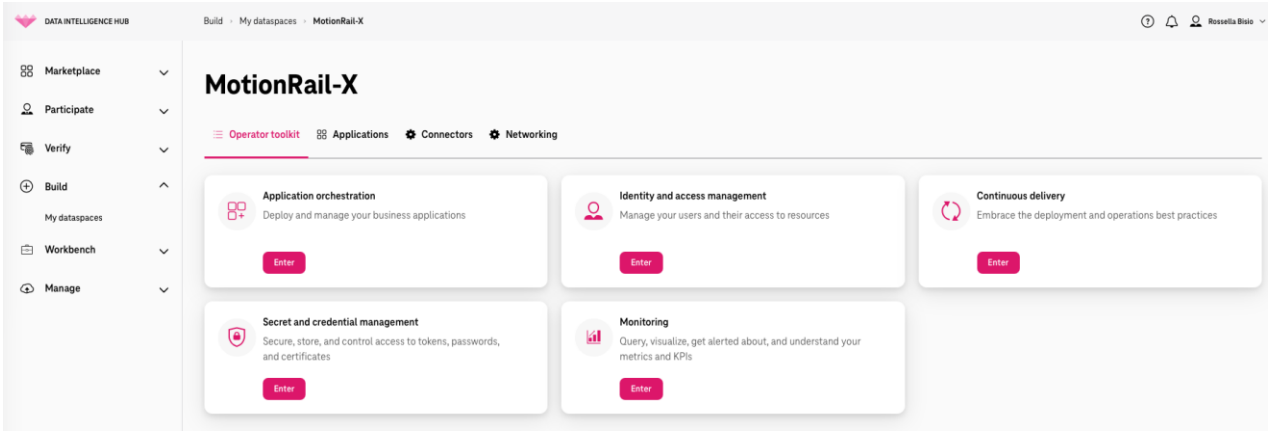


Figure 7. Tools for connector administration provided by T-System

The tools appearing in Figure 7, correspond to the elements in the Support Layer of Figure 5. Entering the ***Application orchestration,*** the user is redirected to the *Kubeapps*[5] environment where they start, stop and configure the instance of the EDC MVD-Connector (the EDC connector version available at the DHI LivingLab).

Keycloak[6] is behind ***Identity and Access management***, used for managing user and group-based

[5] https://github.com/SAP/kubeapps: an in-cluster web-based application that enables users with a one-time installation to deploy, manage, and upgrade applications on a Kubernetes cluster.
[6] https://www.keycloak.org/

access to the connector.

Secret and credential management gives access to an instance of Vault[7], where all sensitive data (e.g., database credentials, tokens, access keys) is securely stored.

Monitoring enters a Grafana web interface presenting data about the traffic to the connector, checking the apps (our connector) status and logs, this is useful when something fails during data transfer).

User Interfaces, API endpoints and modules for connector administration can change with data space and/or connector version.

7.3. Execution of data transfer via connector

Data Exchange in MotionRail-X follows the standard process summarized in those phases, involving the data provider's connector and the data consumer's connector:

1. The data provider publishes a data offer
2. The data consumer finds an interesting offer (for example by searching, functionality offered by clicking on 'browse catalogue' in the dashboard in Figure 6)
3. The data consumer starts the negotiation, carried out by the two connectors, producing in case of success a contract between both
4. With a valid contract the data provider can then trigger the data transfer.

The process of publishing an offer can be summarized in the following figure, it consists in essence, in associating an asset to the policies for assessing it and using the data the asset describes.

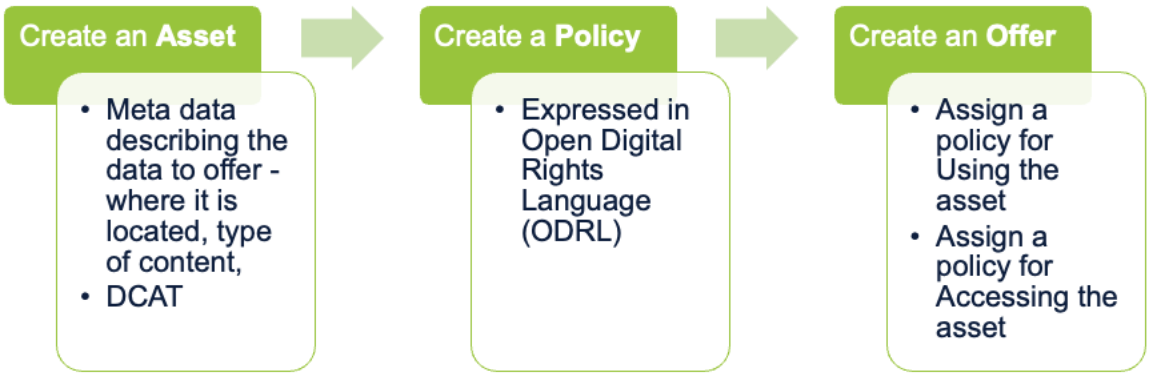


Figure 8. Process for creating an offer

If an asset does not exist yet in the providers' catalogue, it is necessary to create it. Figure 9 show the interface for managing asset for one of our partner's connector:

[7] https://developer.hashicorp.com/vault

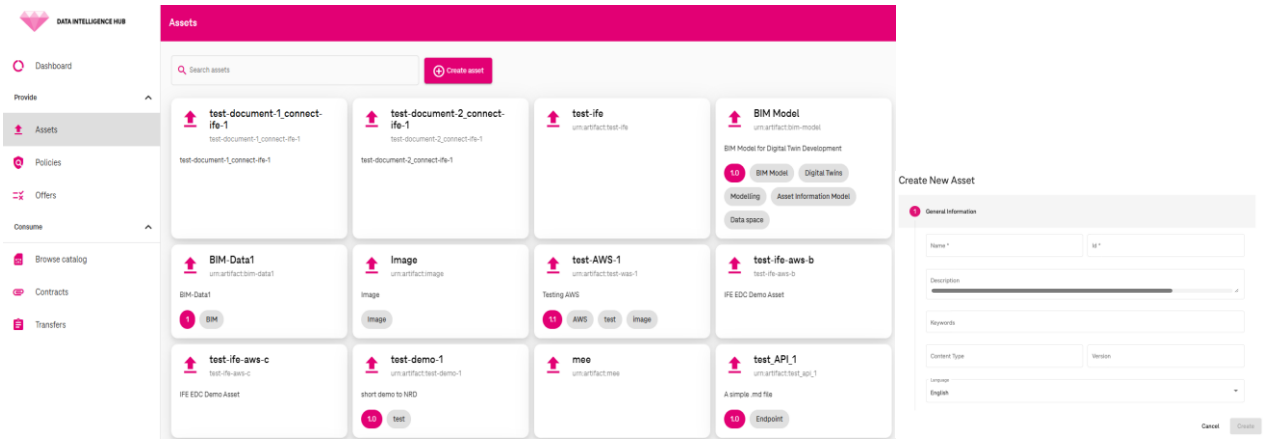
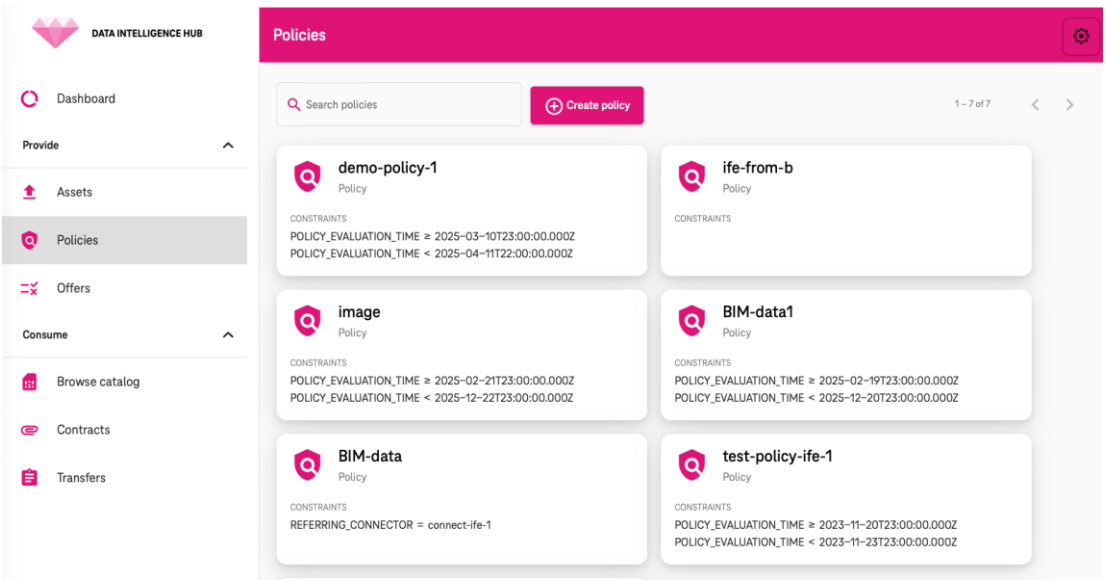


Figure 9. User Interface for managing assets, on the right the pop up window for creating an asset.

An asset is represented by metadata:

- describing the content of the data to share. A subset of the World Wide Web Consortium's Data Catalog Vocabulary DCAT*[8] is used. This information is visible to the public.
- The link on how to access the data, and the credential for accessing: this information is used exclusively by the provider's connector.

A data provider has usually a set of policies defined to share its data, if none of the already defined policies is suitable for the case, new ones must be created. Below, a screen shot of the interface for managing policies and for creating offers, from the connector of one of our partners. Offers are the result of associating to an asset a policy for access and use.



[8] org/TR/vocab-dcat-3

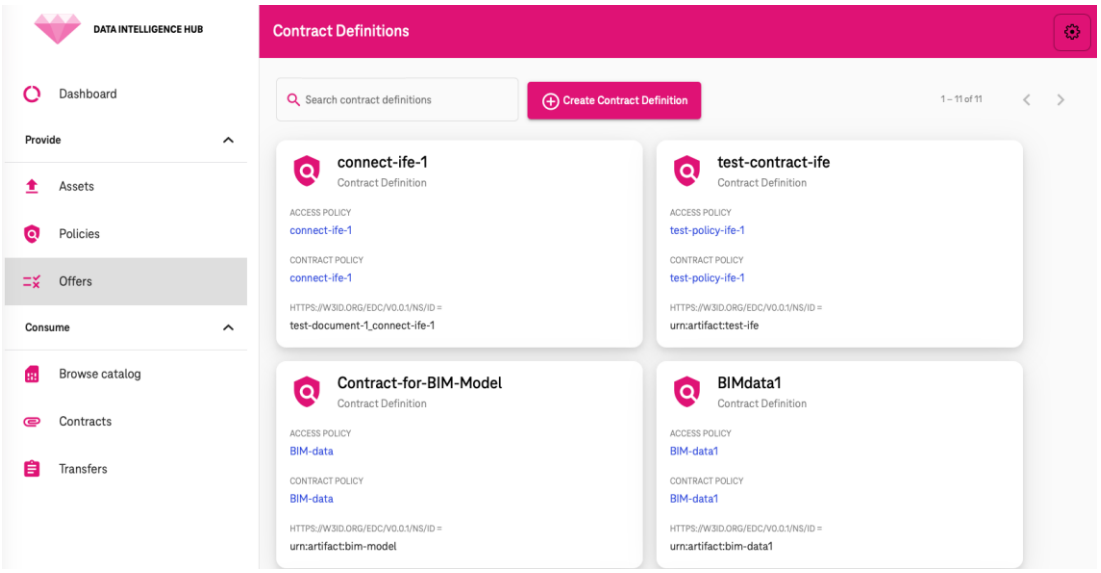


Figure 10. LivingLab interfaces for managing policies and offers/contract definitions.

On the data consumer side, it is possible to navigate among catalogues from other participants. The next figure shows the catalogue offered from one partner as seen from another partner. By clicking on one element in the catalogue, a pop-up window shows more details about the offer and presents a button for starting the negotiation of a contract.

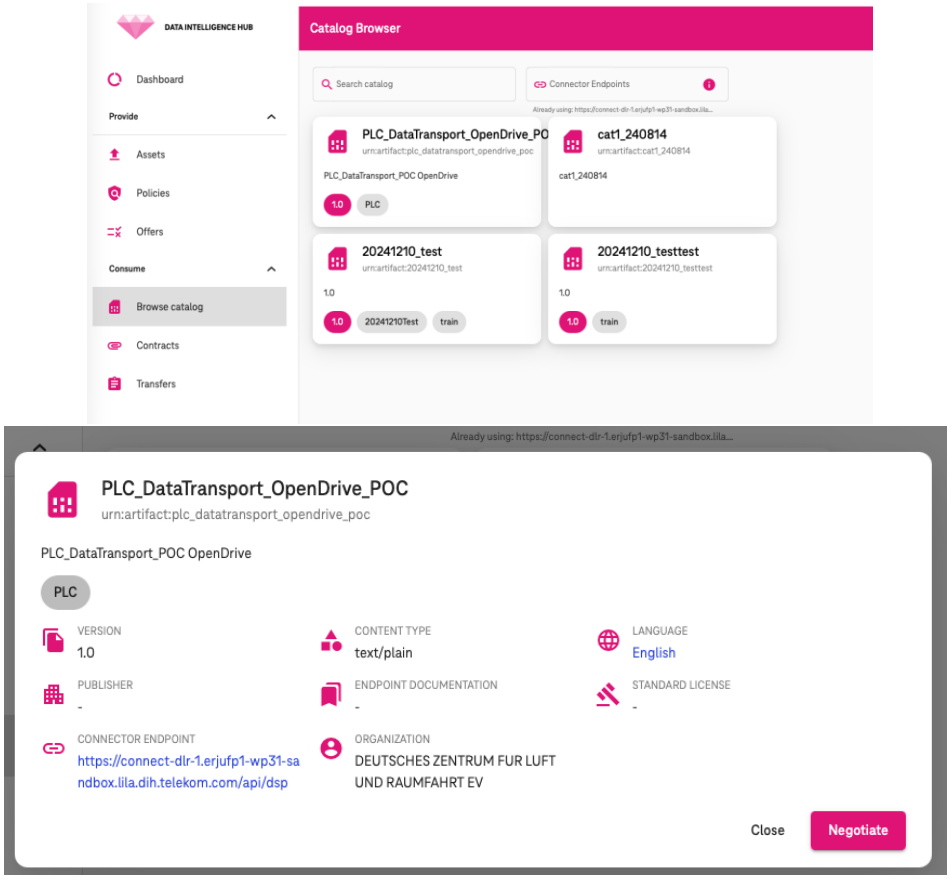


Figure 11. Showing the catalogue of one of our partners

Once an asset of interest has been selected, the processes for negotiation and then transfer can

start, as shown in Figure 12



Figure 12 – Process from negotiation to data transfer

The following figure shows the interface after the successful negotiation for cat1_2400814

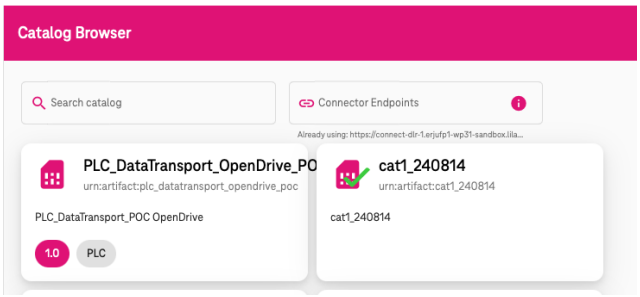


Figure 13. Successful negotiation of test asset

The resulting contract appears then in the list, where it is possible to start the actual data transfer.:

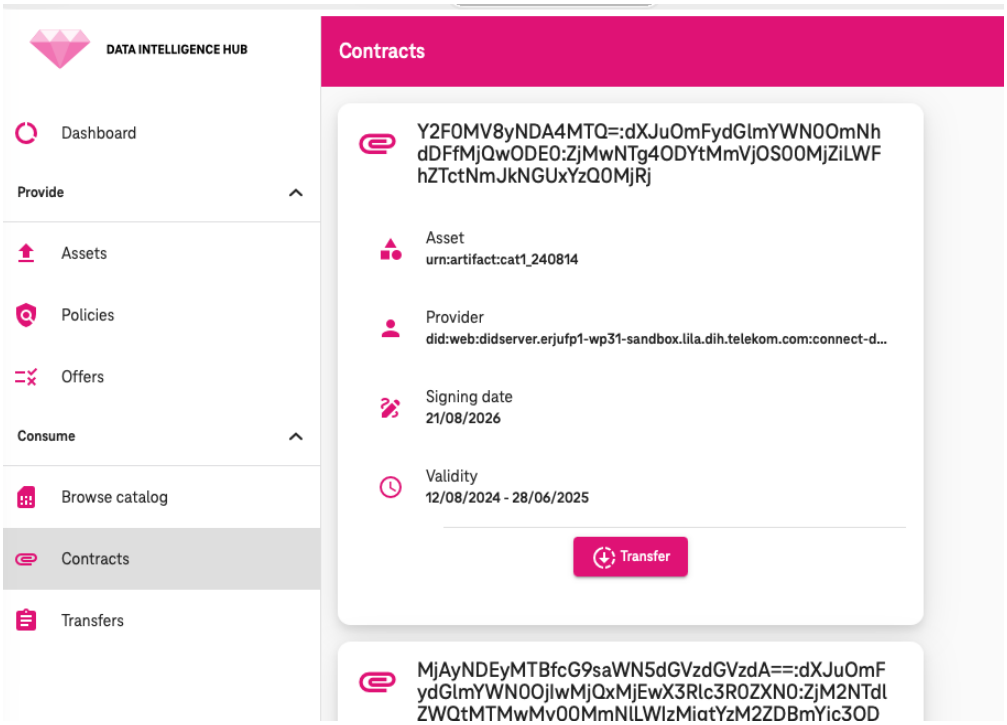


Figure 14. Resulting contract of negotiated data asset

7.4. An example of application

By accessing the connector via APIs, it is possible to develop custom software adding many interesting functionalities. The process can be automated by gathering external data from the data space and sending it to a digital twin, which performs the required computations and subsequently makes the resulting data available in the data space. An example of this process is schematized in the following figure.

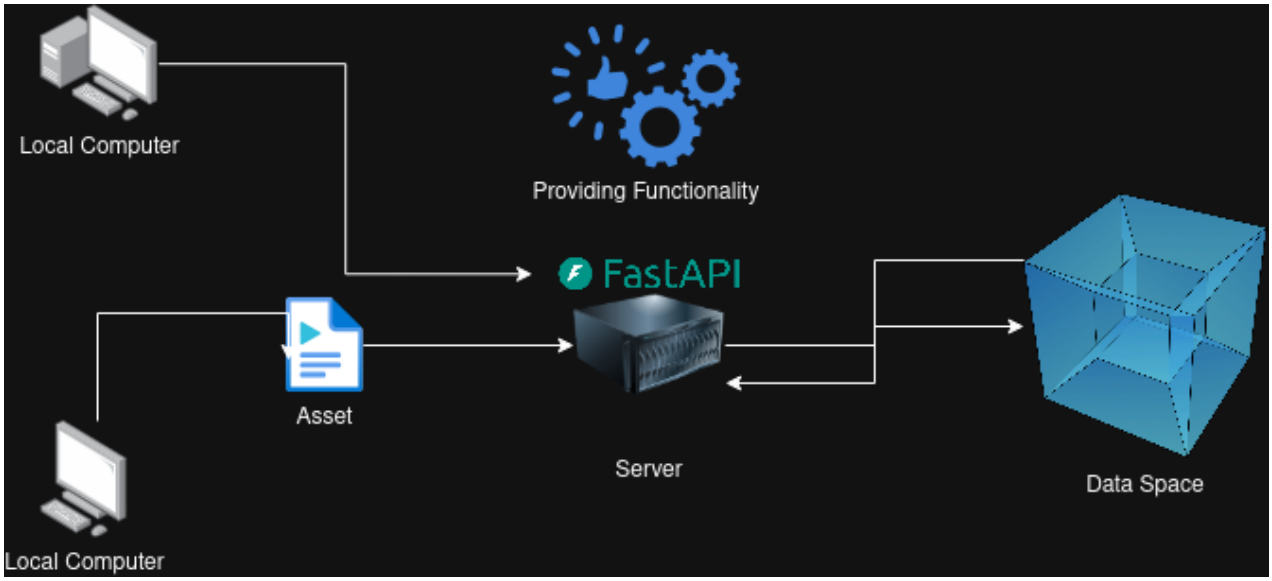


Figure 15. A sketch for an application externalizing advanced computation based on data collected from a data space and providing back the results to the data space.

In the Motional deliverable D31.3 – "IDSA-Compliant App Store" is presented an application working as a searchable repository for packaged software components developed in Motional FP1, such as compiled Digital Twin Functional Mock-up Units, common domain ontology, and semantic automated cross-format converters according to the common domain ontology.
The Data space and its APIs provide the basic functionality, however, for more dedicated use-cases it is necessary to provide a server with additional logic. The webserver with a Fast-API backend has been implemented to enable various logic.

The Motional App Store uses a connector to provide or consume data. It is able to read the information from the meta data broker and to deliver it to either connected automated services or to allow manual access by human users through its front-end GUI. An overview of the app store within the data space context is shown in Figure 15.

7.5. Security, reliability, trust aspects

In the following, aspects of security, trust and reliability in the first version of the rail data space are analysed individually. Figure 16 presents an overview of the components in the Core Service Layer of DHI LivingLab involved in the data transfer. These components and their interactions are referred in the following discussion.

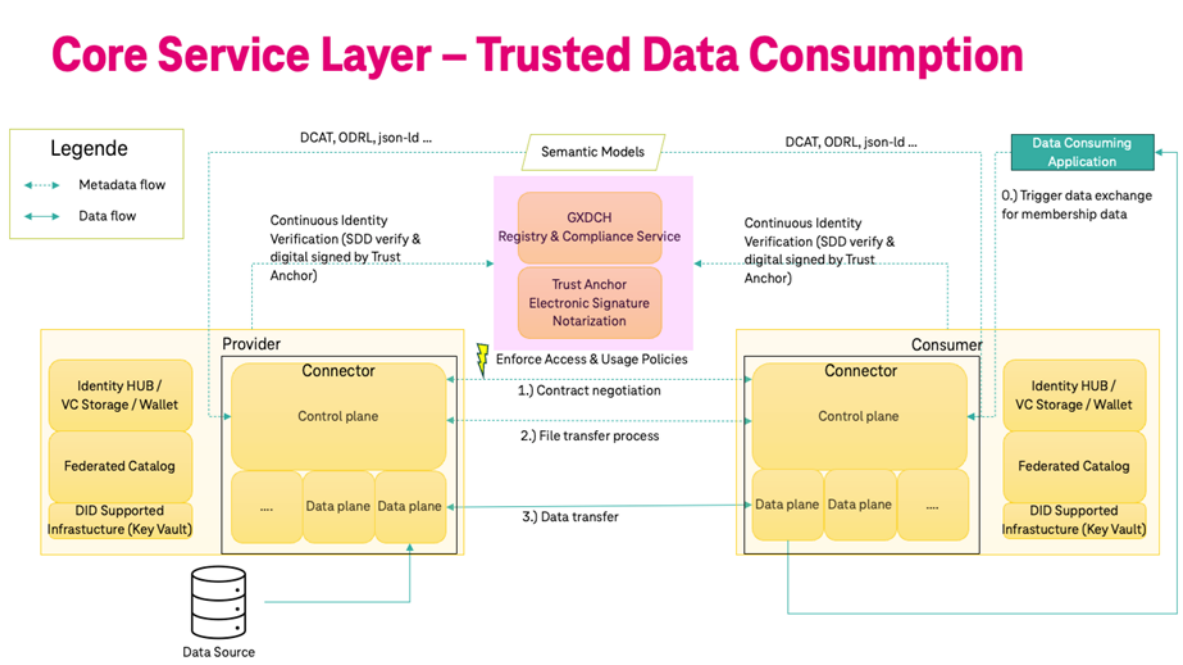


Figure 16. Overview of components involved in data exchange between two connectors. Source T-system.

7.5.1. Secure Data Exchange

In the DIH LivingLab, all connector-to-connector traffic is forced through an *ingress controller*, that terminates Transport Layer Security (TLS)[9], using certificates issued by a trusted Certificate Authority (CA). Plain HTTP listeners are not exposed to the internet, so confidentiality, server authentication and TLS level integrity protection are enforced for every message before it can reach the connector via the Data Security Protocol (DSP). The ingress also acts as a first line of defence against denial-of-service traffic by absorbing and rate-limiting requests at the edge, satisfying the implicit availability requirement for authenticated, encrypted, integrity-protected connector as demanded by the mandatory secure communication protocols (Appendix B/ Security Profile in Reference architecture model – [version 3.0 April 2019] criterion).

On top of TLS, the connector enforces mutual authentication at the DSP layer using DCP/IATP (Decentralized Claims Protocol, former Identity and Trust Protocol). Each participant has a stable identifier expressed as a DID (Decentralized Identifier)[10] (typically did:web or did:key), whose DID Document publishes the verification keys and the URL of the participant's Credential Service. Before issuing or accepting a DSP request, the connector executes a Self-Issued ID Token + Verifiable Presentation exchange:

1. The caller signs a Self-Issued OpenID connect token (SI-Token) with the private key referenced in its DID Document and attaches it to the request.

[9] That ingress controller is a gateway server that decrypts secure HTTPS web traffic from outside a network before passing it along as regular HTTP traffic to internal backend applications.

[10] Special type of globally unique identifier defined by the W3C that lets people, organizations, or objects self-identify without relying on a central authority

2. The receiver resolves the caller's DID, validates the SI-Token signature, and, when the request requires attested attributes (e.g. membership in the dataspace, a specific role, a given level of assurance), pulls the corresponding Verifiable Presentation (VP) from the caller's Credential Service.
3. The receiver verifies the VP, the contained Verifiable Credentials and the issuer signatures against the federation's Trust Anchor list / Trust Framework.

Because the SI-Token is signed per request and the VP is fetched and verified on demand, both parties are cryptographically convinced of the other's identity and current attribute set before any business message is processed — without any central Dynamic Attribute Provisioning Service (DAPS) in the trust path.

When the connector terminates TLS itself — for example in deployments without a managing ingress — it can be configured with a JKS or PKCS#12 keystore for the TLS material, and the corresponding passwords can be supplied through environment variables or a secret store rather than baked into images. The DID signing keys and any wallet material used by the Credential Service are held in a secret backend (Kubernetes secrets, a managed KMS, or an external vault) and are never written to image layers. JWT/JWS algorithms used for SI-Tokens and VC proofs are restricted to families consistent with state-of-the-art catalogues (e.g. EdDSA, ES256, RS256 per BSI TR-021021 and NIST SP 800-175B). In deployments where a TLS-terminating ingress is already in place (as in the DIH LivingLab), the TLS portion of this configuration is not required, since the ingress owns the TLS material and the connector only handles applicationlayer SI-Token / VC verification.

Security does not stop at the wire. The connector contract-negotiation engine treats policies (ODRL, expressed in JSON-LD as part of DSP) as first-class objects: each offered asset is published together with a policy in a ContractRequest / ContractAgreement flow, and any policy whose rules the connector cannot enforce is rejected automatically. Combined with integrity-protected logging of access-control decisions, data accesses and configuration changes, this gives operators an auditable trail of who obtained what data under which conditions.

Data at rest is in a persisted state — contract agreements, transfer process state, asset descriptions — is written to a managed PostgreSQL database that runs on a private network in the cloud, isolated from the public internet and reachable only from the connector. This closes the loop between in-transit security (TLS + DCP) and at-rest security.

7.5.2. Reliable Data Exchange

The connector is split into a control plane (managing catalogues, contract negotiation, policy evaluation, transfer orchestration, DCP token acquisition and VP resolution) and one or more data planes (the Data Plane Framework, DPF) that move the actual bytes. Because the data planes are stateless workers selected per transfer, they can be scaled horizontally and independently of the control plane, so a spike in transfer volume does not degrade catalogue browsing or contract negotiation latency. The DPF can also act as a proxy when source and sink cannot speak directly,

which keeps transfers feasible across asymmetric network topologies.

The connector supports both data-push (provider initiates the upload to a destination) and data pull (consumer fetches from a provider-exposed endpoint) flows. The pull flow is preferred when sovereignty matters because it removes the risk of mis-routed deliveries and lets the consumer prove data was handled correctly; the push flow is used when latency or large-volume streaming dominates. Having both available means an operator can choose the most reliable pattern for each specific exchange rather than being forced into a single transport model.

For production, the in-memory stores are replaced with a managed PostgreSQL service running on a private cloud network. The managed service provides automated failover across availability zones, periodic backups with a defined retention window, and the ability to scale vertically or horizontally without service interruption. Because failover and backups are handled by the cloud provider, the connector itself does not need to embed any custom high-availability logic.

The ingress controller performs hostname/path routing and load-balances requests across multiple connector replicas, so a single replica failure does not interrupt the dataspace endpoint. The connector is delivered as an OCI (Open Container Initiative[11]) container image and deployed through a continuous-delivery pipeline, giving operators reproducible rollouts and straightforward rollbacks. Health checks ensure that orchestration only marks the connector ready once its trust dependencies (DID resolver, Credential Service, Trust Anchor list endpoint) are actually reachable.

Replacing a central DAPS with Trust-Anchor-System based on DCP also has a reliability dimension: there is no single token-issuance service whose outage halts the whole federation. Each participant operates its own Credential Service, DIDs are resolvable from the URL embedded in the identifier (did:web) or directly from the key (did:key), and Verifiable Credentials are long-lived artefacts that the holder can re-present without contacting the original Issuer. The federation only needs to keep its Trust Anchor list reachable, which is a much smaller and easier-to-replicate dependency than a stateful token service.

The managed-database and ingress layers are covered by support contracts and Service Level Agreements (SLAs) from the cloud provider, while the application layer is monitored through cloud-native metrics and logs. Operators have a defined contact path and a published revision history, so reliability claims are backed by a real support process rather than only by architectural design.

7.5.3. Trusted Data Exchange

Trust in a federated data space cannot be created by a single vendor; it must be derived from a federation-wide trust framework. With DCP/IATP, that framework is expressed as:

[11] https://opencontainers.org/

- A list of recognised Issuers (universities, ministries, certification bodies, the data-space governance body itself), each identified by a DID and a public key;
- The schemas of the Verifiable Credentials those Issuers must sign (e.g. Dataspace Membership Credential, Connector Compliance Credential, Security Profile Credential);
- The policies under which those credentials are accepted by other participants.

Each connector is identified by a DID rather than by a single X.509 certificate, decoupling identity from any single PKI hierarchy and allowing participants to bring their own existing organisational identities into the data space.

A static identity alone is not enough — attributes such as a participant's current security profile or membership status can change over time. The connector therefore presents and verifies a Verifiable Presentation on every connection, expressing the attributes currently attested by recognised Issuers. The federation relies on credential lifecycle (expiry, status lists, re-issuance) to make trust decisions revocable without re-issuing the underlying DID, as described in the IDSA Dataspace Trust Frameworks.

Every connector publishes a DCAT-style catalogue / self-description (in JSON-LD) describing its offered datasets, the access policies and the contract policies that apply. Counterparties consume this catalogue over DSP and validate it against the agreed schema before negotiation. This means a participant can mechanically verify, before any business interaction, that a counterparty actually supports the security and usage-control features required by the use case.

Trust in a federation also requires a way to find counterparties, typically realised through a Federated Catalog (one or more aggregator services that crawl participant catalogs over DSP), a dataspace registry of DIDs or IDS Metadata Broker. Combined with the integrity-protected audit logs of every contract negotiation and data access, participants have both the discovery mechanism to locate trustworthy peers and the evidence base to prove, after the fact, that a given exchange happened under an agreed policy.

While the selected configuration demonstrates the identity and trust mechanisms required for connector interactions, the implementation-specific persistence and lifecycle management of DIDs and credentials are not assessed in detail in this deliverable. The specification and verification of DID and credential storage, trust-anchor management, and revocation procedures are therefore left to implementation-specific documentation and are particularly relevant for production-oriented deployments.

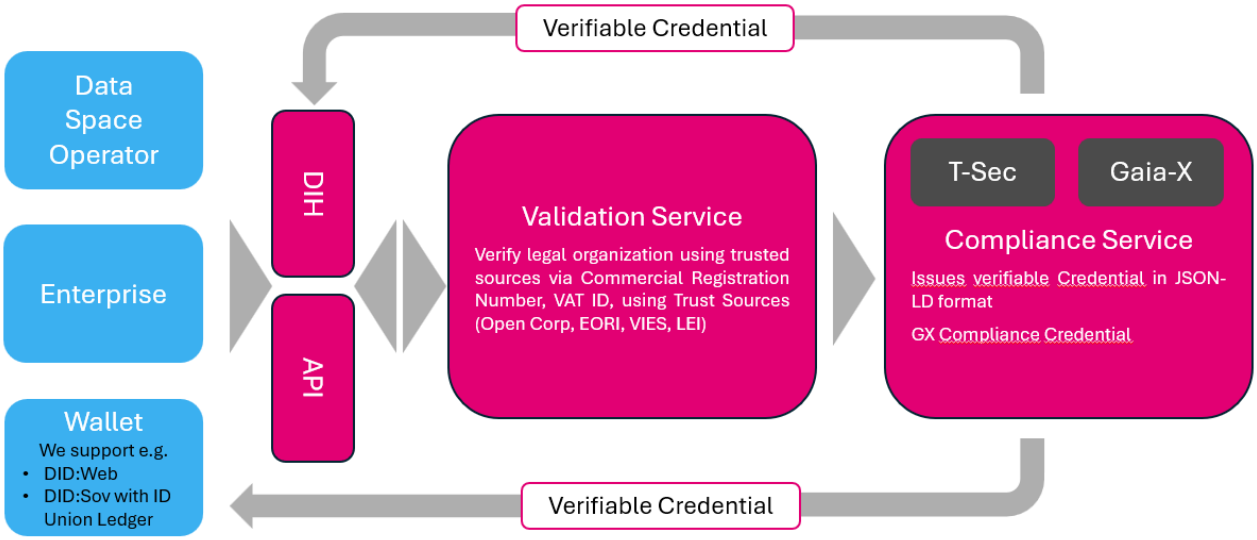


Figure 17. DIH Verification Building Blocks

8. Validation of the Connector Implementation

The objective of the validation activities was to assess whether the connector implementation deployed within the MOTIONAL Federated Rail Data Space fulfils the functional and non-functional requirements and supports secure, reliable and sovereign data exchange between participating organizations.
Rather than validating the connector as an isolated software component, the activities focused on evaluating its integration within the overall Rail Data Space architecture. Consequently, the validation considered the interaction between connectors, metadata brokerage, governance mechanisms, and application services implemented within Work Package 31.

The validation followed an incremental approach consistent with the methodology described in section 5. Following connector deployment within the T-Systems LivingLab, the implemented environment was progressively evaluated using representative railway use cases from D26.2 use case repository contributed by different partners of the MOTIONAL consortium (including cross-FP use case test tracks). Each use case and demonstration assessed complete end-to-end data exchange processes including participant authentication, metadata publication, discovery of digital resources, contract negotiation, policy enforcement and secure data transfer. The demonstrations were executed within the common LivingLab environment, thereby ensuring that all participating organizations interacted through the same federated infrastructure.

The validation covered both functional and operational aspects of the connector implementation. Functional validation concentrated on verifying the successful execution of the complete connector lifecycle, including

- participant onboarding,
- connector registration,
- metadata publication,
- catalogue discovery,
- policy evaluation,
- contract negotiation,
- secure data transfer,
- interaction with complementary data space services.

Operational validation focused on deployment aspects including

- interoperability between organisations,
- connector configuration,
- operational stability,
- integration with existing enterprise systems,
- usability within representative railway scenarios.

Together, these activities provided practical evidence for the applicability of connector technologies within a Federated Rail Data Space.

Functional Testing

For each use case functional tests were carried out to:

- verify data exchange flows between providers and consumers within the T-Systems data space;
- ensure proper handling of different data types (static, real-time dynamic, event-based, on-demand);
- validate the transmission mechanisms according to the defined modalities (pushed/pulled, manual/automatic, on-demand/event-driven).

The tests confirmed compliance with the expected behaviours, while also highlighting some limitations of the current T-System connectors, which do not support real-time dynamic data transmission beyond static data modes.

Performance and Scalability Testing

Load and scalability tests were performed to evaluate the system's ability to:

- handle different volumes of data (e.g., JSON files in MB, compressed digital maps in KB, external weather datasets);
- ensure availability and responsiveness of interfaces under scenarios with frequent updates or concurrent requests;
- minimize the impact on network load, especially in cases of high-frequency updates (e.g., vehicle position reports or train-generated data at track passage).

The results showed that the architecture is well-suited for scenarios with static data, while the processing of dynamic data requires further optimization.

Compliance Verification with IDSA Certification

A key element of validation was the assessment of compliance with IDSA (International Data Spaces Association) principles. Specifically:

- rules for controlled data access were respected, with data shared only among authorized partners;
- security and integrity mechanisms were ensured, particularly for sensitive data (e.g., operational directives, maintenance forecasts)

8.1. Rail-specific Test Use Cases and Test Data Exchange Scenarios

The railway use cases served as the principal application-oriented basis for assessing whether the connector implementation can support data-sharing requirements arising in representative railway scenarios. The four use cases considered in the final validation context cover predictive infrastructure monitoring, maintenance decision support, Digital Twin-based asset services, and train positioning and yard-related information exchange. The detailed descriptions and technical specifications of the fully implemented use cases are provided in Annex A.

The use cases identified in this project represent scenarios designed to validate the capabilities of federated data exchange within the European railway sector. The tests were carried out within a federated architecture based on the Data Space model provided by T-Systems, with multiple partners collaborating to simulate realistic data exchange scenarios using synthetic yet representative datasets. The following sections offer a detailed overview of each use case, outlining the participating partners, the technologies employed, and the tests conducted.

The following table summarizes the Key Performance Indicators (KPIs) defined to evaluate the effectiveness and technical performance of the data exchange activities conducted within the identified use cases. Each KPI is associated with a specific objective, a measurable metric, and a brief explanatory note to clarify its purpose and interpretation. These indicators support an evidence-based assessment of the system's capabilities in terms of interoperability, data quality, performance, and integration feasibility.

Table 5. KPIs for technical performance evaluation

KPI	Objective	metrics	Notes
Provider connector	Checking connector availability	Y | N	How the provider connector works
Consumer connector	Checking connector availability	Y | N	How the consumer connector works
Average data access time	Checking data availability	min	The average data access time through the Data Space, measured from the moment of request.
Percentage of files/data exchange	Data format validity	Y | N	Verify that the exchanged files conform to the expected format specifications.
Completeness of data	Check presence of required fields	%	Ensures that all expected information has been provided, thereby guaranteeing the complete usability of the data.
Parsing errors	capability to accurately interpret data	Number of errors	To determine whether the data has been correctly interpreted and whether the format has been properly handled.
Average data Transfer time	Data Space performance	min	Measures the time required to transfer data from the source system to the recipient system within the Data Space.

In the following, some of the data exchange tests and results are presented in addition to the fully implemented use cases described in Annex A:

Test Data Exchange Scenario 1: Rail Infrastructure Data Federation

Test (03/04/2025): Image file exchange test (***File Type :*** .jpg ***File size:*** 2 MB)

- ***Purpose:*** validate the functionality of connectors for different file types.
- Involved Partners:

  Provider: FSTechnology
  Consumer: Hitachi
- Technologies/Tools Used:
  - FSTechnology: Azure Blob Storage
  - Hitachi: AWS
  - Federated Data Space architecture (T-Systems)

Table 6. KPIs scenario 1, Test 1

KPI	Objective	Observed measurements	Result (OK | nKO)
Provider connector	Checking connector availability	Y	OK
Consumer connector	Checking connector availability	Y	OK
Average data access time	Checking data availability	3 min	OK
Percentage of files/data exchange	Data format validity	Y	OK
Completeness of data	Check presence of required fields	100 %	OK
Parsing errors	capability to accurately interpret data	0 errors	OK
Average Data Transfer time	Data Space performance	3 min	OK

OK = Test successful; nKO = Test failed

The data exchange test was successful only with FS acting as the provider. At that time, the Hitachi connector was not functioning correctly as a Provider.

Test (05/06/2025): Text file exchange test (.txt) containing a short message

- ***Purpose:*** validate the functionality of Hitachi connectors for different file types.
- Involved Partners:

  Provider: FSTechnology
  Consumer: Hitachi
- Technologies/Tools Used:
  - FSTechnology: Azure Blob Storage
  - Hitachi: AWS
  - Federated Data Space architecture (T-Systems)

Table 7. KPIs scenario 1, test 2

KPI	Objective	Observed measurements	Result (OK | nKO)
Provider connector	Checking connector availability	Y	nKO
Consumer connector	Checking connector availability	N	nKO
Average data access time	Checking data availability	Na	nKO
Percentage of files/data exchange	Data format validity	Na	nKO
Completeness of data	Check presence of required fields	Na	nKO
Parsing errors	capability to accurately interpret data	Na	nKO
Average Data Transfer time	Data Space performance	Na	nKO

OK = Test successful; nKO = Test failed

The data exchange test failed with FSTechnology as a provider and Hitachi as a Consumer. The file never arrived. Could have been an issue during the configuration of connector during the deployment.

Test (21/03/2025): Exchange of a .txt file containing fictitious data based on the "Dynamic Data" submodel

- ***Purpose:*** validate the functionality of Hitachi connectors for different file types.
- Involved Partners:

  Provider: FSTechnology
  Consumer: V2C2
- Technologies/Tools Used:
  - FSTechnology: Azure Blob Storage
  - V2C2: REST API
  - Federated Data Space architecture (T-Systems)

Table 8. KPIs scenario 1, test 3

KPI	Objective	Observed measurements	Result (OK | nKO)
Provider connector	Checking connector availability	Y	OK
Consumer connector	Checking connector availability	Y	OK
Average data access time	Checking data availability	3 min	OK
Percentage of files/data exchange	Data format validity	Y	OK
Completeness of data	Check presence of required	100%	OK

	fields		
Parsing errors	capability to accurately interpret data	0 errors	OK
Average Data Transfer time	Data Space performance	3 min	OK

OK = Test successful; nKO = Test failed

The data exchange was successfully completed.

The Testing and Validation activities identified limitations mainly concerning real-time data handling, which will require future enhancements to ensure full scalability and interoperability in complex operational scenarios.

Below are tables summarizing the findings of the tests:

Test Data Exchange Scenario 2: Rail Infrastructure Data Federation
The partners involved are Hitachi and FSTechnology.
The requirements are summarized as:

- Data Model: defined by Hitachi partner
- Data Format: JSON
- Data Format Size: MB

Table 9. Data exchange scenario 2

PROVIDER	CONSUMER	DATA TYPE	HOW DATA TRANSIT THROUGH THE T-System DATA SPACE	T-System LIMITS
Railway Infrastructure Manager	Railway Operations Manager/Signalling Supplier	Track Topology	Pulled on demand or pushed on topology change events (e.g., quarterly).	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Railway Infrastructure Manager/Technology Supplier	Maintenance Technician/Technolooy Supplier/ Signalling Supplier	Data Sensor	Pushed in **real-time**, event-driven; transmitted when a train passes	T-System Connectors do not handle data transfer other than static data

Train Operator	Railway Infrastructure Manager/Signaling Supplier	Train Data	Pushed in real-time, generated per track section passage.	T-System Connectors do not handle data transfer other than static data
Maintenance Company (i.e. Mermec, Hitachi)	Maintenance Technician/Signaling Supplier	Track Maintenance Data	Pulled **on demand**; updated manually or through maintenance systems when activities are logged.	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
External Weather service provider	Railway Operations Manager/Signaling Supplier	Weather Data	Pulled **on demand** from external/local weather service APIs or systems.	• On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries. • It is not permitted to share data with third parties outside the partnership.

Test Data Exchange Scenario 3: Track and Positioning Regional Lines & Data Yard Automation

The partners involved are Wabtec and FSTechnology.
The requirements are summarized as:

- Data Model: digital track map (or a list of positions of critical features on the line)
- Data Format: WGS84 coordinates or digital map compressed file
- Data Format Dimension: KB

Table 10. Data exchange scenario 3

PROVIDER	CONSUMER	DATA TYPE	HOW DATA TRANSIT THROUGH THE T-System DATA SPACE	T-System LIMITS
Yard Manager / Railway Infrastructure Manager	Regional train control and signaling system integrator	Yard Track Topology	**Static data**, pulled **on demand** or on update events; pushed manually or automatically when layout changes.	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Railway Infrastructure Manager	Regional train control and signaling system integrator	Regional Line topology	**Static data**, pulled **on demand** from infrastructure systems; updated manually or periodically (e.g., quarterly).	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Railway Rolling Stock Operator	Railway Infrastructure Manager	Vehicle Position Reports	**Real-time dynamic data**, pushed continuously or periodically by Yard/Regional systems; event-driven.	T-System Connectors do not handle data transfer other than static data
Yard Manager / Railway Infrastructure Manager	Railway Rolling Stock Operator	Operational Directives	**Static Data**; Event-based data, pushed manually by authorized users (e.g., Yard Manager) via secured interfaces.	NA

Test Data Exchange Scenario 4: Monitoring of Track Settlement & Identification of Single-Faults in Switches

The partners involved are V2C2 (Virtual Vehicle) and FSTechnology.

The requirements are summarized as:

- Data Model: defined & provided by V2C2 partner
- Data Format: JSON
- Data Format Dimension: MB

Table 11. Data exchange scenario 4

PROVIDER	CONSUMER	DATA TYPE	HOW DATA TRANSIT THROUGH THE T-System DATA SPACE	T-System LIMITS
Infrastructure manager/Train Operator	Research Company	Track measurement & Vehicle collective	Pulled **on-demand**, the vehicle collective has to be updated automatically	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Infrastructure Manager	Research Company	Track Geometry & Maintenance Actions	Pulled **on-demand**; updated manually or through maintenance systems when activities are logged.	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Railway Rolling Stock Operator/Infrastructure Manager	Research Company	Static vehicle & Infrastructure	**Static data**, pulled **on-demand** or on update events; pushed manually or automatically when topology(layout changes	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Asset Manager	Research Company	Forecasting & Vehicle Mix	**Event-based data**, pushed manually by authorized users (e.g., Asset Manager).	On-demand data is retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.
Research Company	Asset	Sleeper	**Event-based data**;	On-demand data is

	Manager	Forecasts Output	pushed automatically when calculation/results are available.	retrieved only when explicitly requested, not in real time. It suits situations with infrequent updates or when minimizing network load, typically accessed via APIs or queries.

The test data exchange scenarios as well as the fully implemented use cases in Annex A evaluate the connectors and functionalities around the data space environment.

The performance measurements evaluate the end-to-end data exchange workflow in the LivingLab and do not separately quantify the latency attributable to contract negotiation and connector handshaking. Assessing the contribution of these individual stages would require dedicated measurements and is therefore more appropriately addressed in a production-oriented performance evaluation under defined operating conditions.

8.2. Demonstrator

As described in FP 1 Maturity Check Point 7 Supporting Documents, it was expected that a demonstrator with a TRL 7 was developed within WP31. Therefore, certain capabilities had to be implemented:

- **Standardised connectors**, which are software components for secure and trusted data exchange across participants in the federation, using IDSA provided sample code, reference implementations, testbed services for interoperability compliance, technical specifications, starter kit and co-creation platform. This is presented in the current document.
- **Meta-data broker**, i.e. a comprehensive data catalogue, that contains machine-readable semantic descriptors of digital resources participating in the federation that are published by resource providers enabling resource discovery by resource consumers. This is presented in Deliverable *D31.2 IDSA-compliant meta-data broker and discovery services in federated data space.*
- **App-Store** as searchable repository of packaged software components such as compiled Digital Twin Functional Mock-up Units, common domain ontology graph developed in work package CDM, and semantic automated cross-format converters according to the common domain ontology. This is presented in Deliverable *D31.3 IDSA-Compliant App Store in federated data space*.

The resulting demonstrator was then presented to the public during the *FLAGSHIP PROJECT 1 MOTIONAL DIGITAL FOUNDATION DEMOSTRATION & VALIDATION EVENT* on 29th April 2026 and later validated by two external validators during the Validation Event for WP31 on 7th May 2026.

8.2.1. Demonstration Event

A demonstrator of the rail data space including working connectors, meta data broker and an implemented app store with two available use cases was demonstrated during the *FLAGSHIP PROJECT 1 MOTIONAL DIGITAL FOUNDATION DEMOSTRATION & VALIDATION EVENT* on 29th April 2026.

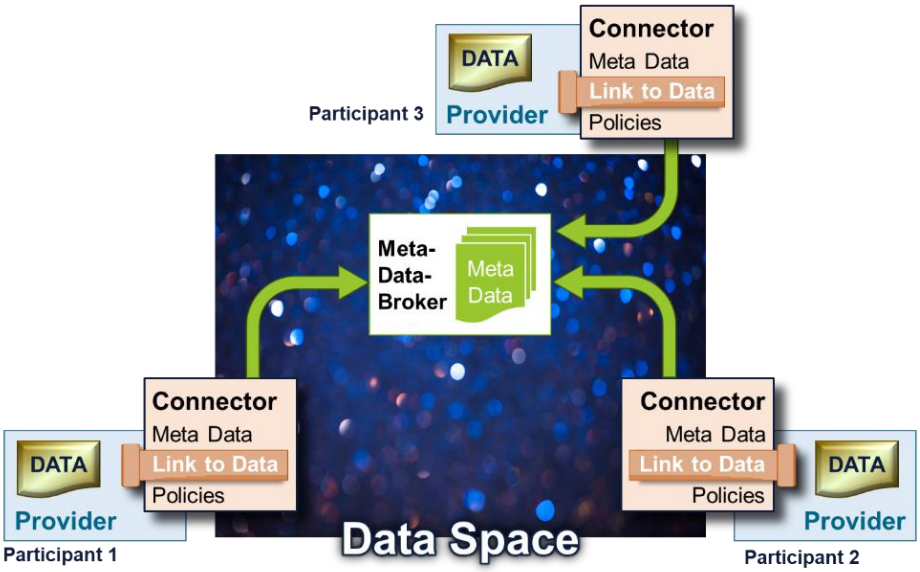


Figure 18. Publishing of data offers to meta data broker

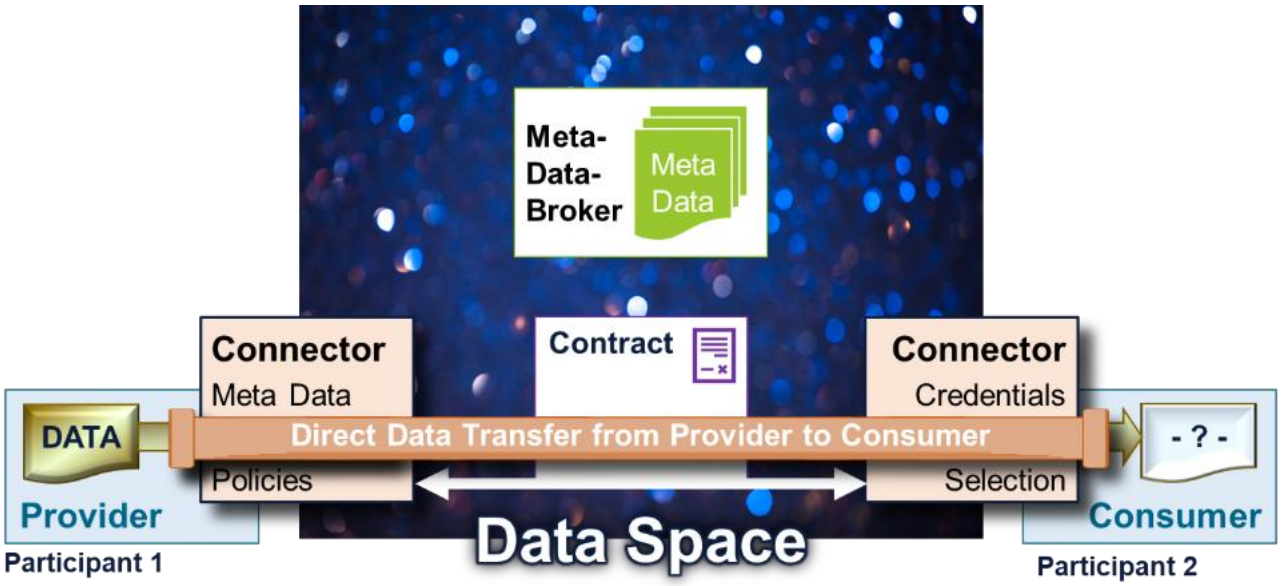


Figure 19. Secure data transfer through the connector.

There, an introductory video was presented, which was originally created and shown at the InnoTrans 2024. Then, an overview of the data space was given, including an introduction of participants and a description of connectors, the meta data broker and the app store. Next, the question of how to share data was answered by introducing data offers as shown in Figure 18. Once an offer is published, it can be searched for by a consumer, providing their credentials, a destination for the offered data to be transferred to and by selecting one of the offered policies. Then, a contract is formed and the data transfer is started automatically as shown in Figure 19.

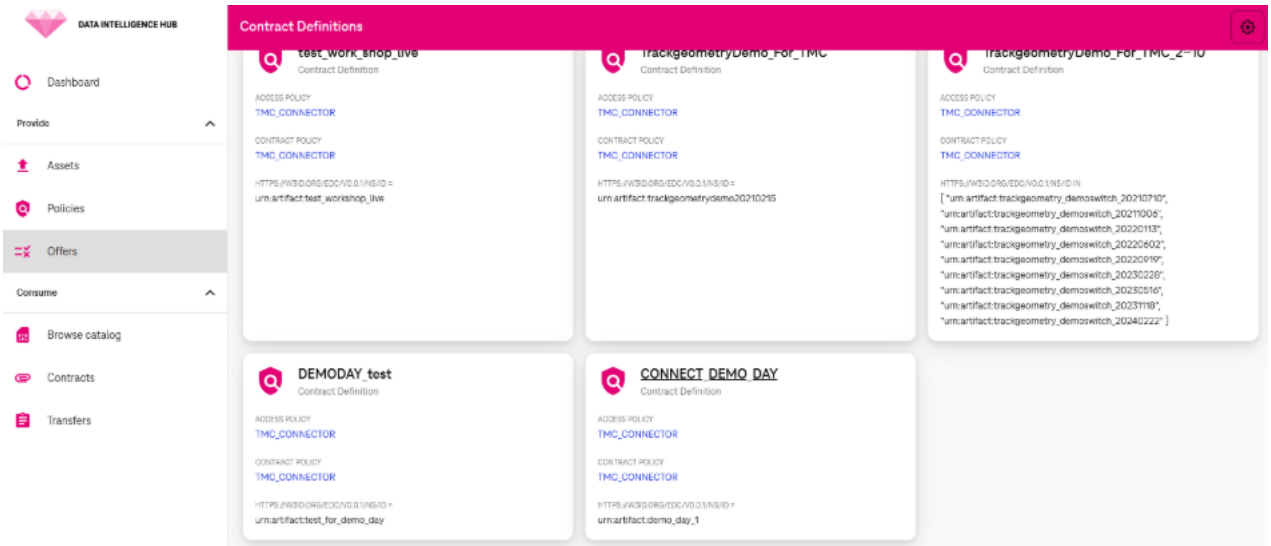


Figure 20. Screenshot of the LivingLab sandbox environment including a created data offer.

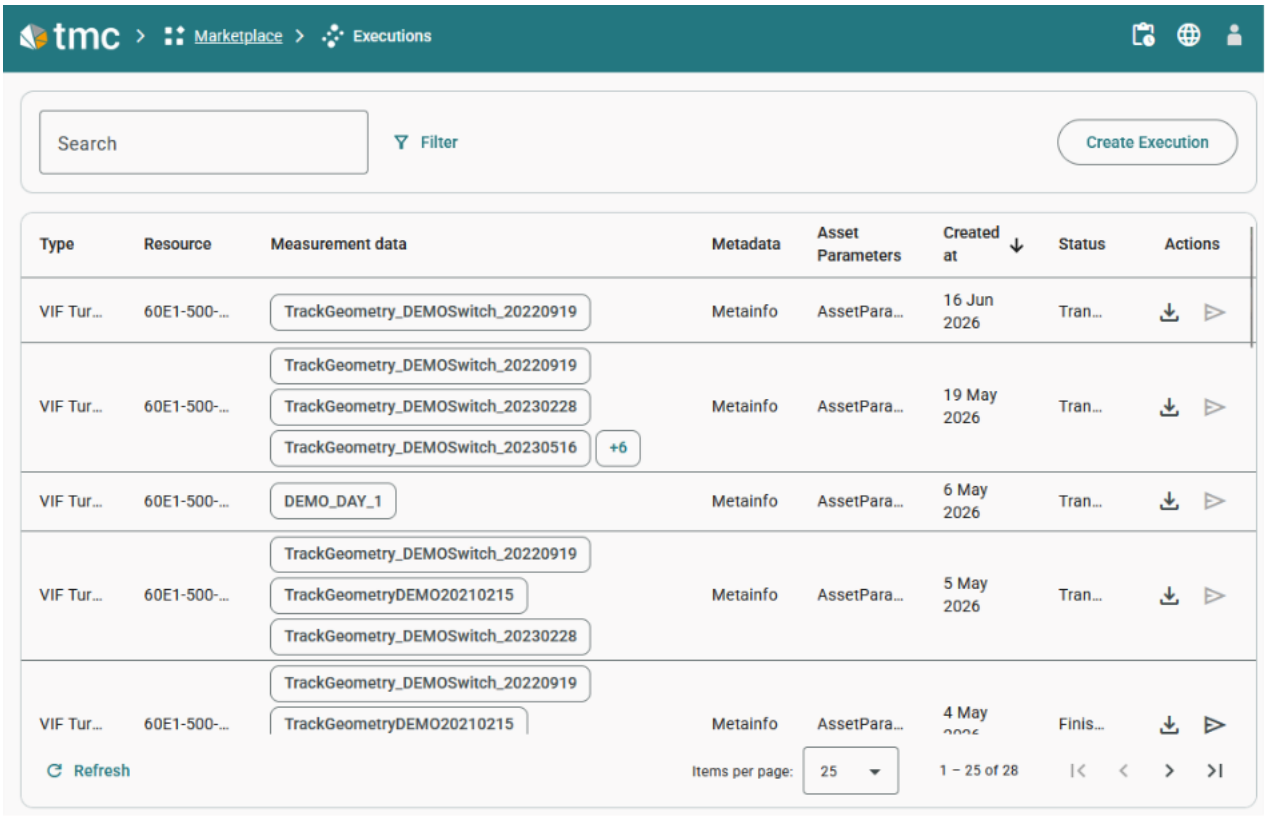


Figure 21. Screenshot of the App-Store including executed use-cases.

Using a video of the LivingLab sandbox environment, the creation of offers containing assets (meta data and link to data) and policies (access and usage) was demonstrated. A screenshot is shown in Figure 20 with the created data offer

Next, the example use-case *Monitoring of Track Settlement and Identification of Single-Faults in Switches* was presented. Then, a pre-recorded video showed the implementation in the app-store (see also Figure 20). The use-case was executed using the front-end of the app store (Figure 21) and the results where then shown to be directly transferred to Zentrak, the maintenance decision tool (see also Annex A).

Thus, it could be shown that the whole pipeline, from data through connectors to digital twin and then maintenance decision tool was implemented and working.

8.2.2. Validation of Demonstrator

Based on the demonstrator presented during the demonstration event discussed in subsection *8.2.1 Demonstration Event*, a separate Validation Event was held on 7th May 2026. There, the goal was to demonstrate TRL 6 “Technology demonstrated in a relevant environment (industrially relevant
environment in the case of key enabling technologies)”. According to BRIDGE2HE H2020-101005071[12], this means that “the prototype has to be demonstrated in a real environment, so to

[12] BRIDGE2HE. (2022). Guiding notes to use the TRL self-assessment tool (Grant Agreement No. 101005071). Horizon

confirm the engineering is feasible". In case of a software, it must be a "Beta version of the software functionalities tested by selected end-user under a control mode".

To test the functionalities, four validators were invited to test the data space. They were given access to the tmOS Marketplace with 2 implemented use cases: the "Monitoring of Settlement and Identification of single Faults in switches" and the "Maintenance Decision Tool" use case, along with an onboarding session consisting of a presentation and a Q&A session. Then they were given a deadline of two weeks to test the capabilities. They were able to successfully use the demonstrator, proofing TRL 6. Afterwards, they were asked to fill out a questionnaire. The detailed responses can be found in Annex B.

The questionnaire responses, presented in detail in Annex B, show that the validators view the Federated Data Space and App Store primarily as a strategic enabler for the rail sector rather than a merely technical tool. Both participants rated the relevance of the proposed Data Space to their organisation as moderate. The expected impact was primarily associated with maintenance and reliability, data integration and interoperability, and cross-border harmonisation. The most valuable benefit identified was easier access to data and services combined with secure interoperability between systems, reflecting the broader ambition of the Federated Data Space to overcome data fragmentation across the rail value chain. At the same time, the validators indicated that the technology is not yet ready for large-scale deployment: expected adoption timeframes range from less than one year to more than three years, and financial return on investment as well as legal and governance compliance were named as the primary barriers to adoption. Trust-building elements such as guarantees of data sovereignty, auditability and certification mechanisms, were consistently highlighted as prerequisites for wider participation. Overall, the validation confirms that, from a macroeconomic perspective, industry stakeholders recognise the potential of data space technology to reduce costs, harmonise cross-border operations and enable new digital services for the rail sector. However, regulatory clarity, demonstrated technical maturity and clear economic value are seen as the critical success factors that still must be addressed before broader industry adoption can take place.

8.3. Validation Results

The demonstrations and implemented use cases (Annex A) confirmed the successful deployment and operation of IDSA-compliant connector technology within the MOTIONAL Federated Rail Data Space. The validation demonstrated interoperability between participating organisations and confirmed the successful execution of the principal connector functions throughout the complete data exchange lifecycle.

The implemented environment successfully supported

- secure participant authentication,

Europe NCP Portal. Retrieved September 16, 2026, from https://horizoneuropencpportal.eu/sites/default/files/2022-12/trl-assessment-tool-guide-final.pdf

- publication and discovery of metadata,
- policy-controlled access management,
- contract negotiation,
- trusted data transfer,
- interaction with complementary services including the metadata broker and App Store.

Overall, the demonstrations confirmed that connector technology provides a suitable technical foundation for implementing sovereign railway data exchange within federated environments.

Table 12. Connector capability validation

Capability	Validation Status	Evidence	Reference
Connector deployment	Successful	LivingLab deployment	Section 7
Participant onboarding	Successful	Demonstration	Section 7
Metadata publication	Successful	Broker interaction	Section 7 + 8
Catalogue discovery	Successful	Demonstration	Section 7 + 8
Policy enforcement	Successful	Contract negotiation	Section 7 + 8
Secure communication	Successful	Connector interaction	Section 7 + 8
Data transfer	Successful	End-to-end demonstration	Section 7 + 8
Interoperability	Successful	Multi-partner demonstration	Section 7 + 8

8.4. Discussion

The validation demonstrated that mature connector technologies already provide the functionality required to establish secure and interoperable railway data spaces. Rather than requiring the development of proprietary connector software, the project showed that existing IDSA-aligned implementations can be successfully configured and integrated into representative railway environments. The demonstrations further confirmed that connector technologies should not be considered as isolated software products but as one component of a broader federated ecosystem including metadata brokerage, governance services and application platforms. The practical experience gained during deployment highlighted the importance of configuration, onboarding procedures and interoperability testing, which proved to be considerably more relevant than implementing additional connector functionality.

8.5. Limitations

Although the validation successfully demonstrated the feasibility of connector-based railway data exchange, several limitations remain. The demonstrations were performed within the controlled LivingLab environment established for Work Package 31 and therefore do not fully represent large-

scale operational deployments involving numerous independent organizations. Furthermore, the project focused on validating interoperability and integration rather than evaluating long-term operational performance, scalability or production readiness. Future activities should therefore investigate large-scale deployment scenarios, onboarding procedures and cross-data-space interoperability (depending on technology etc.) between multiple European sectoral data spaces.

The validation found that the tested T-Systems LivingLab configuration did not support the required real-time dynamic data transmission. This result applies to the implementation and source/sink paths tested but does not establish an inherent limitation of all EDC-based implementations or architectures. As Section 7.5.2 distinguishes control plane orchestration from data plane transfer, event-driven scenarios require compatible transfer mechanisms and end-to-end validation. This capability was not demonstrated in D31.4 and remains a topic for upcoming projects.

Validation used one managed T-Systems LivingLab data-space deployment with multiple participant connectors, not federation between independently operated data spaces. All results demonstrate feasibility for selected configurations, not general compatibility with railway repositories. *D31.4* does not quantify the staff time, elapsed time or cost required for endpoint integration and onboarding; a general integration-effort estimate cannot be derived.

8.6. Lessons Learned

The implementation and validation activities provided several lessons for the establishment of a Federated Rail Data Space. First, the project demonstrated that the main challenge does not necessarily lie in developing new connector technologies, but rather in successfully integrating mature, interoperable and standards-based components into a federated ecosystem. The use of EDC-based connectors enabled the project to focus on configuration, integration and validation within representative railway scenarios while providing the fundamental mechanisms required for secure and sovereign data exchange. This indicates that future development activities can benefit from reusing established connector technologies instead of developing proprietary middleware.

Second, the project experience showed that connector technology alone is insufficient to establish an operational Federated Rail Data Space. Governance, semantic interoperability and organisational onboarding proved to be equally important success factors. In particular, the successful exchange of data across organisational boundaries requires not only interoperable technical interfaces, but also agreed governance mechanisms, compatible semantic representations and processes that allow new participants to be integrated into the federation.

Third, the validation activities highlighted the importance of evaluating connectors as part of the wider data space ecosystem rather than as isolated software components. The demonstrations covered the complete exchange lifecycle, including data publication, discovery, negotiation, policy-compliant transfer and downstream consumption, thereby showing that integration with complementary services such as the metadata broker and application services is essential for practical interoperability. At the same time, the validation demonstrated that the current implementation is better suited to static and non-real-time data exchange, while dynamic data

transmission and large-scale operational deployment require further investigation.
Overall, the lessons learned suggest that the further evolution of European Rail Data Spaces should focus less on developing additional proprietary connector functionality and more on ecosystem integration, governance, semantic interoperability, organisational onboarding and cross-data-space interoperability. This provides a direct basis for the recommendations and future work identified in the following conclusion.

9. Conclusions

The Rail Data Space Connector provides a trusted, secure, and interoperable implementation for data exchange within the European rail sector. By complying with IDSA standards, the solution enables a federated and decentralized data-sharing ecosystem, thereby paving the way for digital transformation in rail transportation.

The establishment of a Federated Rail Data Space requires secure, reliable and trusted mechanisms for exchanging data across organisational boundaries while preserving data sovereignty and interoperability. Against this background, Deliverable D31.4 investigated the applicability of IDSA-compliant connector technologies as a central technical enabler for federated railway data exchange. The work did not aim to develop a new connector technology, but to assess, configure, integrate and validate an existing IDSA-aligned implementation within the MOTIONAL Federated Rail Data Space.

The methodology followed a structured sequence from requirements analysis and technology selection to configuration and integration, demonstration, validation and evaluation. Based on the identified requirements, EDC-based connectors deployed in the T-Systems LivingLab were selected as the technological foundation and integrated with complementary WP31 services, including the metadata broker and App Store. The subsequent validation used representative railway use cases and assessed the complete data exchange lifecycle, covering participant authentication, metadata publication and discovery, contract negotiation, policy enforcement, secure data transfer and interoperability between participating organisations.

The results demonstrate that the implemented connector environment successfully provides the principal capabilities required for federated railway data exchange. The demonstrations confirmed secure participant authentication, metadata publication and discovery, policy-controlled access, contract negotiation, trusted data transfer and interaction with complementary data space services. In particular, the project demonstrated that mature, standards-based connector technologies can be successfully configured and integrated into representative railway environments without requiring the development of proprietary connector middleware. This approach therefore represents the most suitable solution within the scope of the project, as it enables the available resources to be directed towards integration, onboarding, interoperability and validation rather than reproducing established connector functionality.

Overall, the planned objectives of the deliverable have been achieved: an IDSA-aligned connector implementation was deployed, integrated into the Federated Rail Data Space and validated in representative railway scenarios. The work also demonstrates that connector technologies should be considered as part of a broader federated ecosystem comprising metadata brokerage, governance mechanisms and application services rather than as isolated software components. This has implications for subsequent development activities within the Rail Data Space and for other European sectoral data spaces seeking to establish interoperable and sovereign data exchange infrastructures.

The findings are nevertheless subject to the scope of the validation. The demonstrations were conducted in a controlled LivingLab environment and therefore do not fully represent large-scale operational deployments involving numerous independent organisations. In addition, long-term operational performance, scalability and production readiness were not comprehensively

evaluated. Future work should therefore focus on larger multi-organisational deployments, more automated onboarding procedures and cross-data-space interoperability between European sectoral data spaces.

The validation supports policy-controlled data exchange for selected source/sink configurations within one managed LivingLab deployment. It does not establish federation between separately operated data spaces, general integration with operational railway repositories, real-time capability in the tested configuration or quantified onboarding effort. Wave 2 should assess these gaps alongside protocol conformance, cross-domain federation, hosting portability, streaming adapters, and the portability of assets, policies, identity/trust configuration and contract records when connector implementations change.

10. References

[1] B. Otto, A. Burmann, „Europäische Dateninfrastrukturen“, Informatik Spektrum, Vol. 44, No. 4, pp. 283 – 291, 2021.

[2] N. Jahnke, I. Jussen-Lengersdorf, T. Schoormann, F. Möller, „Designing Federated Data Marketplaces in Industrial Production: Findings from a Prototypical Implementation“, 19th International Conference on Wirtschaftsinformatik, Würzburg, Germany, 2024.

[3] F. Möller, I. Jussen-Lengersdorf, V. Springer, A. Gieß, J. Schweihoff, J. Gelhaar, T. Guggenberger, und B. Otto, „Industrial data ecosystems and data spaces,“ Electronic Markets, Vol. 34, pp. 1–17, 2024.

[4] Gieß, A., Hupperz, M., Schoormann, T., & Möller, F. (2024). What does it take to connect? Unveiling characteristics of data space connectors. Proceedings of the 57th Hawaii International Conference on System Sciences. 4238-4247.

[5] D. Heimbigner, D. McLeod, „A federated architecture for information management“, ACM Trans. Inf. Syst., Vol. 3, No. 3, pp. 253 – 278, July 1985.

[6] R. Abraham, J. Schneider, J. vom Brocke, „A taxonomy of data governance decision domains in data marketplaces“, Electronic Markets, Vol. 33, No. 1, 2023.

[7] N. Duan, „Design Principles of a Federated Service-oriented Architecture Model for Net-centric Data Sharing“, The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 6, No. 4, pp. 165 – 176, 2009.

[8] C. A. Lee, R. B. Bohn, M. Michel, „The NIST Cloud Federation Reference Architecture“, NIST, Gaithersburg, 2020.

[9] Matsunaga, I., Michikata, T., & Koshizuka, N. (2023). ITDT: International testbed for dataspace technology. In 2023 IEEE International Conference on Big Data (BigData) (pp. 4740-4747). IEEE.

[10] Nast, M., Rother, B., Golatowski, F., Timmermann, D., Leveling, J., Olms, C., & Nissen, C. (2020). Work-in-progress: Towards an international data spaces connector for the internet of things. In 2020 16th IEEE International Conference on Factory Communication Systems (WFCS) (pp. 1-4). IEEE.

[11] Peixoto, A. R. A. (2023). Usage policy control data app for data spaces (Master's thesis, Universidade do Minho (Portugal)).

ANNEX A: Use Cases

Next to the transfer of data, one of the goals during the development of the rail data space was the implementation of services. This would enable different use-cases ranging from prediction of track settlements to maintenance decisions.
The first step was to create detailed descriptions of the proposed use cases to later derive necessary technical requirements for the data-space and app-store. These could range from necessitating simple data transfers to handling of streaming data or even real-time data transfers. The different requirements introduced different complexities, some of which necessitated additional improvements of the underlying connector technology. Since the current connector technology in the data space sandbox provided by T-Systems LivingLab was not able to meet all necessary prerequisites, it was not possible to fully implement all use cases. Here, the focus for the upcoming Wave 2 and 3 activities is to further explore and develop the rail-specific connector requirements such as the real-time data exchange.

This section lists all discussed use cases including their description, the requirements related to the data space, their implementation status and, if available, their interface specification. These use cases are:

- Monitoring of Track Settlement and Identification of Single Faults in Switches
- Maintenance Decision Tool
- Digital Twin of Point Machine
- Track and Positioning regional Lines and Data Yard Automation

1. Monitoring of Track Settlement and Identification of Single Faults in Switches

This use case was developed in WP 10 and WP 11 of *FP3 – Iam4Rail* by voestalpine Rail Systems, voestalpine Signaling Austria, and Virtual Vehicle Research. It aims to predict the quality of the switch with regards to track settlement while also identifying single faults. Therefore, measured data from a real switch is continuously fed the simulation model. The free parameters in the simulation are trained on the provided data – historical and current– to give accurate predictions on the future behaviour. The more data is available, the better the prediction will be. This prediction can then be used to estimate necessary maintenance actions by comparing the prediction with a limit specified by the infrastructure manager. The use case is implemented in the Digital twin sandbox developed by Virtual Vehicle Research and connected to the data space. As such, it can be executed through the ERJU App Store demonstrator.

Figure 22 provides an overview of the use case. The data space is depicted on the left and acts as the data provider, delivering the inputs required for the use case. Its execution can either be triggered manually by a user or automated to run whenever new data becomes available. The use case itself is implemented in a Digital Twin sandbox developed and hosted by Virtual Vehicle Research. Within the sandbox, the data is used to train a model that predicts the development of

a previously defined quality index. The resulting behaviour of the quality index is then transferred back to the App Store, which acts as the data consumer.

An infrastructure manager can subsequently compare the time dependent development of the quality with a predefined quality threshold. Taking into account the costs and availability of machinery and track access, this information can support decisions on necessary maintenance. Such decisions can also be supported by automated tools, as described in the "Maintenance Decision Tool" use case in Section 2 of ANNEX A that uses the output of the "Monitoring of Track Settlement and Identification of Single Faults in Switches" use case as input.

Table 13. Overview of Roles and Requirements

Data Type	Size	Format	Provider	Consumer	Data Transfer
Vehicle Collective	MB	.json	Train Operator	Research Company	Pulled on-demand, updated regularly
Track Layout	MB	.json	Infrastructure Manager	Research Company	Pulled on demand, Static data
Track Geometry	MB	.json	Infrastructure Manager	Research Company	Pulled on-demand, updated regularly
Maintenance Actions	MB	.json	Infrastructure Manager	Research Company	Pulled on-demand, updated regularly
Vehicle Models	MB	.spck	Rolling Stock Operator	Research Company	Pulled on demand, Static data
Forecast Window	KB	.json	Asset Manager	Research Company	Pushed manually by user Event-based data
Forecast Output	KB	.json	Research Company	Asset Manager	Pushed automatically when results are available, Event-based data

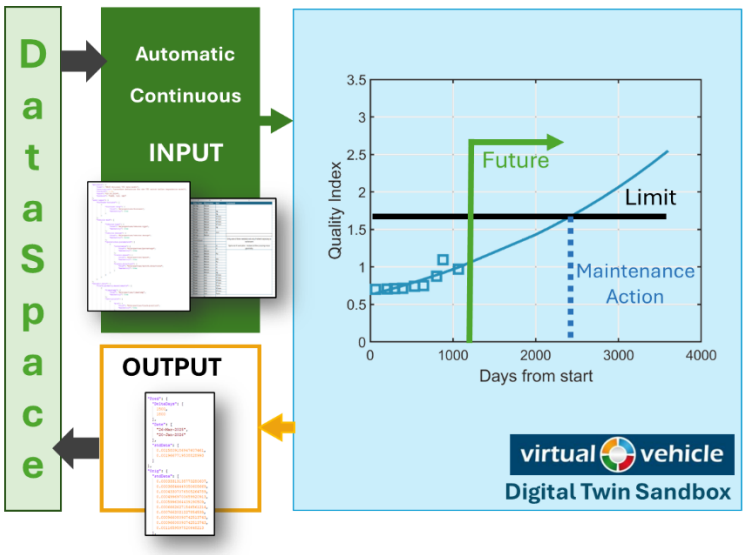


Figure 22. Overview of the use case "Monitoring of Track Settlement and Identification of Single Faults in Switches"

1.1 Interface description and Data Model

This use case requires data from different sources. The first source is called user data and consists of the forecast horizon, which consists of future dates for which the quality should be predicted, and the vehicle mix that passes the switch in regular intervals. In most cases, the latter will be automatically generated from existing operational data. However, the acquisition of new vehicles in the near future or changes in operational planning might interfere with the prediction. By giving the user the option to decide for themselves on the actual vehicle mix used for the prediction, such changes can be accounted for. An overview of the user inputs is given in Table 144-

Table 18. Static Data Vehicle

Component	Parameter	Format	Type	Dimension	Unit
metadata	vehicle-type	JSON	String	Scalar	-
	vehicle-design	JSON	String	Scalar	-
carbody	carbody-mass	JSON	Float	Scalar	kg
bogie	bogie-mass	JSON	Float	Scalar	kg
primary-suspension	stiffness	JSON	Float	Scalar	N/mm
	damping	JSON	Float	Scalar	Ns/m
Secondary-suspension	stiffness	JSON	Float	Scalar	N/mm
	damping	JSON	Float	Scalar	Ns/m
wheelset	mass	JSON	Float	Scalar	kg
	wheel-profile	JSON	String	Scalar	-

Table 199.

Table 14. User Inputs

Category	Parameter	Format	Data Type	Dimension	Unit	Comment
Forecast Horizon	Forecast Step	CSV	Float	List	months	
Vehicle Mix	Vehicle Type	CSV	Float	List	-	Can always change and is usually determined from the measured vehicle collective (see Additional Quantities)
	Vehicle Design	CSV	Float	List	-	
	Occurrence	CSV	Float	List	percentage	
	Travel Speed	CSV	Float	List	m/s	
	Travel Direction	CSV	Float	List	-	

Table 15. Dynamic Data

Category	Parameter	Format	Data-Type	Dimension	Unit
Track Geometry	time-stamp	CSV	Datetime	List	-
	position	CSV	Float	List	km
	longitudinal-level	CSV	Float	List	M
Maintenance Actions	time-stamp	CSV	Datetime	List	-
	maintenance-type	CSV	String	List	-

Table 16. Output

Category	Parameter	Format	Data Type	Dimension	Unit	Comment
Forecast Horizon	forecast-step	CSV	Float	List	months	Output values always per sleeper for forecast horizon (see user input)
Sleeper	Bending	CSV, Mat	Float	List	m	
	compression	CSV, Mat	Float	List	Pa	
	force	CSV, Mat	Float	List	N	
	settlement	CSV, Mat	Float	List	m	

Table 17. Static Data Super-structure

	Data	JSON	Float	List	mm
Switch	Switch Type	JSON	String	Scalar	-
Switch Geometry	Geometry CAD	STP	Float		-
	Geometry Scan	STL	Point Coud		-
	Geometry Calipri	XML, Mat	Float		-

Wheel Trajectory		Track Position	CSV	Float	List	m
		Vertical Movement	CSV	Float	List	m
Rail		Profile Type	JSON	String	Scalar	-
		Elasticity	JSON	Float	Scalar	Pa
Sleeper	Sleeper	Number	JSON	Integer	Scalar	-
		Track Position	JSON	Float	Scalar	km
		Modulus of Elasticity	JSON	Float	Scalar	Pa
		Length	JSON	Float	Scalar	m
		Width	JSON	Float	Scalar	m
		Height	JSON	Float	Scalar	m
		Mass	JSON	Float	Scalar	kg
	Sleeper pad	Stiffness	JSON	Float	List	N/mm
		Damping	JSON	Float	List	Ns/m
	Ballast Pad	Stiffness	JSON	Float	List	N/mm
		Damping	JSON	Float	List	Ns/m
		Modulus of subgrade reaction	JSON	Float	List	Pa/m
	Ballast	Stiffness	JSON	Float	List	N/mm
		Damping	JSON	Float	List	Ns/m
		Modulus of subgrade reaction	JSON	Float	List	Pa/m

Table 18. Static Data Vehicle

Component	Parameter	Format	Type	Dimension	Unit
metadata	vehicle-type	JSON	String	Scalar	-
	vehicle-design	JSON	String	Scalar	-
carbody	carbody-mass	JSON	Float	Scalar	kg
bogie	bogie-mass	JSON	Float	Scalar	kg
primary-suspension	stiffness	JSON	Float	Scalar	N/mm
	damping	JSON	Float	Scalar	Ns/m
Secondary-suspension	stiffness	JSON	Float	Scalar	N/mm
	damping	JSON	Float	Scalar	Ns/m
wheelset	mass	JSON	Float	Scalar	kg
	wheel-profile	JSON	String	Scalar	-

Table 19. Additional quantities

Value	Parameter	Format	Type	Listtype	Unit	Comment
Deflection Measure-ments	Time Stamp	CSV	Datetime	List	-	Measurement of the vertical deflection with special measuring trolleys. This enables to determine the system parameters stiffness and damping of the ballast (or overall superstructure).
	Distance to Reference	CSV	Float	Sub-List	km	
	vertical-deflection	CSV	Float	Sub-List	m	
Settlemen t Measure-ments	Time Stamp	CSV	Datetime	List	-	Measurement of the vertical settlement with a stationary measurement at the turnout. They enable to calibrate the system parameters 'travel distance'.
	Track Position	CSV	Float	Sub-List	m	
	Settlement	CSV	Float	Sub-List	m	
Hammer Tests	Time Stamp	CSV	Datetime	List	-	Measurement of the impedance of the rail system. They enable to determine the system parameters stiffness and damping for sleeper soling.
	Distance to Reference	CSV	Float	Sub-List	m	
	acceleration	CSV	Float	Sub-List	m/s^2	
Vehicle Collective	Time Stamp	CSV	Datetime	List	-	If the vehicle mix is not specified by the user
	Count	CSV	String	List	-	
	Type	CSV	String	List	-	
	Design	CSV	String	List	-	
	Axles Count	CSV	Integer	List	-	
	Weight	CSV	Float	List	kg	
	Travel Speed	CSV	Float	List	m/s	
	Travel Direction	CSV	Float	List	m/s	

1.2 Implementation Status

A demo version of this use case was fully implemented within the FP1 MOTIONAL Federated Data Space demonstrator. This demo version was reduced in functionality since the main goal was the development of the underlying framework technology and IT infrastructure. The use case was live presented during the demonstration event and part of the validation.

2. Maintenance Decision Tool

The use case “Maintenance Decision Tool” was realized by the zentrak platform, a digital asset and

maintenance management solution that supports infrastructure managers in making data-driven maintenance and investment decisions throughout the complete lifecycle of railway assets. The tool combines asset information, maintenance records, condition monitoring data, and analytical results from external applications to provide a comprehensive decision-support environment. It is implemented as the asset management endpoint of the MOTIONAL Data Space demonstrator and serves as the consumer of prediction results generated by external Digital Twin and analytics services.

Within the implemented MOTIONAL use case, the Maintenance Decision Tool receives prediction results generated by the "Monitoring of Track Settlement and Identification of SingleFaults in Switches" application through the tmOS Marketplace (TMC central application hub). The transferred results are linked to the corresponding turnout and become part of the digital asset record. This allows maintenance engineers and asset managers to combine historical asset data, current condition information, and predicted future asset behaviour within a single software environment.
The Asset Management functionality provides a standardized asset and component register, lifecycle tracking, installation history, localization information, digital product passports, and asset health indicators. Maintenance Management functionality enables maintenance planning, inspection management, checklist-based execution, work order management, condition monitoring integration and trend analysis. Through these capabilities, maintenance strategies can evolve from corrective and preventive approaches towards condition-based and predictive maintenance.

A key element of the solution is the Digital Asset File concept. Each asset can be uniquely identified through a Digital Touch Point based on GS1-compliant Data Matrix Codes. By scanning the code, users obtain direct access to asset-related master data, technical documentation, maintenance guidelines, inspection records, warranty information, and lifecycle data. This allows maintenance personnel to access all relevant information directly in the field via mobile devices.

The Maintenance Decision Tool platform is designed for interoperability and can exchange data with external systems through standardized interfaces. Within the MOTIONAL demonstrator, turnout master data is synchronized with the tmOS Marketplace, while prediction results generated by external Digital Twin services are transferred back into the Maintenance Decision Tool for further analysis and maintenance planning. This demonstrates how a federated data space can connect data providers, analytics services, and asset management systems while maintaining data sovereignty and secure data exchange according to IDSA principles. An overview of the roles and requirements is given in Table 20.

Table 20. Overview of Roles and Requirements

Data Type	Size	Format	Provider	Consumer	Data Transfer
Turnout Master Data	KB	JSON	Asset Manager	Research Company	Pulled periodically, updated on demand
Maintenance Records	KB-MB	JSON	Asset Manager	Maintenance Manager	Updated regularly

Condition Monitoring Data	MB	JSON	Monitoring Systems	Asset Manager	Pulled periodically
Prediction Results	KB	JSON	Research Company	Asset Manager	Pushed automatically when available
Maintenance Recommendations	KB	JSON	Asset Manager	Maintenance Manager	Generated on demand

2.1 Implementation Status

The integration between tmOS Marketplace and zentrak has been implemented and demonstrated within the MOTIONAL Federated Data Space demonstrator. Turnout master data can be synchronized from zentrak to tmOS, and prediction results generated by external analytics services can be transferred back into zentrak and associated with the corresponding asset. The complete workflow from data acquisition through the federated data space, algorithm execution, and maintenance decision support has been successfully demonstrated during the validation activities of WP31

3. Digital Twin of Point Machine

This use case demonstrates how a Digital Twin of a railway point machine (LH 826) can be exposed as an interoperable data asset through a Federated Data Space, enabling secure and standardised data exchange between infrastructure managers, asset management systems, certification bodies and other authorised stakeholders. The data described here originates from FP1 WP29. Diagnostic data, health scores, simulation outputs and FMU-based evidence generated by the Digital Twin are made available through provider endpoints and consumed on demand by authorised participants using standardised interfaces.

Hitachi Rail Deutschland can act as the DATA PROVIDER, retaining full control over the data at source, while the Data Space holds only metadata, catalogue entries, access and usage policies, and contract templates. The Data Space itself does not store the actual data; all exchange occurs directly between connectors. This ensures that data sovereignty is fully maintained — no central copy exists and access is strictly governed through negotiated contracts and enforced usage policies.

The use case is closely aligned with FP1 MOTIONAL activities on point machine monitoring and predictive maintenance, where the Digital Twin of the LH 826 point machine is implemented as an FMU-based simulator. The simulator replicates the physical behaviour of the switch mechanism and publishes the following data assets through the Federated Rail Data Space:

- Point machine FMU diagnostic events (MDM format)
- Health score and Residual Useful Life (RUL)
- Operational state: Normal / Degraded / Fault
- Real-time data: current, force, stroke duration
- Simulation scenarios including fault injection

Development and validation of the LH 826 Point Machine Digital Twin simulator is based on FMU technology.

Publication of simulation outputs, health scores and FMU-based certification evidence is achieved through standardised provider endpoints using data space.

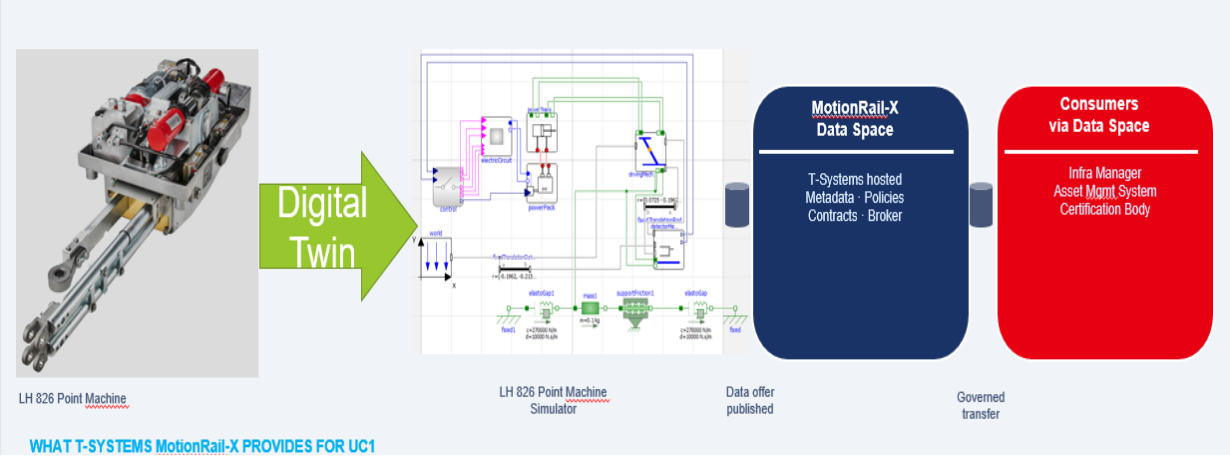


Figure 23. Overview of the use case: "Digital Twin of Point Machine"

3.1 Implementation Status

While the roles and requirements were specified for this use case as given in Table 21, a full implementation of the use case within the data space was not realized and will be the focus of wave 2.

Table 21. Overview of Roles and Requirements

Data Type	Size	Format	Provider	Consumer(s)	Data Transfer
Track Topology	MB	JSON	Railway Infrastructure Manager	Railway Operations Manager/Signalling Supplier	Pulled **on demand** or on update events; pushed manually or automatically when topology changes (e.g., quarterly).

Data Sensor	MB	JSON	Railway Infrastructure Manager/Technology Supplier	Maintenance Technician/ Technology Supplier/Signalling Supplier	Pushed in **real-time**, event-driven; transmitted when a train passes
Train Data	MB	JSON	Train Operator	Railway Infrastructure Manager/Signalling Supplier	Pushed in **real-time**, generated and transmitted when train passes that specific track section.
Track Maintenance Data	MB	JSON	Maintenance Company (i.e. Mermec, Hitachi)	Maintenance Technician/ Signalling Supplier	Pulled **on demand**; updated manually or through maintenance systems when activities are logged.
Weather Data	MB	JSON	External Weather service provider	Railway Operations Manager/Signalling Supplier	Pulled **on demand** from external/local weather service APIs or systems.

4. Track and Positioning regional Lines and Data Yard Automation

This use case demonstrates how train positioning and operational context information can be exposed as interoperable data services through a Federated Data Space, enabling secure and standardized data exchange between infrastructure managers, railway operators, service providers and other stakeholders. Positioning information acquired on board the train, together with contextual data describing the operational environment, are made available through provider endpoints and consumed on demand by authorized participants using standardized interfaces.

The proposed approach replaces bespoke point-to-point integrations with a scalable data-sharing architecture, allowing a single implementation to support multiple applications while remaining independent from the underlying communication technology. Connectivity therefore is transparent to the data services and can rely on terrestrial (4G/5G) or satellite communications according to operational availability.

The use case is closely aligned with FP6 activities on train positioning and train-to-cloud communications, where the on-board system acquires GNSS-based positioning data, processed through a Precision Navigation Module (PNM), and publishes both live vehicle position and contextual information through the Federated Data Space. This integration demonstrates how positioning evolves from a standalone function into a reusable digital asset capable of supporting multiple operational services, particularly in regional and non-interoperable railway environments.

The implementation has been progressively validated through laboratory integration and end-to-end demonstrations, including:

- Integration of the on-board application with GNSS/PNM positioning equipment for live train/vehicle positioning acquisition.
- Publication of live positioning and train context data through standardized provider endpoints.
- Successful interoperability testing with the FDS using provider and consumer connectors.
- Validation of on-demand data retrieval mechanisms for positioning, contextual information, and track geometry data.
- Integration of communication technologies with transparent support for both terrestrial and satellite connectivity.
- End-to-end validation of train-to-cloud data exchange, from the on-board system to authorized data consumers.

Figure 24 illustrates the overall architecture adopted for the use case. The on-board application acquires live train positioning and contextual information, which are exposed through FDS provider connectors. Data exchange is independent of the comms technology and can transparently rely on terrestrial (4G/5G) or satellite connectivity, enabling authorized consumers and services to access the information through standardized interfaces.

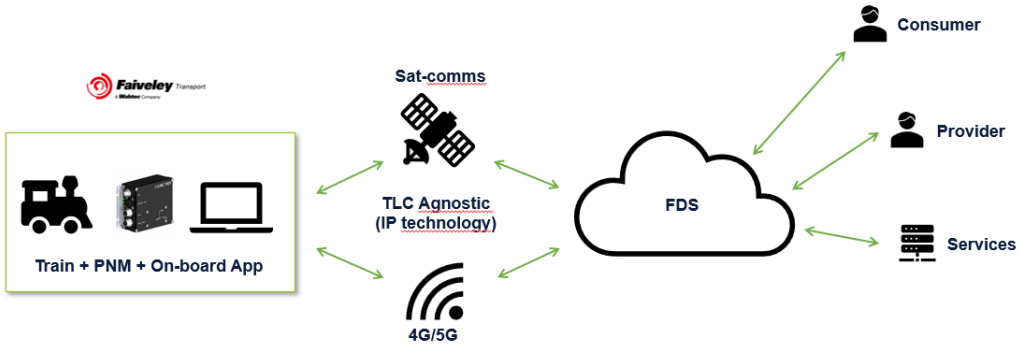


Figure 24. High-level architecture of "Track and Positioning regional Lines and Data Yard Automation" use case

4.1 Implementation Status

The implementation has been progressively validated through laboratory integration and end-to-end demonstrations, including:

- Integration of the on-board application with GNSS/PNM positioning equipment for live train/vehicle positioning acquisition.
- Publication of live positioning and train context data through standardized provider endpoints.
- Successful interoperability testing with the FDS using provider and consumer connectors.
- Validation of on-demand data retrieval mechanisms for positioning, contextual information, and track geometry data.
- Integration of communication technologies with transparent support for both terrestrial and satellite connectivity.
- End-to-end validation of train-to-cloud data exchange, from the on-board system to authorized data consumers.

The roles and requirements were specified for this use case as given in Table 22.

The use case successfully demonstrated the technical interaction between the Federated Data Space framework and the on-board positioning capabilities developed within EU-RAIL's FutuRe FP6 project, validating the feasibility of exposing interoperable train positioning and contextual data services. However, the activities within FP1 were primarily focused on establishing and validating this demonstrative integration, rather than delivering a fully operational and mature data-sharing service.

As this use case is not planned to continue within the FA1 Wave 2 activities, its further evolution from the Federated Data Space perspective falls outside the scope of this project. Nevertheless, the results achieved provide a solid foundation for future developments, and the demonstrated interaction can be further extended within EU-RAIL FA6 FutuRe Wave 2 activities, particularly in the context of G2 regional railway lines.

Table 22. Overview of Roles and Requirements

Data Type	Size	Format	Provider	Consumer	Data Transfer
Vehicle Position Records	kB	JSON	Railway Rolling Stock Operator	Regional Train Control Signaling System Integrator	Real-time dynamic data, pulled on demand or periodically by Yard/Regional systems; event driven.
Vehicle Context Records	kB	JSON	Railway Rolling Stock Operator	Regional Train Control Signaling System Integrator	Real-time dynamic data, pulled on demand or periodically by Yard/Regional systems; event driven.

Yard Track Topology	kB	JSON	Yard Manager Railway Infrastructure Manager	Regional Train Control Signaling System Integrator	Static data, pulled on demand or on update events; pushed manually or automatically when layout changes.
Regional Track Line Topology	MB	JSON	Railway Infrastructure Manager	Regional Train control Signaling system integrator Railway Rolling Stock Manager	Static data, pulled on demand or on update events; pushed manually or automatically when layout changes.

ANNEX B: Interaction with other Flagship Projects

This section describes the interactions between FP1-MOTIONAL WP31 and the other Europe's Rail Flagship Projects (FPs), with a focus on knowledge exchange, sharing of experience on data-space technologies and identification of potential cross-fertilisation opportunities. The main interactions concern FP3 (IAM4RAIL) and FP6 (FutuRe), which are the FPs whose scope shows the strongest thematic alignment with the Rail Data Space activities carried out in WP31 and whose use cases have been mapped in D26.2. Lighter, more general interactions with FP2, FP4, FP5 and FA7/System Pillar are summarised at the end of the section. In the case of sensitive documents, only this section will be shared with other FPs.

5. Interaction with FP3 – IAM4RAIL (Integrated Asset Management for Rail)

One of the main interactions with FP3 was the exchange of knowledge and experience on how a federated data-space approach can support asset-management processes, and to the identification of common ground for future cross-fertilisation.

Sharing of experience on data space technologies: the FP1 WP31 team shares with FP3 the lessons learned on the adoption of the IDSA reference architecture, on the role of the Metadata Broker as a discovery layer and on the governance implications of a federated approach, so that FP3 can take these elements into account when defining its own asset-management data flows.

In addition, the use cases relevant to the Federated Rail Data Space were collected in D26.2 and linked to FP3 (in particular the “Rail Infrastructure Data Federation” and “Monitoring of Track Settlement and Identification of Single-Faults in Switches” from WP 10 and WP11) are used as a reference to discuss with FP3 how a federated data space could, in the future, support similar asset-management scenarios.

6. Interaction with FP5

The interaction with FP5 focused on knowledge exchange with CEIT in Spain and on the planned onboarding of additional participants to the LivingLab. The activity was intended to broaden the range of organisations able to participate in the Federated Rail Data Space and to support the use of additional cross-Flagship use cases. In parallel, the exchange provided an opportunity to share experience regarding data space and connector technologies and thereby support technology acceptance beyond the immediate WP31 consortium context.

From the perspective of WP31, this interaction primarily addressed the organisational and integration requirements associated with extending a federated data space to additional participants. The planned onboarding demonstrated that the applicability of connector technologies depends not only on their technical capabilities, but also on the availability of suitable onboarding procedures and the ability of new participants to integrate their systems and organisational processes with the existing federation. This observation is consistent with the findings from the WP31 implementation and validation activities, which identified organisational onboarding and ecosystem integration as important prerequisites for the further deployment of Federated Rail Data Spaces.

7. Interaction with FP6 – FutuRe (Innovative rail services for regional and capillary lines)

The interaction with FP6 is focused on extending the discussion on the Rail Data Space to regional and multimodal contexts and on identifying opportunities for reciprocal contamination between the two FPs.
Knowledge exchange on regional use cases: the FDS-relevant use case collected in D26.2 and linked to FP6 (Track and Positioning Regional Lines & Data Yard Automation) is used to discuss with FP6 how the concepts developed in WP31 could be relevant for regional-line services and yard automation contexts: FP6's WP9 Task 9.10 demonstrator ("G2 Regional Lines of Train-to-Cloud Communications") offered an early practical use case for validating Federated Data Space connectivity outside a purely synthetic test environment. The demonstrator transmits train data – including GNSS-based positioning, integrated as part of WP10 Subtask 10.3.1 ("Individual demonstrators for Cost-effective fail-safe highly accurate train positioning on G2 lines") – from an onboard unit over commercial radio bearers (satellite as primary, cellular as fallback) to a cloud-side sandbox.

For the data-space leg of this chain, an EDC connector was provided by FSTechnology, allowing incoming train position/context data to be consumed and visualized (via a webapp developed by FT, with an integrated OpenStreetMap/Leaflet interface) on successful retrieval from the sandbox. Test traffic was routed to the T-Systems Data Intelligence Hub LivingLab / FDS sandbox using a lightweight tunnelling setup suitable for this demonstration stage.

While still limited to a sandbox-scale integration rather than a production data space, the exercise

confirmed that a G2-line train-to-cloud pipeline can hand off positioning and status data to an IDSA-compliant connector with no bespoken integration effort beyond the connector itself – a useful data point for WP31's broader interoperability goals.

ANNEX C: Validation Questionnaire

Based on the demonstrator, a Validation Event was held on 7. May 2026. There, the goal was to demonstrate TRL 6 "Technology demonstrated in a relevant environment (industrially relevant environment in the case of key enabling technologies)". According to BRIDGE2HE H2020-101005071[13], this means that "the prototype has to be demonstrated in a real environment, so to confirm the engineering is feasible". In case of a software, it has to be a "Beta version of the software functionalities tested by selected end-user under a control mode".

To test the functionalities, four validators were invited to test the data space. They were given access to the app store with 2 implemented use cases: the "Monitoring of Settlement and Identification of Single Faults in switches" and the "Maintenance Decision Tool" use case, along with an on-boarding session consisting of a presentation and a Q&A session. Then they were given a deadline of two weeks to test the capabilities. Afterwards they were asked to fill out a questionnaire. The detailed responses can be found in Table 23-Table 30.

Table 23: Participant Profiles

Question	Participant 1	Participant 2
Organisation Type	Infrastructure Manager	Research or University
Your Role & Data Focus	R&D	Technical

Table 24: Strategic Relevance & Expected Impact

Question	Participant 1	Participant 2
How relevant is the proposed Data Space to your organization	Moderately relevant	Moderately relevant
Which key business areas does it address?	• Maintenance & Reliability (e.g. predictive maintenance) • Data Integration & Interoperability (e.g. reducing fragmentation)	• Data Integration & Interoperability (e.g., reducing fragmentation)
What is your expected major impact of Rail Data Space	Cost reduction	Cross-border harmonization
What is the single most valuable expected benefit?	Easy access to data and services	Secure interoperability between systems

[13] BRIDGE2HE. (2022). Guiding notes to use the TRL self-assessment tool (Grant Agreement No. 101005071). Horizon Europe NCP Portal. Retrieved September 16, 2026, from https://horizoneuropencpportal.eu/sites/default/files/2022-12/trl-assessment-tool-guide-final.pdf

Table 25: Priority Use Cases for the Rail Data Space

Question	Participant 1	Participant 2
List your Top 3 use cases	• Bring together data & services/Algorithms from different partners à maintenance, Simulations	• improvements in safety and multimodal operating times • Digital twin developments of co-simulations • Decision support applications
Timeframe for adoption	More than 3 years	Less than 1 year
Primary adoption barrier	Financial (ROI/Cost)	Compliance (Legal/Gov)

Table 26: Technical Validation

Question	Participant 1	Participant 2
Which data would you share if provided with granular access controls?	To be discussed internally	Operational Data
What sovereignty guarantees are strictly required for you to share data?	• Strict Purpose Limitation (Cannot be used competitively) • Full Auditability & Ability to Revoke Access	• Strict Purpose Limitation (Cannot be used competitively) • Guaranteed Anonymization / IP Protection • Full Auditability & Ability to Revoke Access
Which standards are essential for interoperability?	-	• TSI • ISO/CEN/CENELEC • Asset Administration Shell (AAS) • IDS / Gaia-X
Which best describes your primary capability for external data integration today?	Level 2 (Transitional): Automated but point-to-point (e.g. custom APIs, SFTP file drops)	Level 4 (Advanced): Already utilizing decentralized data space connectors (e.g., Eclipse Dataspace Components)

Table 27: Governance & Trust Framework

Question	Participant 1	Participant 2
What is critical to build trust in the Data Space?	• Data sovereignty guarantees • Clear liability framework • Auditability	• Data sovereignty guarantees • Transparent access rules • Certification mechanism • Auditability
Would you participate in the creation of a governance board?	No	No

Table 28: Business Model & Sustainability

Question	Participant 1	Participant 2
Acceptable business models	-	Pay-per-use / Transaction
Required ROI timeframe	-	Strategic/Long-term only

Table 29: Risks & Critical Success Factors

Question	Participant 1	Participant 2
Biggest implementation risk?	-	A key point is the system's auditability. Failing to provide a seamless implementation could pose a risk to the adoption of these technologies by the railway ecosystem.
Biggest adoption barrier?		Legal issues involved in obtaining identification
Critical success factors (rank top 3)	• Regulatory backing • Technical maturity • Clear economic value	• Technical maturity • Industry alignment • Clear economic value

Table 30: Final Feedback / overall Validation

Question	Participant 1	Participant 2
What should be improved before moving to deployment	-	It would be nice to have the ability to share data directly from the connector
What would convince you to actively participate?	-	It would be beneficial to further promote the use of these types of systems among railway operators and infrastructure managers. I don't think they're ready for it yet.

Additional comments or recommendations?	• GUI is now designed for one application; there is a switch to zentrak. If other services exist in the future, the workflows in the GUI have to be updated, e.g. “transfer”-button • What about the legal and financial framework? Is it planned to integrate the processing of payment? For data and use of services?	-