SM4RTENANCE

European Deployment of Smart Manufacturing Asset 4.0 Multilateral Data Sharing Spaces for an Autonomous Operation of Collaborative Maintenance and Circular Services

Title	**SM4RTENANCE Portal & core services - First release**
Document Owners	Jeremy Decis (Dawex)
Contributors	Marcelo Ambrosio (Innovalia) Christian Racca (TOP-IX) Sebastian Opriel (Sovity) Maximilian Wagner (VDMA) Zisis Kyroudis (Atlantis),Vasiliki Vlahodimitropoulou (OTE), Pascal Hubert (AFN)
Dissemination	PUBLIC
Date	31/07/2025
Version	1.0

Digital Europe Grant Agreement N.101123490

Version History

Nr.	Date	Author (Organization)	Description
0.1	01/03/2025	Jeremy Decis (DAW)	Deliverable structure
0.2	01/04/2025	Jeremy Decis (DAW)	Initial Draft
0.3	15/06/2025	Jeremy Decis (DAW)	Second version integrating outcomes from the Bilbao SM4RTENANCE GA
0.4	01/07/2025	Marcelo Ambrosio (INNO)	Review by INNO, Added Sections 4.3.1, 4.3.4, 4.3.5, 4.5.
0.5	14/07/2025	Christian Racca (Top-IX)	Review by Top-IX
0.6	18/07/2025	Vasiliki Vlahodimitropoulou (OTE)	Review, Added Section 7.1, Contributions to 4.2.1, 4.2.2, 4.3.4, 4.4.1, 4.4.2
0.7	21/07/2025	Pascal Hubert (AFN)	Section 7.2
1.0	31/07/2025	Jeremy Decis (DAW)	Final version

Document Fiche

Authors	DAW
Reviewers	INNO, Top-IX, OTE
Work package	WP3
Task	T3.2, T3.3, T3.4, T3.5, T2.5, T5.3
Nature	DOCUMENT
Dissemination	PUBLIC
Keywords	Data space, Federation, Portal, Data exchange, Interoperability

Disclaimer

Acknowledgement

This document is a deliverable of the SM4RTENANCE project. This project has received funding from the European Union's Digital Europe programme under the call DIGITAL-2022-CLOUD-AI-03-DS-MANUF, GA N 101123490.

Table of contents

List of figures

List of Tables

Abbreviations and Acronyms

Acronym	Meaning
AAS	Asset Administration Shell
AASX	Asset Administration Shell Exchange
AI	Artificial Intelligence
AI-MATTERS	AI in Manufacturing TesTing and experimentation facilities for EuRopean SMEs
API	Application Programming Interface
BMBF	German Federal Ministry of Education and Research
CAD	Computer-aided design
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CLI	Command-line interface
DAPS	Dynamic Attribute Provisioning Service
DCAT	Data Catalog Vocabulary
DGA	Data Governance Act
DID	Decentralised Identities
DIY	Do it yourself
DMZ	Demilitarized zone
DPP	Digital Product Passport
DS	Data Space
DSSC	Data Space Support Center
DT	Digital Twin
DTR	Digital Twin Registry
EDC	Eclipse Dataspace Components
ERP	Enterprise Resource Planning
EU	European Union
FA3ST	Fraunhofer Advanced Asset Administration Shell Tools
FATE	Federated AI Technology Enabler
FL	Federated Learning
FRAND	fair, reasonable and non-discriminatory
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management
ID	Identification
IDS	International Data Spaces
IDSA	International Data Spaces Association
IDSI	IDS-Industrial Community
IDTA	International Digital Twin Association
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IIoT	Industry Internet of Things
IMF	Information Modeling Framework
IP	Intellectual Property

ISO	International Organization for Standardization
IT	Information Technologies
IaaS	Infrastructure as a Service
IoT	Internet of Things
KIT	Keep It Together
KPI	Key Performance Indicator
MES	Management Enterprise System
MIT	Masachussets Institute of Technology
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OPC	Open Platform Communications
OPC-UA	Open Platform Communications - Unified Architecture
OWL	Web Ontology Language
PCF	Product Carbon Footprint
PLC	Programmable Logic Controller
PMI	Product Management Information
PST	Prima Tool Service
PoC	Proof of Concept
QIF	Quality Information Framework
RDF	Resource Description Framework
REST	REpresentational State Transfer
RUL	Remaining Useful Life
SAMM	Semantic Aspect Meta Model
SDK	Software Development Kit
SGD	Stochastic gradient descent
SHACL	Shapes Constraint Language
SLA	Service Level Agreements
SME	Small and Medium Enterprise
SMTP	Simple Mail Transfer Protocol
STEP	Standard for the Exchange of Product Model Data
SaaS	Software as a service
TBC	To be confirmed
TEF	Testing and Experimentation Facility
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WP	Work Package
XML	Extended Markup Language
ZDM	Zero-Defect Manufacturing

List of partners

Short name	Legal name
AFS	AFNET SERVICES
ATLA	ATLANTIS ENGINEERING AE
AVL	AVL LIST GMBH
BAIDATA	ASOCIACION PARA DESARROLLO DE LA ECONOMIA DEL DATO
BEMAS	BELGIAN MAINTENANCE ASSOCIATION BEMAS ASBL
CARSA	CONSULTORES DE AUTOMATIZACION Y ROBOTICA SA
CEA	COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
CEFRIEL	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA' BENEFIT
CERTH	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS
COMAU	COMAU SPA
CORE	CORE INNOVATION AND TECHNOLOGY OE
DATAPIXEL	DATAPIXEL SL
DAWEX	DAWEX SYSTEMS
DGS	DGS SPA
DOM	DOMINA SRL
EFNMS	EUROPEAN FEDERATION OF NATIONAL MAINTENANCE SOCIETIES VZW
EITM	EIT MANUFACTURING SOUTH SRL
FIDIA	FIDIA SPA
FILL	FILL GESELLSCHAFT MBH
FIWARE	FIWARE FOUNDATION EV
Fraunhofer	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV
IDSA	INTERNATIONAL DATA SPACES EV
IJSS	IJSSEL TECHNOLOGIE BV
IMECH	CONSORZIO INTELLIMECH
INNO	ASOCIACION DE EMPRESAS TECNOLOGICAS INNOVALIA
ITEMA	ITEMALAB S.R.L.
MADE	MADE SCARL
NTTDES	NTT DATA SPAIN, SL
NTTDSL	NTT DATA SPAIN SOLUCIONESTECNOLOGICAS SL
OTE	ORGANISMOS TILEPIKOINONION TIS ELLADOS OTE AE
PIA	INDUSTRIE 4.0 OSTERREICH – DIE PLATTFORM FUR INTELLIGENTE PRODUKTION
PIAC	FRATELLI PIACENZA S.P.A.
PRIMA	PRIMA INDUSTRIE SPA
SCHN	SCHNEIDER ELECTRIC INDUSTRIES SAS
SCSN	STICHTING SMART CONNECTED SUPPLIER NETWORK
SIE	SIEMENS AKTIENGESELLSCHAFT
SOVITY	SOVITY GMBH
SQS	SOFTWARE QUALITY SYSTEMS SA
SYXIS	SYXIS VSI

TNO	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO
Top-ix	CONSORZIO TOP-IX - TORINO E PIEMONTEEXCHANGE POINT
TRIMEK	TRIMEK SA
TXT	TXT E-TECH SRL
UiO	UNIVERSITETET I OSLO
UNI	UNIMETRIK SA
VDI	VDI TECHNOLOGIEZENTRUM GMBH
VDMA	VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU (VDMA)

1. Executive Summary

The SM4RTENANCE project aims to enable the deployment of federated, trusted, and interoperable manufacturing Data Spaces across Europe. Leveraging open-source technologies, standardized protocols, and Gaia-X and IDSA-aligned frameworks, this first release focuses on establishing the foundational technical and semantic building blocks required to support collaborative maintenance, circular economy services, and industrial data sharing.

This deliverable presents the initial architecture and core services that form the basis of the SM4RTENANCE Data Space federation. These include a modular frontend portal, a centralized backend engine, and supporting infrastructure that jointly facilitate identity management, semantic interoperability, data product registration, and trusted data exchange.

The SM4RTENANCE Portal acts as a federative orchestrator, enabling selective onboarding, cross-domain data interoperability, and access to decentralized services such as identity federation, digital twin registries, and federated catalogues. The architecture has been designed through a collaborative process involving technical partners and pilot leads, and it anticipates future integration with SIMPL and other European middleware ecosystems.

This first release ensures GDPR and DGA compliance, define the path to integrate with Gaia-X and Dataspace Protocol (DSP) standards, and to provide extensible services to support use cases such as predictive maintenance, asset lifecycle management, and business model innovation. It lays the groundwork for the upcoming M30 release and for broader alignment with EU Data Space strategies.

2. Introduction

The transformation of Europe's industrial base towards greater digital sovereignty, innovation, and competitiveness requires new foundations for how data is accessed, exchanged, and governed. The European Strategy for Data, published by the European Commission in February 2020, sets a clear ambition to create a single market for data that will ensure Europe's global leadership in the data-driven economy. Central to this vision is the deployment of sectoral and cross-sectoral Common European Data Spaces—federated infrastructures that enable trustworthy, sovereign, and interoperable data sharing across organisations, countries, and domains.

Within this policy framework, the manufacturing sector has been identified as one of the priority domains for the establishment of a Common European Data Space. The goal is to unlock the potential of industrial data to support more efficient production, predictive maintenance, circular business models, and the emergence of digital services built around trusted data exchange. Achieving this vision requires robust, standards-based architectures that combine technical enablers (identity, semantics, connectivity) with governance mechanisms and compliance frameworks aligned with EU regulations such as the GDPR and the Data Governance Act (DGA).

The SM4RTENANCE project contributes directly to this European effort. It focuses on enabling a federated, multilateral manufacturing Data Space that supports the collaborative use of industrial data assets, particularly those related to smart assets, predictive maintenance, and lifecycle optimization. By leveraging open standards (Gaia-X, IDSA, DCAT, RDF, SHACL), distributed architectures (EDC, DAPS, DIDs), and operational services validated

through industrial pilots, SM4RTENANCE creates the conditions for deploying a sustainable and extensible data ecosystem aligned with the European Data Strategy.
This deliverable (D3.1) presents the first technical implementation release of the SM4RTENANCE Data Space Services and Portal. It builds upon the architectural vision and harmonization principles defined in previous work (notably D2.2) and translates them into a coherent set of modular, functional, and compliant services. These services aim to support the secure and interoperable exchange of data across industrial actors, while respecting the sovereignty of participants and enabling the emergence of decentralized business models.
The development process for this first release followed a collaborative and iterative methodology. Technical and domain experts from across the SM4RTENANCE consortium co-designed the architecture, with early drafts shared on collaborative platforms (e.g. Miro) and refined during the January 2025 General Assembly in Lyon. This participatory approach ensured that the resulting infrastructure reflects the needs of real-world pilot use cases while maintaining alignment with reference frameworks such as Gaia-X, the Dataspace Protocol (DSP), and the upcoming European Data Innovation Board.

The document is structured as follows:

- Section 2 outlines the purpose and scope of the deliverable.
- Section 3 introduces the SM4RTENANCE reference architecture, including its compliance with GDPR and DGA, and its compatibility with European standardization initiatives.
- Section 4 presents the SM4RTENANCE technical architecture, describing both frontend and backend layers, the collaborative design process, and the services included in the first release.
- Section 5 outlines the roadmap towards the M30 release and the consolidation of federation services.

This deliverable is a key milestone for the project, as it operationalizes the architectural foundation of the SM4RTENANCE Data Space. It defines the minimal set of capabilities required to support identity federation, catalogue federation, data product registration, semantic interoperability, and trusted access control. Furthermore, it provides a clear entry point for onboarding participants and evaluating real industrial scenarios.
In the broader context of the Common European Data Spaces strategy, this deliverable contributes to:

- Demonstrate the technical feasibility of interoperable and trusted data sharing in manufacturing.
- Test the alignment of open-source building blocks with European legal and governance frameworks.

Ultimately, SM4RTENANCE aims to transition from isolated pilot deployments around specific manufacturing use cases into a federated ecosystem of interoperable manufacturing Data Spaces, thereby supporting Europe's strategic autonomy, industrial resilience, and innovation capacity as active participants of the data economy.

2.1 Purpose and scope of the deliverable

The purpose of this deliverable is to formally document the initial release of the SM4RTENANCE Data Space Services and Portal, which collectively constitute the foundational infrastructure for enabling trusted, interoperable, and sovereign data sharing across European manufacturing ecosystems. This release forms part of the strategic roadmap of SM4RTENANCE to support the deployment of federated Data Spaces aligned with the European Strategy for Data and contributes to the operational realization of a Common European Manufacturing Data Space.

As stated in the European Commission's Communication on the European Strategy for Data (2020), establishing sectoral Data Spaces—including manufacturing—is central to achieving Europe's digital sovereignty. These Data Spaces are intended to facilitate the availability, discoverability, interoperability, and lawful re-use of industrial and business data, with full respect for European values and regulations. Within this context, SM4RTENANCE acts as a first mover in designing and implementing a Data Space federation portal.
The first release presented in this deliverable is a milestone in this trajectory.
Specifically, this deliverable addresses the following objectives:

- To provide a detailed specification of the technical architecture for the SM4RTENANCE Data Space Federation, including the layering, modular structure, and service composition of both frontend and backend components.
- To describe the first release of SM4RTENANCE services, covering identity federation, digital twin registration, catalogue services, and semantic vocabulary services.
- To demonstrate the alignment of the proposed services with European reference frameworks such as Gaia-X, the International Data Spaces Reference Architecture Model (IDS-RAM), and the emerging Dataspace Protocol (DSP).
- To provide evidence of GDPR and DGA compliance
- To explain how the infrastructure enables selective federation models, allowing for domain-specific, cross-domain, and multi-layered configurations depending on industrial requirements and levels of maturity.

The scope of the deliverable is deliberately focused on delivering a minimal, functional, and extensible infrastructure that supports real-world onboarding and federation scenarios in the pilot domains of SM4RTENANCE (e.g., metrology, machine tools, weaving machines, textile, robotics). It does not attempt to cover the full range of envisioned features for the M30 release but instead establishes a stable and standards-aligned foundation upon which future iterations can build.
The deliverable also outlines how the architecture is open to future integration with complementary European initiatives, including:

- **SIMPL (Smart Middleware for Interoperability**): While evaluating SIMPL assets has revealed current limitations in maturity and modularity, SM4RTENANCE remains aligned with the long-term ambition of interoperating with SIMPL-Labs and SIMPL-Open.
- **Gaia-X Federation Services**: The architecture is compatible with Gaia-X compliance models, service self-description, and integrating Gaia-X Digital Clearing Houses for future trust verification and governance enforcement.
- **Open-source infrastructure components**: The support of Eclipse Dataspace Components (EDC), ODRL for policy enforcement, and standardized vocabularies (DCAT, RDF, AAS) positions SM4RTENANCE for continued evolution in line with the open and community-driven development practices endorsed by the European Commission.

In summary, the deliverable serves as:

- Technical Blueprint: It provides a reference for the design and implementation of the initial deployable version of the SM4RTENANCE Data Space.
- Enabler for Regulatory Compliance: It demonstrates compliance with relevant EU regulatory and legal frameworks.

- Operational Guide: It offers practical instructions for pilot users, service providers, and future stakeholders.
- Strategic Enabler: It contributes to the broader vision of a modular, federated European Manufacturing Data Space, aligned with the Common European Data Space strategy.

2.2 Relation to other WPs and tasks

Deliverable D3.1 constitutes a foundational output directly supporting and operationalising the goals defined under several interdependent tasks within the SM4RTENANCE project.

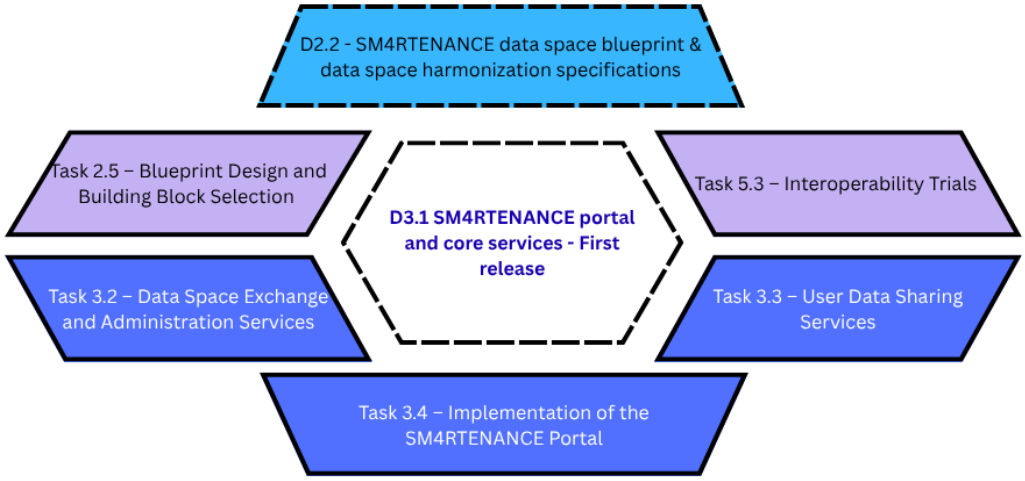


Figure 1. Deliverable D3.1 in relation to other tasks and deliverables.

Task 2.5 – Blueprint Design and Building Block Selection

The design and implementation choices described in this deliverable are grounded in the architectural vision and harmonization specifications established in Task 2.5. D3.1 builds upon the SM4RTENANCE blueprint defined in **Deliverable D2.2** and translates it into deployable service components. The layered modular architecture of the Portal—comprising frontend interaction layers, backend orchestration, and semantic services—has been selected and structured based on the blueprint building blocks identified in T2.5. Furthermore, D3.1 validates the operational environment foreseen in T2.5 by instantiating core services (identity federation, vocabulary service, semantic hubs) that enable federation and interoperability across manufacturing Data Spaces. The deliverable also lays the groundwork for later alignment with external initiatives such as Catena-X, Manufacturing-X, and D4IX through extensible design patterns.

T3.1: Data space infrastructure & interconnection services

Task 3.2 – Data Space Exchange and Administration Services

The first release presented in D3.1 includes key elements required by T3.2 to support Gaia-X aligned data exchange and administration capabilities. Specifically, it operationalizes modules for consent and licensing management, catalogue federation, and ID provisioning. These components have been partially implemented or prepared for future integration, in line with the latest Gaia-X specification. The Portal enables registration, discovery, and controlled access to data offerings through standardized service descriptions and verifiable credentials, thereby addressing the trust and administration requirements defined in T3.2.

Task 3.3 – User Data Sharing Services

The deliverable partially fulfils Task 3.3 by introducing foundational services such as the Data Space Services Broker in case services need a layer to standardise them or aggregate them. These elements support future implementation of user data sharing services, including data provenance, traceability, and anonymisation, as outlined in T3.3. The architecture integrates DLT-compatible service placeholders and includes provisions for multi-tenant catalogues and trust models. Moreover, the enabling of data sharing rooms and service brokers anticipates the deployment of more advanced data clearing mechanisms in future releases.

Task 3.4 – Implementation of the SM4RTENANCE Portal

This deliverable is the core implementation outcome of Task 3.4. It documents the initial technical release of the SM4RTENANCE Portal, including its modular frontend (semantic UI, digital twin UI, network visualisation) and backend services (vocabulary service, metadata broker, credential manager). The portal is implemented as a federation enabler rather than a monolithic application, supporting multiple onboarding pathways (e.g. Sovity Data Space portal, DConnect, MX-Port) and semantic interoperability through shared vocabularies and ontologies. Services for semantic validation, participant registration, and policy-based access control are all implemented in accordance with the specifications defined under T3.4.

Task 5.3 – Interoperability Trials

The components and federation models described in D3.1 will serve as the technical basis for the interoperability trials planned under T5.3. This includes the infrastructure-level federation approaches—such as Shareable DAPS/Broker and MX-Port alignment—and the implementation of interfaces for cross-space identity recognition and catalogue discovery. The portal architecture has been explicitly designed to accommodate and validate interconnections between internal and external Data Spaces, with clear provisions for supporting the SM4RTENANCE compliance and certification framework as required by T5.3 and discussed in WP5 meetings.

2.3 Structure of the deliverable

Deliverable D3.1 is structured to provide a comprehensive overview of the first technical release of the SM4RTENANCE Portal and core services, positioning it within the broader context of the project's architecture, federation strategy, and compliance vision. The document is organized into six main sections:

1. **Executive Summary**

   This section provides a concise overview of the objectives, scope, and outcomes of the deliverable. It

highlights the importance of the portal in enabling federated, trusted, and interoperable data exchange across European manufacturing domains.

2. **Introduction**

The introduction situates the deliverable within the strategic objectives of the European Data Strategy and the SM4RTENANCE project. It outlines the purpose and scope of the deliverable, its alignment with relevant tasks and work packages, and its role as a stepping stone toward a modular and compliant manufacturing Data Space.

3. **SM4RTENANCE Data Space Reference Architecture**

This section presents the foundational architecture that underpins the SM4RTENANCE ecosystem. It elaborates on architectural principles, alignment with EU data regulations (GDPR, DGA), compatibility with Gaia-X and the Dataspace Protocol, and the project's evaluation of SIMPL as a potential integration layer. The section offers both conceptual and compliance-focused insights.

4. **SM4RTENANCE Technical Architecture**

The core of the deliverable, this section details the technical structure of the portal and services. It covers the collaborative design process, infrastructure layering (frontend/backend), enabling services, and federation models. Subsections describe specific components including the semantic hub, identity federation services, the digital twin registry, and the integration of multiple federation pathways (Sovity Data Space Portal, DConnect, MX-Port).

5. **Path Towards M30 Release**

This forward-looking section outlines the strategic vision for the next release (M30), describing the targeted capabilities, methodological approach, and validation strategy. It defines key milestones for scaling the federation and enriching the service stack.

6. **Conclusion**

The deliverable concludes with a synthesis of achievements, a reaffirmation of its contribution to EU Data Space ambitions, and an outlook on the continued deployment and refinement of the SM4RTENANCE ecosystem.

3. SM4RTENANCE Data Space reference architecture

As the foundational technical chapter of this deliverable, Section 3 introduces the reference architecture underpinning the SM4RTENANCE Data Space federation. This architecture is the result of a structured co-design process involving technical partners, domain experts, and pilot stakeholders, and aims to address the specific needs of federated data sharing in the European manufacturing sector. It operationalizes the vision outlined in previous work packages and deliverables—most notably D2.2 on harmonisation specifications—and transforms it into a coherent and deployable framework that aligns with the broader European Data Strategy[1].

The architecture presented in this section is modular, extensible, and fully aligned with emerging European standards and regulatory expectations. It integrates architectural primitives derived from Gaia-X, the International Data Spaces Association (IDSA), and the Dataspace Protocol (DSP[2]), while also ensuring compliance with key legislative frameworks such as the General Data Protection Regulation (GDPR) and the Data Governance Act (DGA[3]). Particular emphasis is placed on federation-enabling components—such as identity management, service discovery, and semantic interoperability—that support sovereign, secure, and trusted collaboration among industrial stakeholders.

This section also provides the conceptual structure of the SM4RTENANCE Data Space architecture across layers and roles. The framework defines a clear distinction between data producers, consumers, intermediaries, and service providers, outlining their responsibilities, flows, and interactions within a dynamic, multilateral, and scalable federation model. Additionally, it details the enabling infrastructure and compliance mechanisms required to support onboarding, interoperability, and data transaction monitoring in a legally robust and operationally sustainable way.

The reference architecture sets the logical composition of services and acts as a strategic blueprint for implementing Data Spaces that are compatible with other sectoral or cross-sectoral ecosystems in Europe. As such, it sets the stage for future convergence with related initiatives, including SIMPL, the Data Spaces Support Centre (DSSC[4]), and national-level digital twin infrastructures.

This section provides the technical and conceptual backbone of the SM4RTENANCE infrastructure by presenting a reference architecture grounded in real industrial needs. It serves both as a foundation for the current release and as a roadmap for subsequent iterations, including the consolidation and generalisation of federation patterns foreseen in the M30 milestone.

3.1 Architecture principles

3.1.1 An architecture compliant with EU data regulations (GDPR, Data Governance Act)

The SM4RTENANCE project is designed to enable a federated, trusted, and interoperable manufacturing Data Space in Europe. At its core is the SM4RTENANCE Portal and its accompanying services, which are engineered to

[1] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
[2] https://github.com/eclipse-dataspace-protocol-base/DataspaceProtocol
[3] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[4] https://dssc.eu/

operationalize the principles of the European data strategy. This framework is built upon a commitment to regulatory compliance, particularly with the General Data Protection Regulation (GDPR [5]), the Data Governance Act (DGA), and the Data Act.

3.1.1.1 Compliance with the GDPR

- *Data Sovereignty and Participant Control:*
  - Each participant maintains full control over their own data and business logic, supporting GDPR's data minimization and purpose limitation principles.
  - Data transactions are policy-based, transparent, and consent-driven, aligning with GDPR Articles 6 and 7[5] on lawful processing and consent.
- *Verifiable Credentials and Identity Management:*
  - The architecture's backend includes a centralized credentials manager to manage credentials (W3C VC6), roles, and permissions, ensuring secure access and policy enforcement for all users and services. This component is designed to be compatible with future federated identity frameworks, providing a scalable and trustworthy foundation.
  - This approach supports Article 5(f)[7] and Article 32[8]
- *Policy-Based Access and Usage Control:*
  - ODRL-based (Open Digital Rights Language) access control policies allow participants to define, enforce, and audit conditions for data use, which is critical for ensuring GDPR-aligned accountability and purpose limitation.

3.1.1.2 Compliance with the Data Governance Act

The SM4RTENANCE architecture reflects several guiding principles of the EU Data Governance Act (DGA), though not through direct implementation of its legal framework. It incorporates mechanisms intended to support data sovereignty, notably by supporting Eclipse Dataspace Components (EDC), allowing for decentralized control over participant data exchange. The onboarding process includes participant identification steps designed to promote trust and transparency, partially addressing the DGA's expectations around intermediary roles.
The SM4RTENANCE Federation will support access and usage of data managed through policy enforcement using ODRL (second release), which enables a level of traceability aligned with best practices in data accountability. While not a full certification mechanism, the project introduces a framework to assess the compliance of key components and services against technical and interoperability requirements.
By being compliant with open standards and drawing on architectural guidelines from Gaia-X, SM4RTENANCE aims to lay down a technically solid foundation for sovereign and lawful data exchange within the European manufacturing ecosystem.

3.1.1.3 The SM4RTENANCE services as an enabler of compliance

The SM4RTENANCE Portal's enabling services are central to its compliance framework.

[5] https://gdpr-info.eu/chapter-2/
[6] https://www.w3.org/TR/vc-data-model-2.0/
[7] https://gdpr-info.eu/art-5-gdpr/
[8] https://gdpr-info.eu/chapter-4/

- **Federated Identity Management**: The Identity Federation service enables the creation, management, and validation of identity information for participants. This service provides proofs that other participants can use for authentication and authorization, supporting decentralized identity and trust propagation. In the second release, the planned support for Decentralized Identifiers (DIDs) and a Dynamic Attribute Provisioning Service (DAPS) will further enhance this by enabling verifiable, decentralized identity and up-to-date attribute information in a zero-trust environment.
- **Interoperable Catalogues:** The Virtual Data (Product) Catalogue provides a directory of available services and data products. These data products are presented in a consumable format, allowing for easy discovery and self-service. This transparency and discoverability are key requirements of the Data Act. The catalogue also uses standardized metadata models such as DCAT v3 and RDF, ensuring that data is described semantically rich and machine-readable, which is crucial for cross-organizational data sharing, aligned with the Article 33 of the Data Act.
- **Data Space Service Monitoring**: The monitoring services ensure transparency, accountability, and operational coherence across the federated Data Space. These services are essential in a federated context due to the heterogeneity and distributed nature of the participants. They provide auditable and verifiable information about data, policies, and services across the ecosystems, which is critical for meeting the transparency and accountability requirements of the DGA and Data Act.
- **Data Space Protocol (DSP) Compatibility**: The long-term ambition of SM4RTENANCE is to be compatible with any Data Space that uses DSP-capable connectors, which is on track to become an ISO/IEC standard. The architecture is designed to be open and flexible, avoiding vendor lock-in and paving the way for innovation across different industrial sectors. This commitment to open standards and interoperability aligns with the EU's strategic vision for a single market for data.

3.2 Alignment with standardization efforts in Europe (Gaia-X, DSP)

3.2.1 Alignment with Gaia-X and European Standards

The technical implementations of the SM4RTENANCE architecture will be compatible with key global Data Space standardisation initiatives:

- **ISO/IEC CD 20151**[1] standard on conceptual foundation of Data Spaces, entitled **'Cloud computing and distributed platforms – Data Space concepts and characteristics',** and **Dataspace Protocol (DSP)**[2], which is currently an Eclipse project and in the process of becoming an ISO/IEC standard.
- Regardless of the underlying technology, all components will also be fully aligned with the ongoing work and de facto standards of **Gaia-X**, ensuring interoperability and compliance within the trusted European data infrastructure.
- From an open-source standpoint, SM4RTENANCE will notably leverage and support key frameworks such as:
    - **EDC – Eclipse Dataspace Components**: the cornerstone open-source connector for secure, sovereign data exchange within and across Data Spaces.
    - **SIMPL**: providing core open-source Data Space components and building blocks.
    - **AAS Specifications:** Define the software structure, interface, and semantics of the Asset Administration Shell, thereby establishing the foundation for the standardized Digital Twin.

The architecture relies on standardized metadata models and technologies such as Gaia-X Self-Descriptions, DCAT v3, and RDF/JSON-LD, ensuring semantically rich, machine-readable representations of participants, datasets, and services. This level of semantic expressiveness is fundamental to support scalable, discoverable, and portable data exchange across different domains and organizations.

This architecture underscores SM4RTENANCE commitment to building a trustworthy, future-proof, and standards-aligned digital ecosystem.

3.3 SIMPL: opportunities for future integration

SIMPL "Smart and Secure Middleware for Promoting Interoperability[9]" is an open-source, smart and secure middleware platform that promotes data access and interoperability across European Data Spaces. SIMPL is deployed across Data Spaces with both centralized and decentralized components. The Smart Middleware Platform is comprised of four architectural layers: the data layer, the infrastructure layer, the administration layer, and the governance layer.

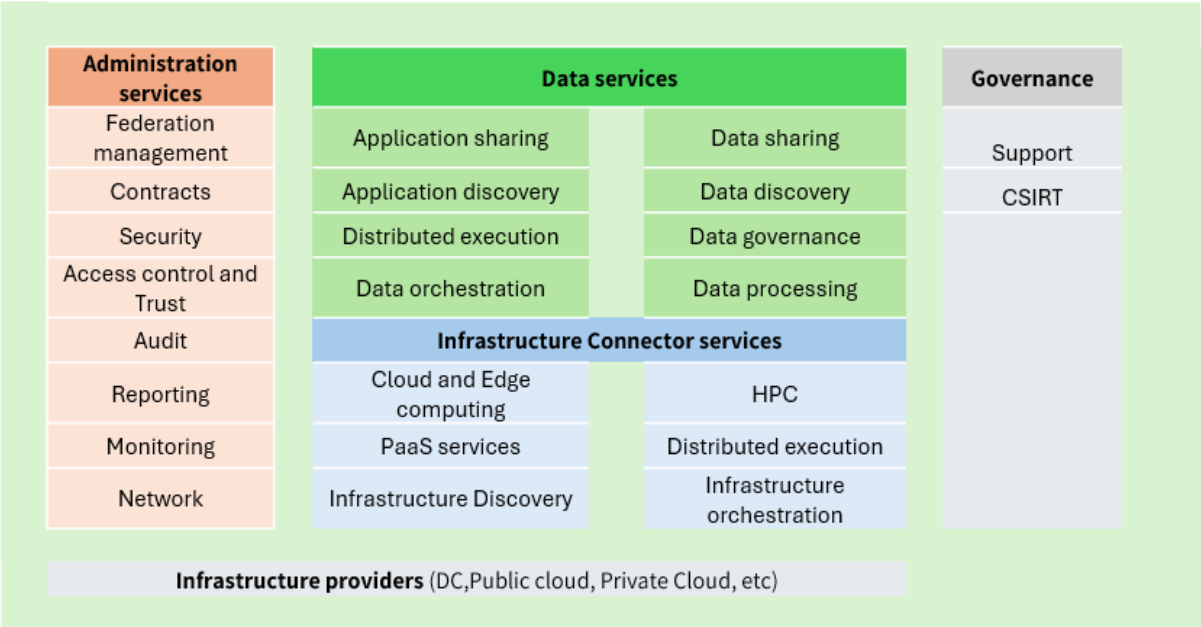


Figure 2. High-level overview of SMP capabilities and architecture layers.

The Data layer comprises the foundational elements necessary to exchange data assets and applications. The Service Management Platform (SMP) provides data consumers with the tools to access various types of data from

[9] https://digital-strategy.ec.europa.eu/fr/policies/simpl

multiple providers, facilitating interoperability between providers and consumers. This layer includes services for sharing and managing data and applications, as well as conducting basic analyses.

The infrastructure layer is responsible for the management of infrastructure assets. This layer allows the SIMPL Platform to connect with third-party infrastructure services, enabling end users to run applications on them. The middleware does not directly provide infrastructure; instead, it enables infrastructure providers to disclose their internal infrastructure to participants in the Data Space. Platform as a Service (PaaS) offerings, such as databases and artificial intelligence hardware, as well as fundamental computing and storage resources like virtual machines and file system storage, can be made available. The infrastructure layer empowers end consumers to discover, use and manage the infrastructure services offered by infrastructure providers. The infrastructure providers offer infrastructure resources and services to the end users to enable them to process the data provided by the data providers. Cloud service providers members of the Gaia-X and SM4RTENANCE initiative can offer services aligned with the Gaia-X principles.

The Administration layer vertically encompasses both the data and infrastructure layers. It provides essential services necessary for the optimal functioning of these layers, as well as the Service Management Platform (SMP) as a whole. These services include security, identity management, access control, monitoring, and more. The administration layer enables the federation of various actors within Data Spaces, enabling them to operate their components effectively.

The governance layer performs cross-cutting functions that are applicable to all of the previously described layers, as it provides potential contingency measures against issues that participants may encounter.

SIMPL is developing a Minimum Viable Product (MVP) that offers the fundamental functionalities required by the majority of Data Spaces. Once this objective is accomplished, SIMPL will be made available to the community for maintenance and improvement, thereby becoming an entirely open-source program.

SIMPL consists of three products: SIMPL-Open, SIMPL-Live, and SIMPL-Labs.

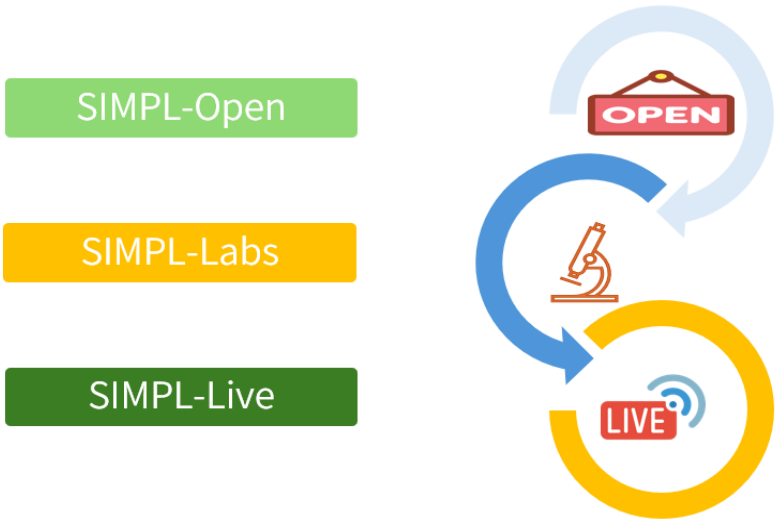


Figure 3. Figure 3: SIMPL components.

SIMPL Open is the open-source software stack that powers Data Spaces and other cloud-to-edge federation initiatives. SIMPL-Open emphasizes leveraging and collaborating with the Data Spaces and open-source community through the use of open-source code, among other methods.

SIMPL-Live represents the adoption of SIMPL-Open within specific Data Space instances. It consists of studies that analyse the feasibility of deploying the SIMPL-Open software stack in identified Data Spaces funded by the European Commission, as well as its implementation. The real-world deployments of SIMPL-Open in identified Data Spaces illustrate how SIMPL-Open can be applied across various sectors, showcasing its versatility and effectiveness in facilitating data-driven innovation.

SIMPL-Labs is a testing environment designed for Data Spaces to evaluate interoperability with SIMPL. It allows sectoral Data Spaces to experiment with deployment, maintenance, and support in their early stages. Additionally, it enables mature Data Spaces to assess their interoperability with SIMPL Open.

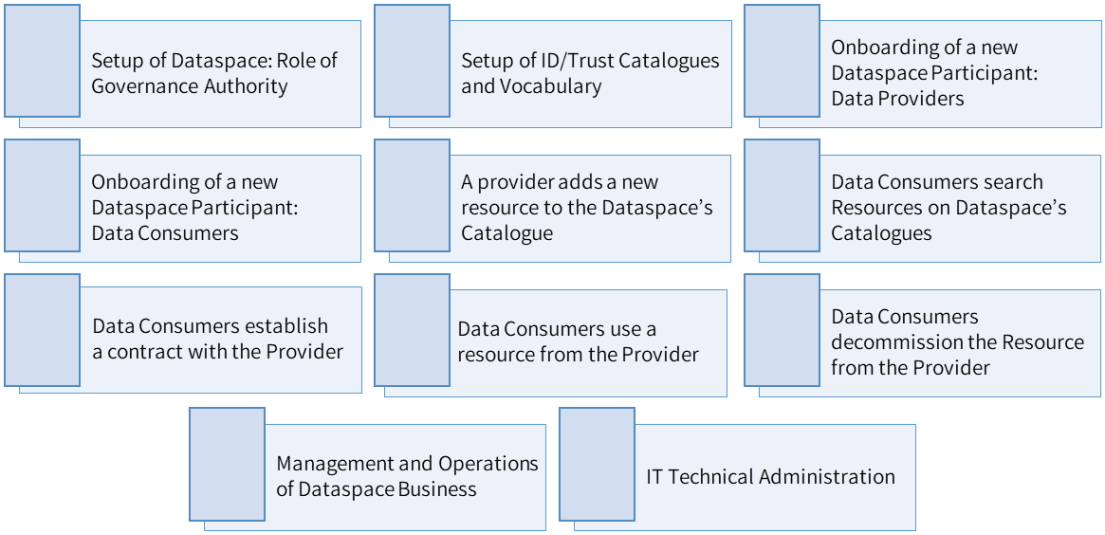


Figure 4. SIMPL Business processes related to Data Spaces.

3.3.1 Status & analysis by SM4RTENANCE and vision for future integration

In order to assess a potential integration of SIMPL assets, the technology providers for SM4RTENANCE have systematically reviewed all SIMPL components that are available, part of their MVP, and examined their technical specificities. The evaluation focused on the availability, implementation status, documentation quality, and maturity level of each component, as well as their relevance and alignment with SM4RTENANCE requirements. The overall assessment reveals that the majority of components are not yet mature or ready for production.
Despite being marked as MVPs, most of SIMPL Open components available face significant implementation or usability issues:

Repository Availability: A majority of components lack public or accessible repositories. For those that are available, the situation is still problematic:

- Many repositories are incomplete,

- Either the documentation is missing, or
- The code is not functional or usable.

Maturity Evaluation:

- Several critical services—such as identity management, authorization, and data orchestration—are not expected to support Self-Sovereign Identities (SSI) before 2026, significantly limiting trust and sovereignty goals in the short term.
- Key modules (e.g., encryption, authenticity verification, usage contracts) are either entirely missing or not usable in their current form.

Dependency on SIMPL Governance: Many core federation components (e.g., resource catalogues, metadata services) cannot operate independently from the SIMPL Governance Authority, reducing flexibility and reusability.

SM4ETENANCE will continue to follow SIMPL deliveries and assess future integrations scenarios as soon as components are ready to be used in an operational environment?

4. SM4RTENANCE technical architecture

The **SM4RTENANCE Data Space Portal** is designed to enable **secure, interoperable,** and **sovereign** data exchange across the manufacturing value chain. Its implementation incorporates open-source technologies, standardized protocols, and cloud-native infrastructure to foster a decentralized and collaborative data ecosystem.

4.1 Collaborative design process

The first release of the SM4RTENANCE portal and core services is the result of a co-design process that engaged technical and domain experts from across the project consortium. The collaborative approach followed a structured sequence:

1. **Initial assessment of available technologies**

   The process began with an internal mapping of existing tools, platforms, and technologies available within the consortium. This included both mature systems and emerging solutions, with the aim of identifying potential components for the initial release. The work has been done leveraging the conclusion of the D2.2 SM4RTENANCE Data space blueprint & harmonisation specifications about the standards, frameworks and technologies relevant for the vision of the project.

2. **Drafting and feedback collection via Miro**

   Based on this assessment, a preliminary architecture draft was prepared. A dedicated Miro board was set up to facilitate asynchronous feedback from all partners. This collaborative workspace enabled partners to annotate, suggest improvements, and discuss alternatives across the different layers of the proposed architecture.

3. **Consolidation during General Assembly in Lyon (January 2025)**

   The proposed architecture was then discussed and refined during the 3rd General Assembly meeting held in Lyon. Feedback from technical partners, pilot leads, and work package coordinators was incorporated to arrive at a consolidated and shared version of the SM4RTENANCE infrastructure.

This participatory design process ensured that the portal and core services architecture align with the needs of the use cases while leveraging the existing strengths of the consortium members.

4.2 Overview of the infrastructure proposal

The SM4RTENANCE infrastructure proposal, drafted and consolidated through the collaborative process described in the previous paragraph, is structured around two main layers:

- **Frontend (Portal / Web Application)**
- **Backend (Centralized Services Engine)**

Together, these layers form the foundation of the SM4RTENANCE ecosystem and will support its modular approach.

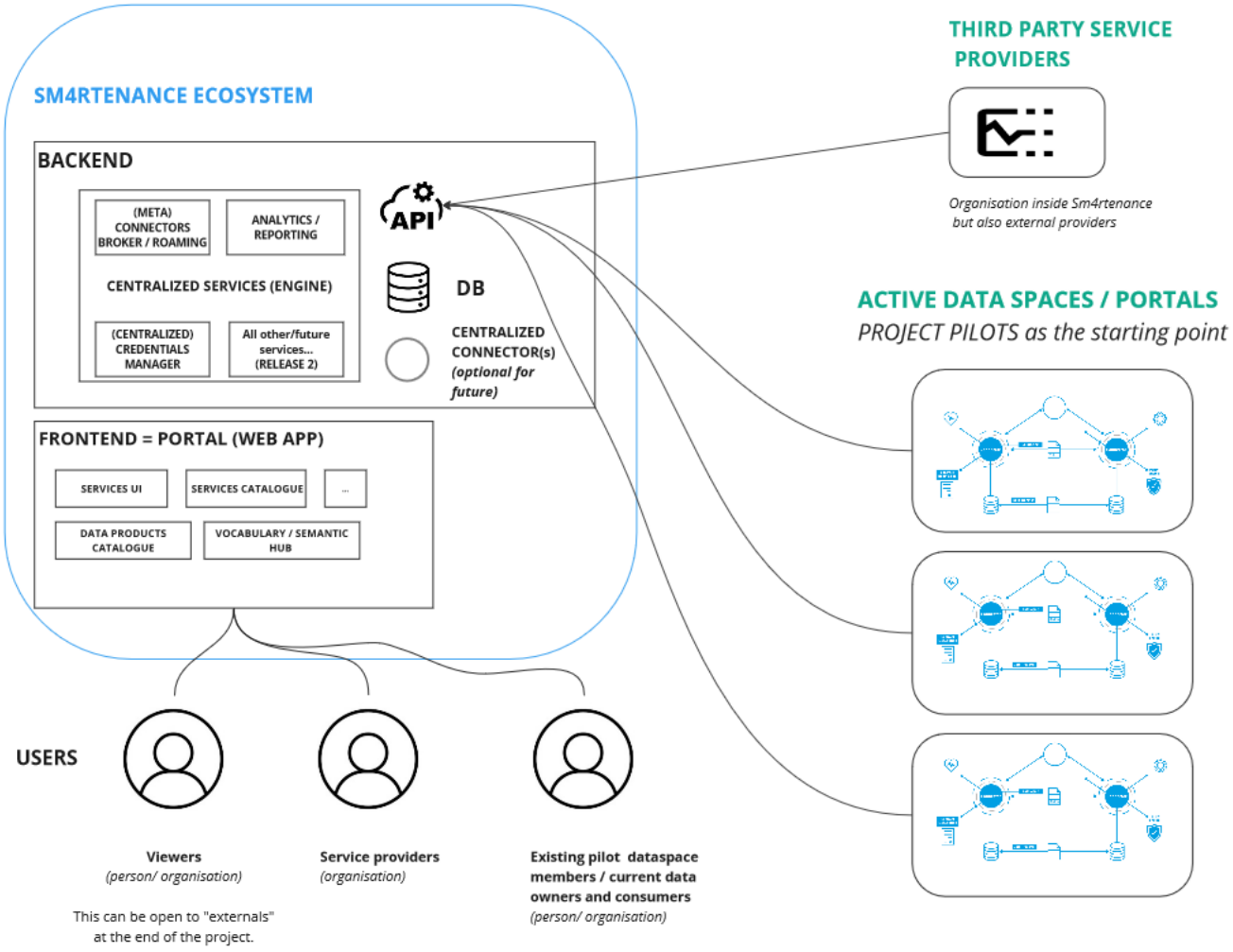


Figure 5. SM4RTENANCE federation architecture.

4.2.1 Frontend – Portal layer

The frontend layer of the SM4RTENANCE infrastructure is envisioned as a modular and extensible **web-based portal**, acting as the main entry point for users into the SM4RTENANCE ecosystem. It supports various user roles and journeys, including onboarding, service discovery, and Data exchange.

The key elements proposed for inclusion are:

Component	Description
Service UI	A unified user interface that should enable smooth access to the portal's functionalities. The UI is intended to support various user journeys, including

	onboarding, service usage, and platform navigation. Its design will evolve to accommodate different user roles and levels of expertise.
Service catalogue	The portal is expected to offer a catalogue of services made available within the SM4RTENANCE ecosystem. This would include both core infrastructural services and domain-specific services offered by pilot partners or third parties. The catalogue aims to be browsable and searchable, facilitating intuitive discovery and selection.
Data product catalogue	A central element of the user experience will be the catalogue of available data products. This feature is proposed to present data assets in a structured and accessible way, supporting their discoverability and reuse within and across pilot domains.
Data Transaction catalogue	To promote transparency and traceability, the portal is expected to include a component that provides users with a historical and real-time view of data exchanges. This will also support future needs around auditing, accountability, and usage monitoring.
Vocabulary/semantic Hub	A critical enabler for semantic interoperability is proposed as a frontend-integrated service that provides users with access to shared vocabularies, ontologies, and controlled terminologies. Its role will be to harmonize access to data products and services, supporting semantic alignment across the ecosystem. Semantic Hub hosts standardized data models that ensure the data shared across the Data Space is semantically consistent. This consistency facilitates accurate interpretation and integration by various systems.

4.2.2 Backend

The backend layer of the SM4RTENANCE infrastructure is conceived as a **Centralized Engine** that will provide the technical backbone for orchestrating interactions, enforcing policies, and enabling secure and sovereign data exchanges within the ecosystem. While some of these components may evolve into distributed or federated services in later releases, the current proposal focuses on a pragmatic, centralized implementation to accelerate integration and pilot readiness.

The following components are proposed as part of the initial backend structure:

Component	Description
(Meta) Connectors	These are envisioned as the primary tools for connecting single Data Spaces. The goal is to integrate standardized connectors, potentially aligned with IDSA specifications, to ensure compatibility across Data Spaces.

Service catalogue	A service catalogue is proposed as a centralized mechanism for registering and discovering services, while the roaming function will allow the ecosystem to interface with external Data Spaces and third-party registries.
Centralized credentials manager	To ensure secure access and policy enforcement, a centralized identity and access management (IAM) component is proposed. This service will manage credentials, roles, and permissions for all users and services. It is also intended to be compatible with future federated identity frameworks, ensuring scalability and trust propagation.
Analytics / reporting module	Basic analytics and reporting capabilities are proposed to support platform monitoring, usage statistics, and early insights generation. The priority will be on logging, service usage tracking, and generating summary metrics for internal evaluation. More advanced AI/ML-driven analytics are planned for later releases.
Database layer (DB)	A centralized data store is proposed to support the operational needs of the portal. This includes storing metadata, service definitions, user credentials, audit logs, and data transaction records. The design is intended to ensure performance, reliability, and compliance with data protection regulations.
All other / future services (Scaffold)	The architecture anticipates future extensions, with a placeholder for additional backend services. These may include data valuation engines, contract negotiation modules, or digital twin integration.

Table 1. Portal structure components.

4.3 The SM4RTENANCE Portal

This section introduces the SM4RTENANCE Portal as a strategic infrastructure to federate European manufacturing Data Spaces. The SM4RTENANCE Portal is positioned as a strategic backbone for a future-proof European manufacturing Data Space ecosystem.
It:

- enables domain-specific and cross-domain interoperability
- supports flexible federation models tailored to business needs
- delivers concrete, pilot-driven implementations
- aligns with Gaia-X, IDSA, and upcoming EU Data Space frameworks.

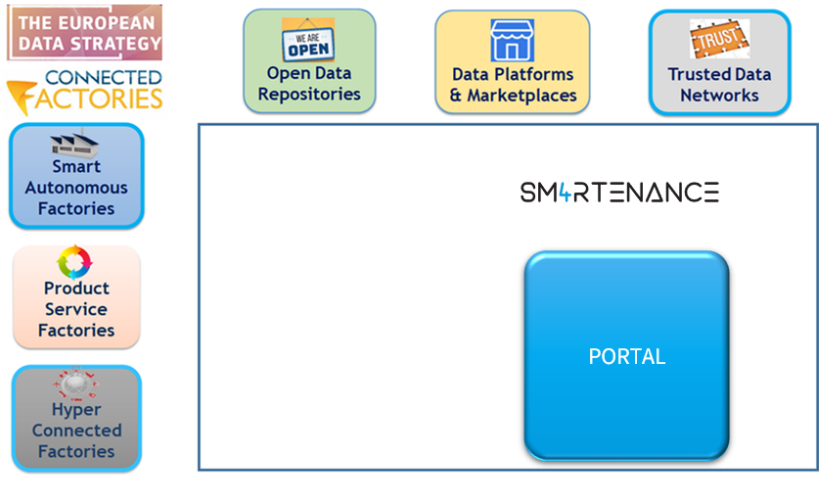
The Portal is not only a technical platform; it is a governance and enablement infrastructure, empowering industrial actors to move from isolated pilots to a confederated, trusted, and interoperable data economy.
The project builds upon the Data Space 4.0 vision and addresses key industrial needs:

- Deployment of operational Data Spaces focused on specific manufacturing use cases.
- Cross-domain data interoperability to increase data reuse and collaboration across industrial actors.
- Support for autonomous service development, including AI-powered predictive maintenance and digital twins.
- Establishment of a Data Space Services Portal to ensure seamless integration and discovery of interoperable services and Data Spaces operators and providers
- Trust framework governance enabling secure and sovereign data exchange through common rules, identity services, and policy enforcement.

The Portal is not merely a technical layer; it is conceived as a federative orchestrator linking Data Spaces, data platforms, and data marketplaces into a coherent, trust-based European ecosystem.
The Portal acts as an intermediation layer between:

- Data Platforms hosting internal industrial data.
- Data Marketplaces exposing valorised data sets for external consumers.
- Trusted Data Spaces formed around federated domains.

The Portal services support connections across multiple ecosystems, reducing fragmentation and lowering the entry barriers for companies, especially SMEs. A core objective is to enable "connect once, collaborate many": companies avoid repetitive integration across silos by interfacing once with the federation.
The Portal is built as a federation enabler, not a monolith, but as a set of modular services supporting decentralized governance, selective onboarding, and extensible interoperability.



- DATA PLATFORMS host more independent confidential **Trusted Industrial Data.**
- DATA MARKETPLACES offer external customers **Valorised Data Sets** provided by Manufacturing Data Spaces.
- **SM4 PORTAL** services link Trusted Data Networks and Data Platforms / Marketplaces federations.
- INDUSTRIAL AI PLATFORMS build models and leverage on cognitive Industrial Digital Twins and SM4 Trusted Data Networks

Figure 6. SM4RTENANCE Positioning and scope.

4.3.1 SM4RTENANCE Portal: the vision

The objective of the SM4RTENANCE Portal is to support the federation of a high diversity of manufacturing domains, to integrate different verticals into the data exchange economy.

- SM4RTENANCE Pilots: Metrology (TRIMEK), Weaving Machines (ITEMA), Laser Cutting (PRIMA), Machine Tools (FIDIA, FILL), Industrial Robots (COMAU), and Textile DPP (PIACENZA), Collaborative Asset Maintenance (IJssel), e-vehicle Battery remaining useful lifetime prediction (AVL).
- External Data Spaces (D4IX, UNDERPIN, Catena-X, etc)

Business Application	Pilot number	Pilot owner	Title
COOPERATIVE CONDITION MONITORING (PdM)	1	TRIMEK	Building a Certified Digital Twin with Data Spaces for Dimensional Quality Control Equipment
	2	ITEMA	Overall Predictive Maintenance through Trusted Data Sharing
	3	FIDIA	Machine Tool Usage Data Sharing
ASSET 4.0 COLLABORATIVE ENGINEERING	4	AVL	Improving Health and Performance of (e)-vehicles
	5	FILL	Milling machine predictive maintenance with Data Spaces
COLLABORATIVE NET-ZERO OPERATIONS SERVICES	6	PRIMA	Smart Predictive Maintenance for laser cutting systems
	7	COMAU	Life Cycle Assessment through Energy Monitoring
	8	IJSSEL	Collaborative Asset Monitoring at a large scale via the existing data space Smart Connected Supplier Network

CIRCULAR ASSET MANAGEMENT	9	PIACENZA	Optimization of the Production Performance through DPP

Table 2. Pilot alignment with the four SM4RTENANCE cores business applications.

The envisioned federation Model allows multiple Data Spaces to remain autonomous while benefiting shared services, such as catalogue federation, identity management, and policy enforcement. As it will be discussed below, the Interoperation agreements – and their degrees – can range from the Data Space level via the federation channels, all the way up to large scale sectoral alignment efforts.

This modular approach acknowledges that different business domains require different federation topologies, and that one-size-fits-all architectures are neither scalable nor acceptable in real-world industrial contexts.
The model supports both vertical (domain-specific) and horizontal (cross-sectoral) collaboration, and provides a multi-layered entry path for industrial actors depending on their maturity and role in the value chain, a common place where industry participants can converge and create new value and business opportunities around the data exchange.

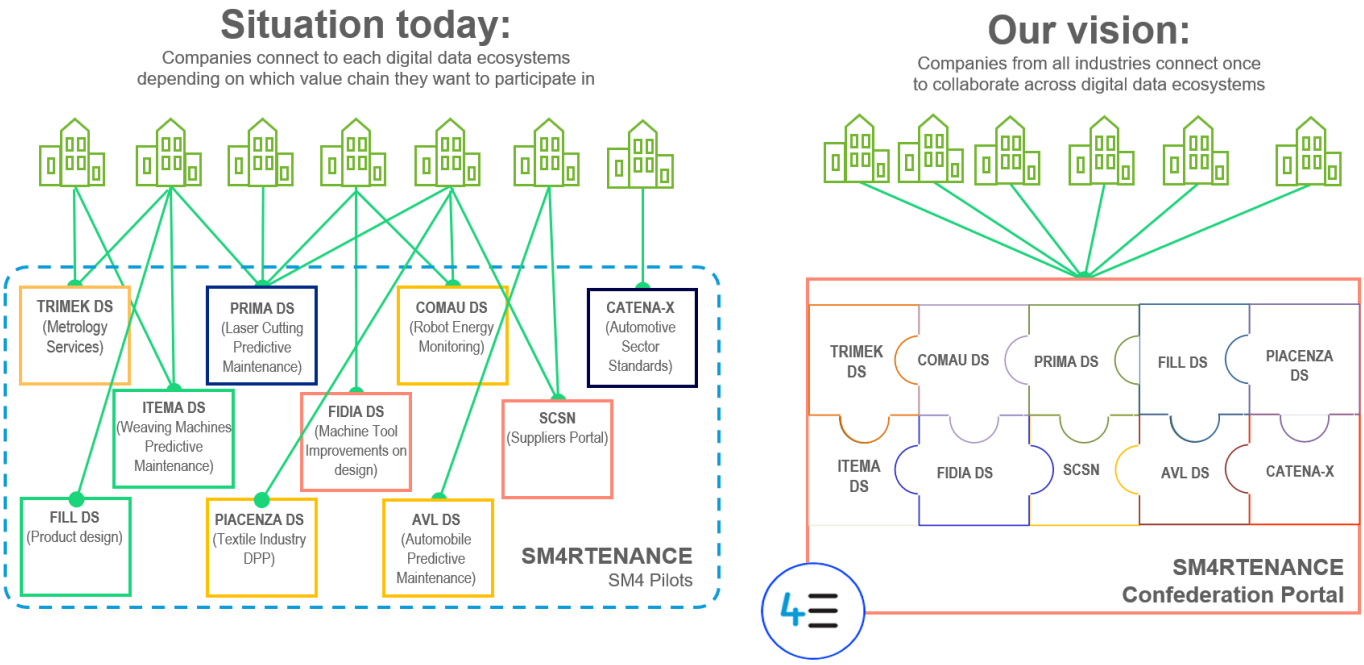


Figure 7. SM4RTENANCE vision.

4.3.2 SM4RTENANCE Portal: the federation layers

4.3.2.1 The federation architecture

The federation architecture can be classified by sectoral scope: Data Spaces centred around affine use cases can choose to streamline their operations with each other, beyond catalogue visibility and mutual ID acknowledgement. Conventions by sector regarding the data, standards adhered to, and pricing are expected to emerge. The large-scale vision of the SM4RTENANCE federation encompasses a number of Data Spaces, leaving room for alignment or aggregation by sector. The sectoral-level federations are set to be administered by consolidated intermediaries, as will be discussed below.

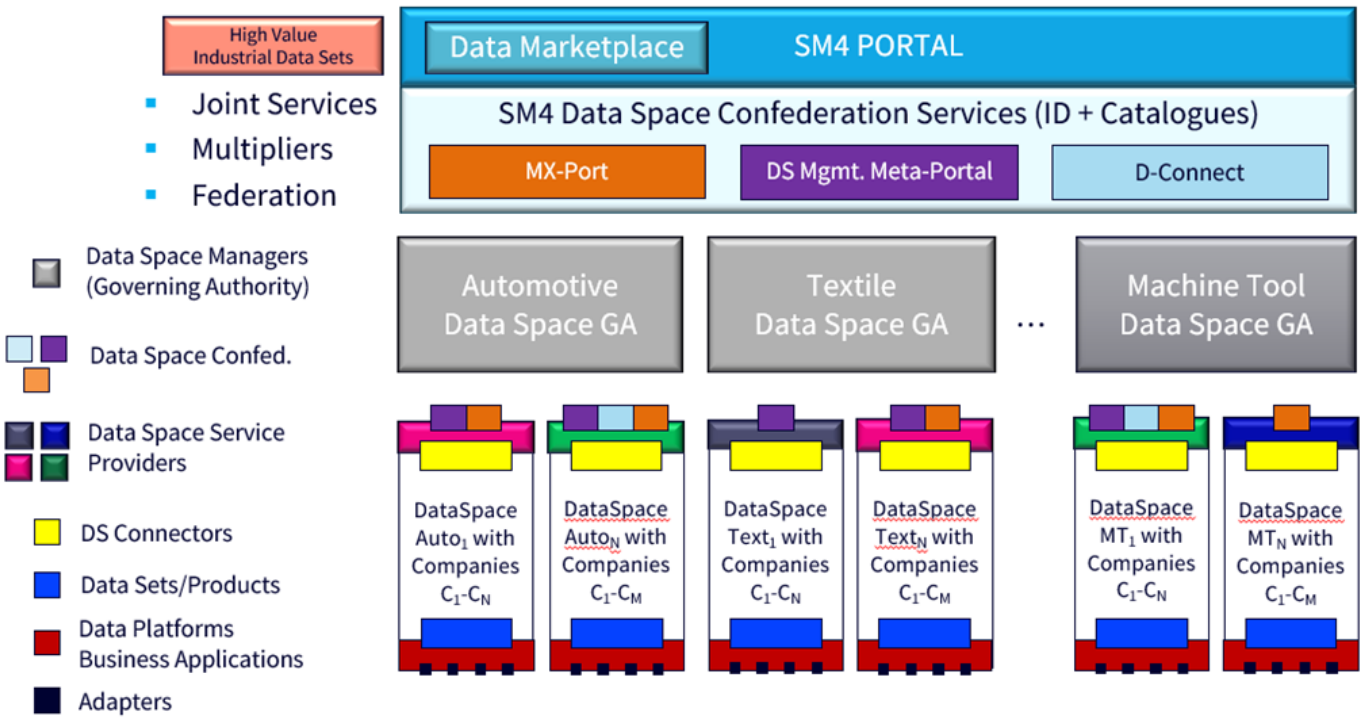


Figure 8. SM4RTENANCE Federation layered approach.

From the bottom layer to the top components:

- **Data Space level:** Each individual Data Space relies on a Data Space Service Provider (DSSP), and gathers a number of companies (participants) that exchange data at that scale. Participants who intend to act as data providers funnel their data into the Data Space environment via the Adapter stage (in a similar vein to the MX-Port Adapter stage, which will be described below), which lifts it from either the shopfloor itself or company ERP systems. Partners may continue operating their preexisting platforms, handling the data exchange through the Data Space, and offering their Data Products in its environment.
- **Intermediary/Sector-level federation:** Sector-specific intermediaries can define additional rules, data standards, practices and regulations for data exchange between similar-trade partners. As Data Spaces are founded around related interests, commonalities should be identified and used to gradually define

standards from the overall consensus (**Semantic bridging** between domain-specific ontologies and templates, **Data pooling** for research and multi-DS analytics use cases, **Pre-visibility compliance** validation**, use case libraries** and toolkits).

- **SM4RTENANCE Federated Data Platform and Portal:** This layer streamlines participation across the entire federation, abstracting away complexities for end users to bring business use cases to fruition. It should expose a straightforward interface for end users, while on the backend being able to work with multiple federation approaches, tailored to the involved partners' data framework specifics. Directly from the Portal, external entities will be able to browse and trade for data sets put on display on the
- **Data Marketplace**. The Data Marketplace is a component of the Portal that will expose data sets for external entities to transact for. These are not regular data sets; quite on the contrary, these will be highly relevant, precise, polished and well-documented ones, voluntarily made available to the market by participants from any Data Space within the federation. These so-called High Value Industrial Data Sets are expected to generate business opportunities with non-federated organisations.

At the time of writing, the federation layer targets unifying different Data Spaces, bridging identities and catalogues from each one, into a wide visibility ecosystem. The intermediate, sector-specific layer concept is yet to be defined, although potential examples to occupy these niches are large entities with a track history in the sector, e.g., Euratex for the Textile sector, Catena-X for the Automotive industry.

The Portal architecture relies on three main **confederators**, that enable the connection with different ecosystems that use different technologies:

- **Sovity Portal:** Federation-wide registry for participants, data offers, and policies from various and heterogenous technology frameworks.
- **D-Connect**: Enables interconnection between identity and catalogue services across domains.
- **MX-Port:** From the shopfloor or ERP systems up to reaching findability across a DS system

The Portal supports selective federation, where each Data Space can opt in to specific shared services without compromising sovereignty.

4.3.2.2 Sovity Portal

In this model, **Sovity Data Space portal solution acts as a metaportal to** aggregate multiple connectors.
Pilots using Sovity's Connector-as-a-Service technology can readily onboard, as their data connectors plug directly into the Sovity meta-portal environment. This means their data offerings and participant information automatically become visible on the SM4RTENANCE Portal to other participants. In contrast, pilots not using Sovity connectors require an integration API so the portal can ingest their Data Space information. The development of such APIs is currently assigned to SQS, Top-IX and CORE, in order to bridge non-Sovity-based systems into the Metaportal. Therefore, the Sovity-based Metaportal approach offers a quick path for those already aligned with Sovity's stack, while still allowing others to connect via standard APIs.
The Metaportal approach architecture is displayed in Figure 3 below.

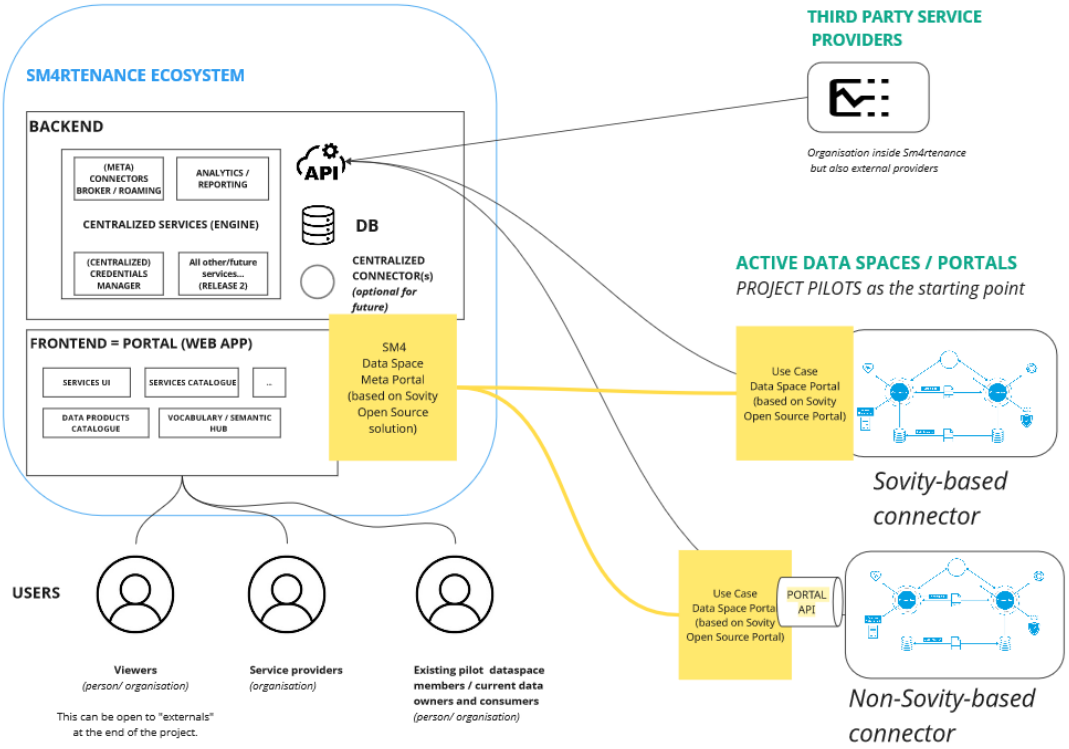


Figure 9. Metaportal solution architecture, in yellow, with its ability to federate Data Spaces, whether or not they rely upon Sovity's connector services.

4.3.2.3 Shareable DAPS/Broker solution (DConnect by SQS)

Highlighting Key Concepts

The federation approach described here enables multiple Data Spaces to interoperate without centralizing control or depending on a single Data Space Service Provider. It builds upon mutual trust, standard-compliant identity management, and shared catalogue services to allow seamless discovery and secure data exchange across independently operated infrastructures.

Federation Model for Interoperable Data Spaces

Rather than enforcing a single entry point or vendor-specific access, this model enables each participant to continue operating its own Data Space connector. The federation is achieved through the linkage of two critical infrastructure elements: identity and catalogue services. Participants agree to interconnect these services under a shared trust and protocol framework, forming a decentralized but interoperable ecosystem.

Identity Trust & Cross-Recognition

Federated identity is based on mutual recognition of credentials issued by IDSA-compliant Identity Providers. If the involved Data Spaces use such providers, the federation enables cross-recognition via a shared DAPS (Dynamic Attribute Provisioning Service) and/or Broker. These components allow participant information and access tokens to be trusted across the federation, ensuring that permissions and identities are consistently enforced without the need for central control.

Federated Discovery & Catalogue Sharing

Data discoverability is achieved through the federation of catalogue services. Participants share a common resource catalogue, making each participant's data offerings visible to others. Even when two pilots operate distinct connector platforms, they can still discover and consume each other's assets as long as they trust each other's identity services and use the same federated catalogue. This mechanism ensures interoperability without requiring uniform software stacks.

Decentralization & Platform Agnostic

At its core, this model promotes decentralization: no single portal holds all the data or metadata. Instead, interoperability is achieved through mutual agreements on identity claims, catalogue standards, and broker protocols. It avoids vendor lock-in by remaining agnostic to the underlying connector implementation. Moreover, the federation is non-binding—participants can dissolve it at any time without impacting their standalone operations, as each Data Space remains fully functional independently.

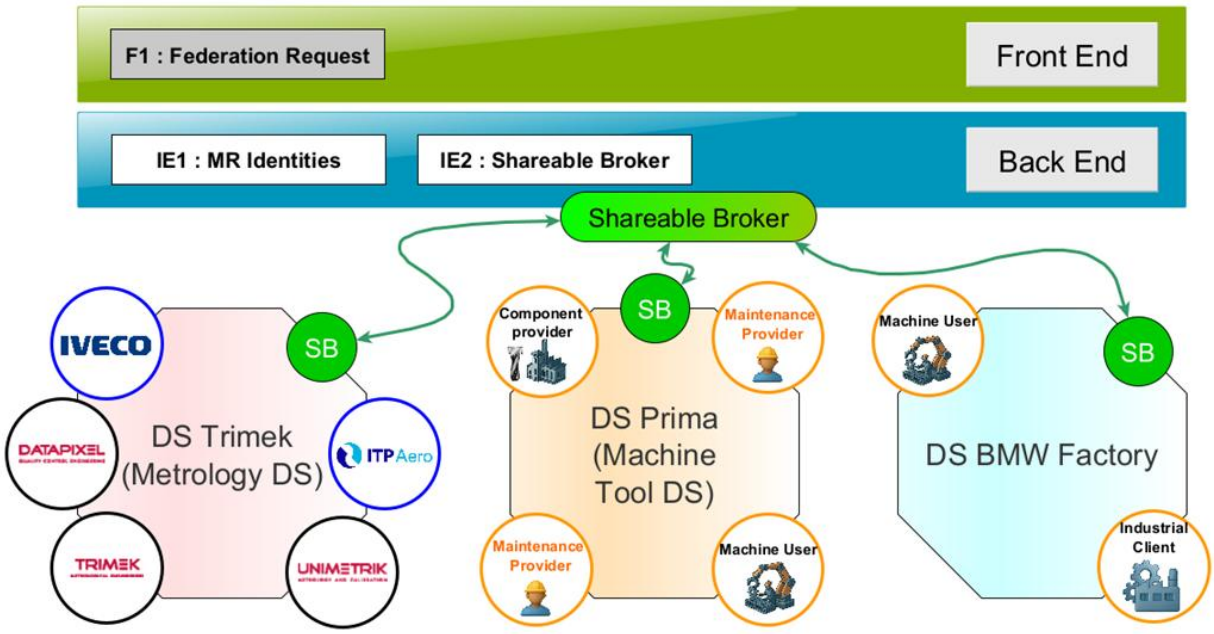


Figure 10. Shareable DAPS/Broker approach, highlighting the shared catalogue interaction between three example Data Spaces.

4.3.2.4 MX-Port Solution and its five-layer structure:

The SM4RTENANCE Portal is evolving towards integration with the Manufacturing-X "MX-Port" concept. This forward-looking solution aligns with the reference architecture being developed under the Manufacturing-X umbrella (notably by the Factory-X project). The MX-Port solution envisions a standardized integration port for manufacturing Data Spaces, which is essentially a common blueprint that any Data Space implementation can follow to achieve interoperability.

In the context of SM4RTENANCE, adopting the MX-Port concept means the portal will make use of the MX-Port five-layer architecture (detailed below) to interface with various data sharing frameworks in a uniform way. SM4RTENANCE adopts a **shared, multi-layer integration model** that leverages standardised adapters, semantic

models, and communications protocols across five different layers rather than merely bridging specific connectors or catalogues. This design promotes openness, scalability, and alignment with decentralized technologies, ensuring it remains future-proof.

The MX-Port approach is considered a longer-term solution, as it aims to provide an open, extensible framework that can accommodate future standards and decentralized technologies beyond what current connector systems offer. The planned support for an MX-Port-based federation option will contribute to positioning SM4RTENANCE as a first-line cross-Data-Space operation in the long run.

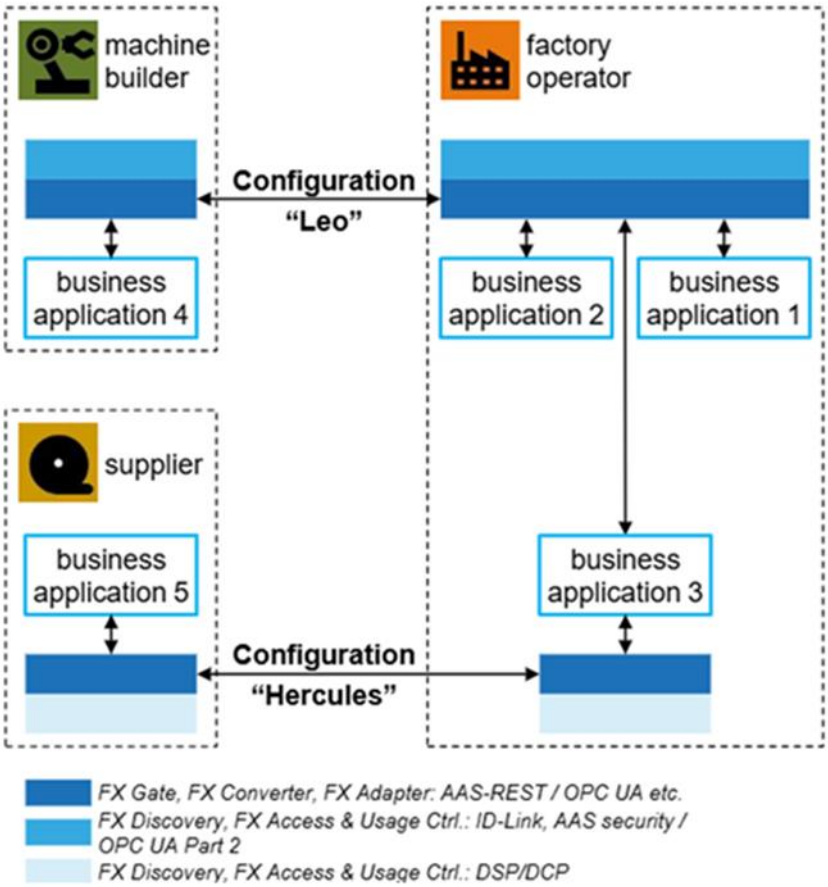


Figure 11. Depiction of MX-Ports interconnection flexibility to enable cooperation between players along a value network, tailored to each pair's technical specifications.

We describe the five layers from bottom to top, i.e., starting from the point where the data is gathered from the source and ending at the layer where it is made searchable for business partners.

Adapter [*Connection to business apps*]: The lowest layer, i.e., the one closest to the machine floor, enables any business application to use the MX-Port by interfacing with data sources or systems. In practice, a Layer 1 component could be a plugin or connector that extracts data from a machine, an ERP system, or an IoT platform's API. It translates proprietary or application-specific data formats and protocols into a form with which the MX-Port's higher layers can work.

Converter [*Semantic model translation*]: The second layer is called Converter and provides the semantic modelling for the data to be exchanged. In other words, Layer 2 is responsible for semantic mapping and normalization. Data from Layer 1 (which can originate from different formats or schemas) gets translated at Layer

2 into a common semantic data representation agreed upon in the ecosystem. For Manufacturing-X, the Asset Administration Shell (AAS) data model is a prominent choice for this common format.

Gate [*Standardized data exchange*]: Layer 3 is responsible for data exchange in a uniform way through a common interface or protocol layer. Once data is in a standard format (from L2), the Gate provides a consistent messaging interface (API) to send/receive that data. In many cases, this is a RESTful web service or an HTTP-based API that others can call uniformly.

Access & Usage Control [*Manage data access*]: The fourth topmost layer enforces security, permissions, and usage policies on the data being shared. Therefore, data providers are able to limit the access and usage of the provided data. This layer is paramount for maintaining data sovereignty, as each provider can specify who is allowed to access their data and under what conditions. Layer 4 typically encompasses authentication, authorization, and possibly license management or digital usage contracts.

Discovery [*Finding partners, assets, or apps***]:** The top layer of the stack is used to find business partners, data assets (e.g. devices) or business applications across the Data Space. The layer essentially deals with federated discovery and network-level interoperability and comprises the services that let participants advertise and find available data offerings or connect.

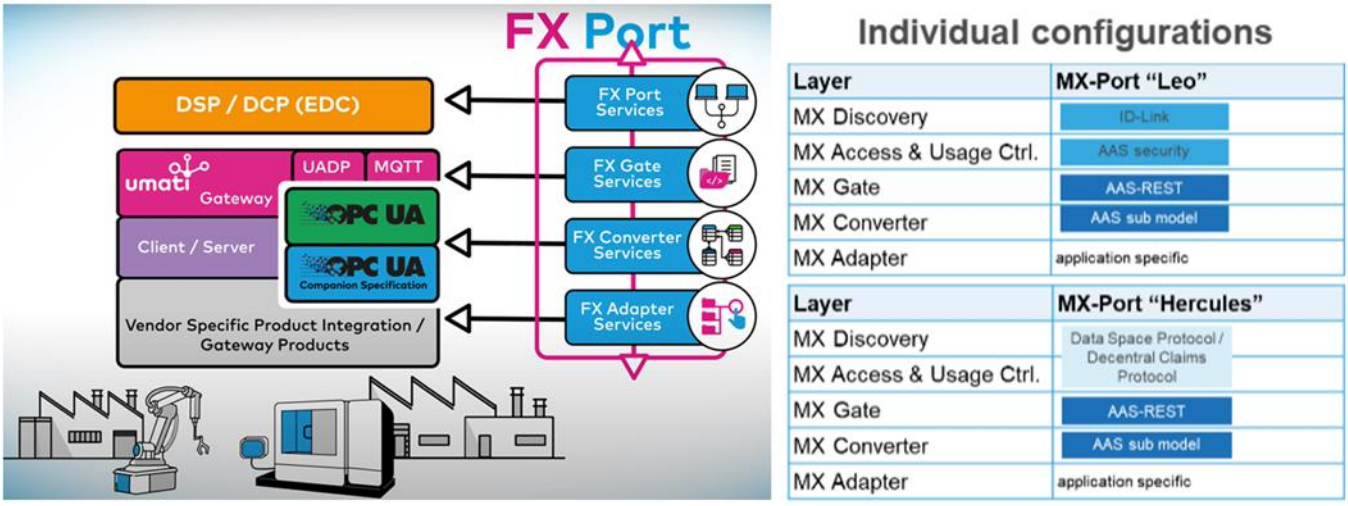


Figure 12. Layer scheme of the MX-Port architecture, along with two example configurations (Leo, Hercules).

OPC UA (Open Platform Communications Unified Architecture) is a standardized communication protocol for industrial automation, developed by the OPC Foundation. It enables reliable machine-to-system and machine-to-machine communication, supporting both Client/Server and Publish/Subscribe (Pub/Sub) communication models. This dual architecture could support a wide range of use cases, from factory-level integration to cloud-based infrastructure.

One of OPC UA's most significant strengths lies in its Companion Specifications. These define standardized data models for various types of industrial equipment, such as machine tools, robots, or injection moulding machine, ensuring that different systems share a common semantic understanding. This help to support large-scale interoperability across vendors, platforms, and ecosystems, which is a cornerstone of the federation ambition of the SM4RETNANCE Portal.

OPC UA is also inherently secure. It incorporates encryption, authentication, and access control, ensuring data integrity and protection throughout the communication chain. Thanks to its flexibility, extensibility, and strong semantic foundation, OPC UA is now more and more used in data-modern industrial data architectures, including data spaces that are built on EDC (Eclipse Dataspace Connector). Within the FX Port architecture, OPC UA serves as the semantic and technical backbone, enabling structured, meaningful data exchange between industrial equipment and federated data infrastructure.
In this context, the Umati gateway plays a pivotal role. Initiated by VDW (the German Machine Tool Builders' Association) and backed by the OPC Foundation, Umati aims to simplify the integration of industrial machinery with IT and data space environments by providing a unified interface built on OPC UA standards.
The Umati gateway supports UADP (User Datagram Protocol) and MQTT, enabling seamless connectivity for both real-time and IoT/cloud scenarios. It abstracts away the complexity of proprietary machine protocols and exposes a standardized, OPC UA-based interface using the relevant Companion Specifications.
This makes Umati a powerful enabler for machines to be connected and made discoverable with minimal effort, accelerating deployment while ensuring compliance with industry standards. Once connected, their data can be funnelled through the FX Port, which provides conversion, transformation, and integration services, ultimately connecting them to data connectors implementing the Dataspace protocol.

4.3.3 SM4RTENANCE Portal: the enabling services

Enabling services refers mutually to federated services and participant agent services, hence services that are needed to enable trusted data transaction in Data Spaces.[10]The enablement services consist of a collection of decentralized services that facilitate participation in the SM4RTENANCE ecosystem.

SM4RTENANCE plans to deliver the following enabling services to provide the required technical and semantic interoperability services for seamless operation of the Data Space Federation:

Table 3. SM4RTENANCE Portal enabling services.

ES-code	Enabling Service	Release 1	Release 2
ES-01	Asset Registration		
ES-02	Business Partner ID		
ES-03	Service Registration		
ES-04	Digital Twin Registry		
ES-05	Industrial Automation support services		

These services are essential for:

- **Identity and trust management**: Ensuring that participants are verified and authorized.
- **Service discoverability**: The process of making services visible and accessible across federated domains.
- **Asset** virtualization: Enabling digital representations (twins) of physical assets for data-driven operations.

[10] https://dssc.eu/space/BVE2/1071253470/Intermediaries+and+Operators

- **AI integration**: Facilitating the use of advanced analytics and machine learning in industrial environments

Asset registration

Asset registration is the service that creates and maintains a record of data assets within the data space ecosystem. It ensures that assets—such as datasets, devices, or digital twins—are findable, accessible, interoperable, trustworthy, and compliant with governance policies. This process typically involves capturing metadata, validating asset information, and managing the lifecycle of each asset record to ensure quality and consistency among participants.

Business Partner ID

Business Partner ID is an **identity management service** that issues and manages unique identifiers for participants (business partners) within the Data Space. The **Business Partner ID** enhances trust in digital interactions by providing a globally unique identifier that ensures precise identification, secure data management, and reliable verification of participants within decentralized networks.

Service registration

Service registration enables participants to publish and register the digital services they offer within the data space, such as APIs, data provision services, or analytic tools. This service catalogues the available offerings, manages their metadata, and facilitates discovery by other participants. It supports lifecycle management and ensures compliance with established usage policies, allowing participants to efficiently find and consume services in a governed environment.

Digital twin Registry

A Digital Twin Registry is a specialized service that manages digital representations of physical assets within the data space. It stores metadata and semantic models, in accordance with standards such as the Asset Administration Shell (AAS). This enables participants to discover, access, and interact with digital twins effectively. The service promotes interoperability and data sovereignty by connecting real-world assets to their digital counterparts, thereby facilitating automation, monitoring, and collaboration.

Industrial Automation Support Services

These services offer support for the integration of industrial automation systems into the data space ecosystem. They encompass the management of real-time data exchange, the assurance of interoperability among automation components (e.g., sensors, controllers), and the implementation of secure communication protocols. These support services facilitate automated data flows, condition-based monitoring, and digital twin synchronization, thereby promoting efficient operations and decentralized control in industrial environments.

The roadmap is designed to be iterative, with progressive alignment to Gaia-X, IDSA, and industry-specific standards.

4.3.4 Portal Look & Feel, experience and Adoption Path

The **SM4RTENANCE Portal** serves as a digital gateway to a cross-sector, federated data ecosystem for the manufacturing industry. It functions as a connective layer between multiple Data Spaces aiming to facilitate secure, trusted, and interoperable data exchange among various sectors such as automotive, textile and machine tools industries. This portal empowers participants to discover, share, and monetize data and services within a secure and standardized framework.

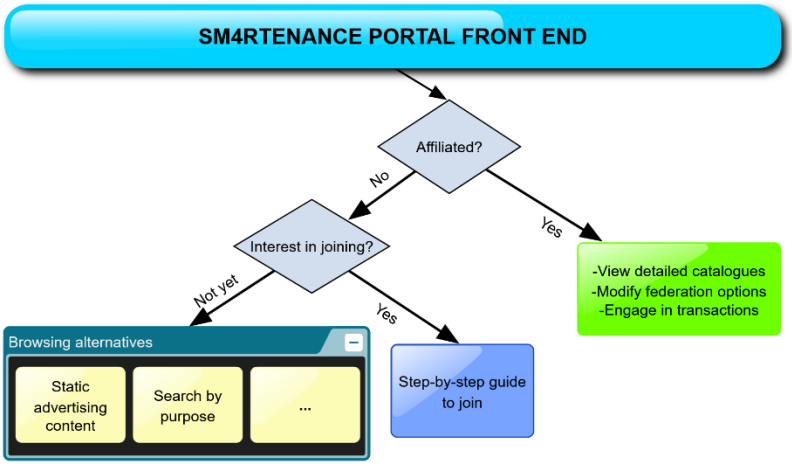


Figure 13. User flow from the SM4RTENANCE front end.

Designed for modularity and scalability, the portal enables you to:

- **Discover** relevant **Data Spaces** and trusted **Service providers**
- **Navigate** through curated, **high-quality datasets** and **advanced analytical tools.**
- **Explore** real-world innovations through engaging **use case presentations**.
- **Interact** with **federated services** through a secure and user-friendly interface.

The **Marketplace Interface** of the SM4RTENANCE Portal serves as a federated access layer for discovering, evaluating, and interacting with industrial data products and services across multiple data spaces.

The following user interface mock-up presents a streamlined portal experience, where a search bar enables browsing the offerings by different categories (machine type, geographical region, industry sector, service provider). The onboarding journey is designed for gradual engagement, with clear support for prospective participants, certified service providers, and advanced users.

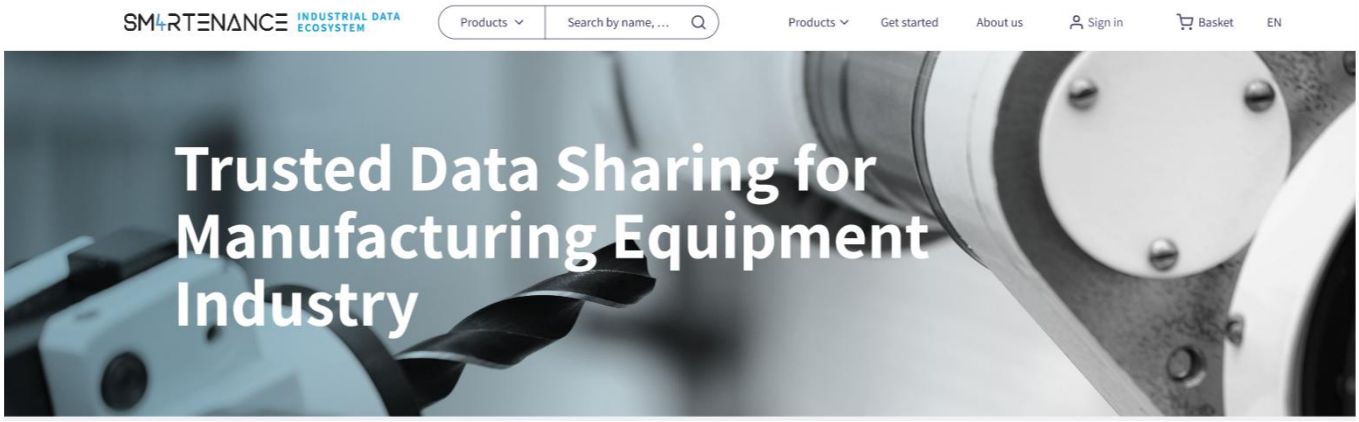


Figure 14. SM4RTENANCE portal mock-ups: homepage.

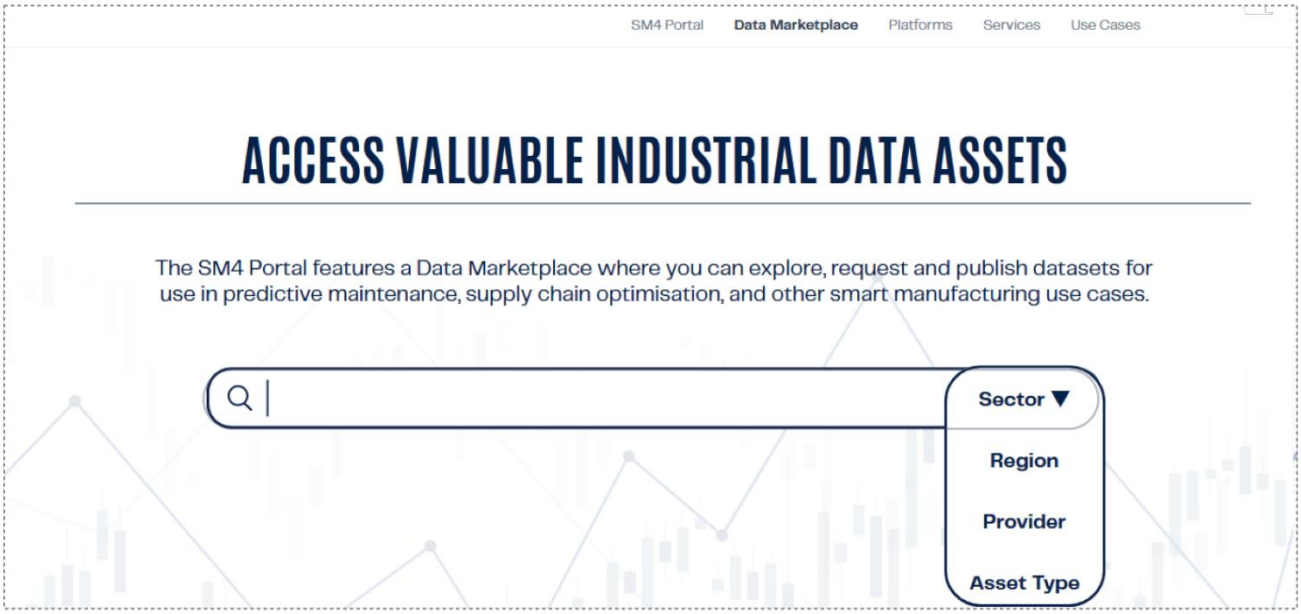


Figure 15. SM4RTENANCE portal mock-ups: search for datasets.

Through federated discovery, an aspiring participant should be able to browse data offers, and assess whether the content offers value to their objectives. The data should be searchable by purpose, for example, *AI models for milling-machine predictive maintenance*, *Digital Product Passport data for circularity assessment*. Once the data is chosen, the data source logistics should determine a pathway, regarding the service providers the participant should reach out to, based on their country of residence. Subsequently, knowing which Data Spaces they will need to interact with, the most appropriate federation approach should be proposed (Metaportal, Shareable DAPS/Broker, MX-Port). The **portal should absorb the technical challenges**, **abstracting them away from the end user**, for whom the experience should be completely streamlined.

The customer journey is depicted here as having three distinct phases, from casual engagement (browsing) to interest and incorporation into the federation system.

Browsing stage: "I am interested in exchanging data"

- Data labelled by purpose, **searchable by purpose.**
- Restricted detail level**: purpose labels visible**, full catalogue should be **behind a federation wall.**
- Convey a clear picture of the value to be gained, possibly through a form of consumer-assigned rating (stars, numerical values, categorical values, or other).
- Make identifiable trademarks and badges visible to inspire trust: Gaia-X compliance, IDS/EDC connectors, IDSA certifications, ISO/IEC 27001.
- Mention the in-use communication protocols, formats, standards and structures that are well understood or well regarded as growing trends in the manufacturing concept: OPC-UA, MQTT, AAS.

At the browsing stage, the user is casually exploring the portal with no strong commitment yet, possibly just evaluating relevance or scoping opportunities. The interface should accommodate this passive posture, making key aspects searchable and visually digestible, particularly through purpose-labelled data categories (such as predictive maintenance, calibration, or supply chain coordination). While deep catalogue access remains restricted behind a federation wall, high-level insights should still be offered to spark curiosity. To convey the value proposition, data purpose entries can display user-assigned relevance or quality indicators like stars, feedback notes, or industry-aligned impact scores. **Trust signals should be encountered at a glance**: clearly visible badges and certifications like Gaia-X compliance, IDSA adherence, Eclipse Dataspace Components, or ISO/IEC 27001 compliance could vest the entire system with credibility. This should be bolstered by displaying the most significant and agreed-upon industrial standards, such as AAS (Asset Administration Shell), OPC-UA, and MQTT, reinforcing the notion of compatibility with modern systems. In order to raise awareness, the portal should showcase ongoing, real-world collaborations across enterprises via the federation. These showcased value-creation opportunities should cover all participant sizes (large enterprises, SMEs, startups) to illustrate that meaningful engagement is accessible at any scale. These case stories, curated by public relations personnel, should maintain freshness and convey dynamism, making the ecosystem feel alive and worthy of further exploration.

Interest stage: "I want to interact with this ecosystem"

- Paint a **clear pathway** for the participant to join.
- Indicate **providers in the same home country or region.**
- *Reverse mapping*: from the **specific target data sets**, indicate which participant companies are the **owners**, and with what **providers** they operate. Indicate which providers, of those available to the participant, would be capable of interfacing with the intended data owner's providers. Make it abundantly clear that there will be a streamlined path towards the target data.
- Facilitate the **path towards contacting the partner** that would enable the intended interoperation.
- Offer a preliminary assessment on the least-resistance-path configuration (Metaportal, Shareable DAPS, MX-Port) based on the potential customer situation.

The portal should present a clear avenue to enable a party evolving from a passive observer to an interested stakeholder. A step-by-step pathway to onboarding must be presented, starting with identifying a local or regional Data Space service provider, preferably residing in the same country or industrial region, in order to reduce technical barriers. If a participant is drawn to a specific data-purpose or dataset (e.g., calibration data for coordinate machines), the portal should identify which company owns the dataset, which provider facilitates it, and which providers near the aspiring user can interoperate with that setup, however only revealing the latter information in order to protect the current participants. This **waypoint-to-waypoint** clarity could prove a strong differentiator. Wherever possible, the portal can offer a preliminary configuration suggestion (e.g., Metaportal, Shareable DAPS, MX-Port) based on basic user attributes, giving the impression of a well-thought-out and responsive gateway. This stage should reduce perceived friction while providing reassurance at every step toward productive participation.

Participant stage: "I am a newly onboarded participant"

- Extended **federated catalogue visibility.**

- More insightful metadata: **contact details**, **standards** adhered to, full **usage conditions**, **compensation** options.
- Unrestricted *reverse mapping* from data to owners to providers to best-interoperable providers
- Set **Identity and Catalogue compatibility** approach: Metaportal, Shareable Broker/DAPS (D-Connect).

Once the party has formally joined the federation, it needs the tools and visibility required to actively participate in the data economy. The portal should unlock the previously-limited access to the federated catalogue, including deeper metadata for each dataset: detailed usage terms, data ownership clarity, technical and legal standards, and any compensation models (monetary or reciprocal) that may apply. Reverse mapping capabilities should now operate in full: a participant should be able to trace any data listing back to its **owning entity**, its service provider, and see which connectors and protocols would most efficiently enable access from their current infrastructure.
Participants have to be assisted by their Data Space Service Provider (DSSP) to choose and configure their identity and catalogue integration mechanism: through the Metaportal, a shareable broker/DAPS like D-Connect, or any other compatible method among the federators. From this point, the participant should be free to focus shifts from discovery and operational readiness into trusted collaboration and value creation. The user should now feel like a fully enabled actor, equipped with the tools, insights, and able to forge partnerships to thrive in the ecosystem.

The **Marketplace Interface** is designed to support future enhancements, including compensation frameworks, detailed usage tracking, and cross-domain service orchestration.

By abstracting technical complexities and creating a unified access layer across federated catalogues drives scalable, interoperable, and value-driven data sharing within the SM4RTENANCE ecosystem.

4.3.5 The user stories

The SM4RTENANCE portal is designed to support a diverse set of users, each playing a distinct role within the ecosystem.

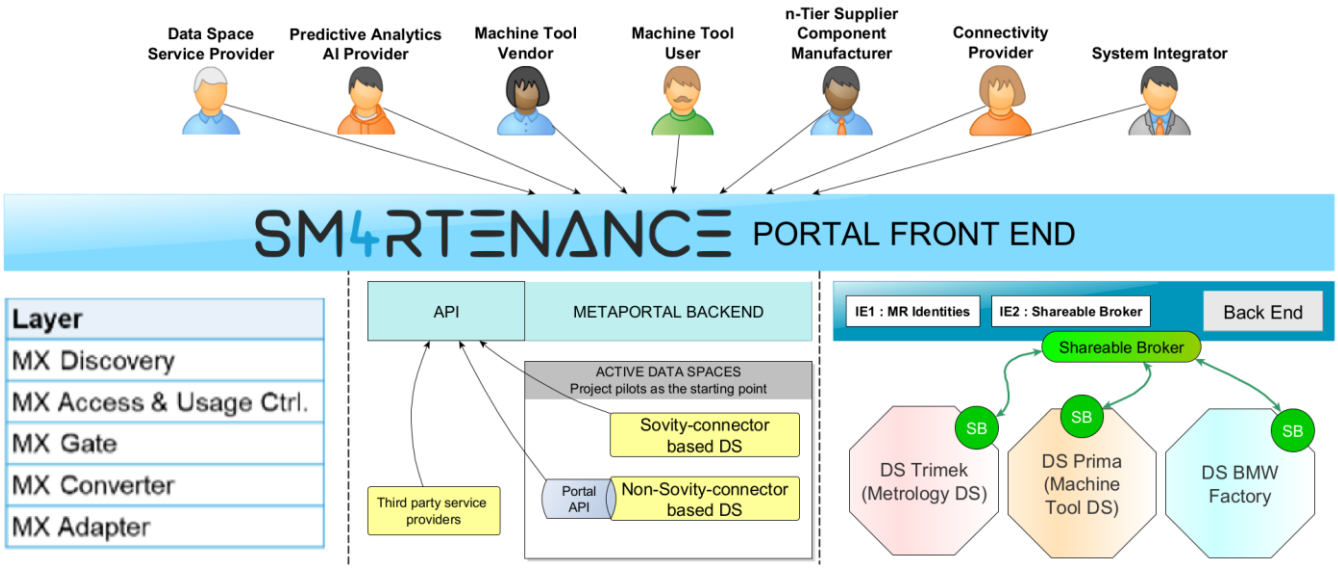


Figure 16. Portal user stories supported.

The platform aims to accommodate three main user groups: data space operators, data and services providers, data consumers

- **Data Space operators** are organisations that operate a data space ecosystem, which function independently of one another.
- **Data and Service providers** are expected to be organizations that contribute data, offer maintenance-related services, or expose analytical tools via the portal. The SM4RTENANCE Portal involves data providers from various sectors and ecosystems, focusing on stakeholders across the manufacturing asset lifecycle.
    - **Manufacturers and OEMs**: Companies that contribute data related to manufacturing processes, asset management, and predictive maintenance trials.
    - **Factories in the Consortium**: Specific pilots offer monitoring/predictive-maintenance services that require an external customer (machine owner, shopfloor operator) to supply the data.
    - And other future organizations from other domains.
- **Data consumers** include both organizational users and individuals who interact with shared data products, request services, or use analytics functionalities.

The user model is intended to evolve in future releases to support more advanced roles and to gradually open to third-party actors beyond the immediate consortium.

The following user stories are tailored to the onboarding into the federation, and what the initial interactions with the federation bring to the different stakeholder types. The following user stories are designed to facilitate onboarding into the federation and illustrate the value of initial interactions for each stakeholder type.

1. AI-Based Predictive-Maintenance Provider [Purpose-oriented search]

User Story: *As an AI-based predictive-maintenance provider, I want to search and filter available datasets by purpose and machine type so that I can expand and offer my service to different machine types and customers.*

- The provider connects to the federation meta-portal, which aggregates catalogues from multiple industrial Data Spaces (e.g., for machine tools, textiles, and automotive).
- Using a unified semantic layer (harmonized by the sectoral intermediaries), the provider filters datasets by purpose labels such as *tool wear prediction* or *motor vibration anomalies*, regardless of the Data Space where that data resides.
- Through federated identity recognition, the provider's credentials are valid across different domains, accelerating dataset access requests without duplicating onboarding or compliance efforts reducing the time to market. In addition, access to diverse real-world datasets enhances model accuracy and service reliability.

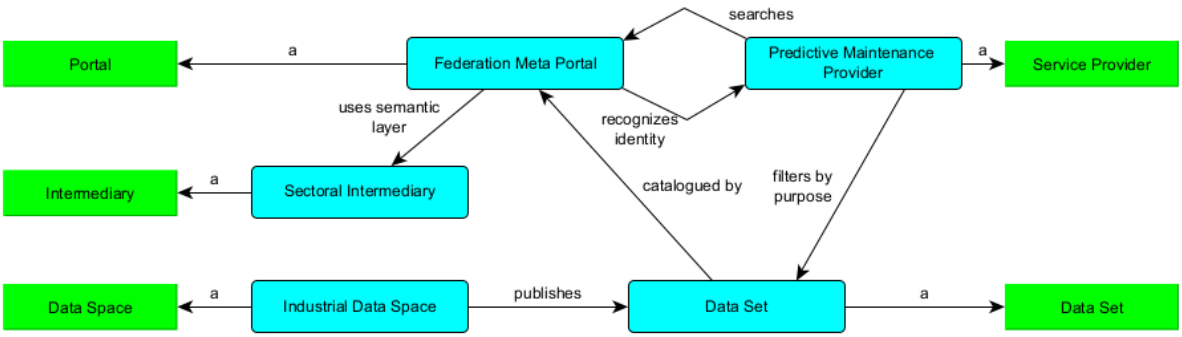


Figure 17. AI-Based Predictive Maintenance Provider user story diagram.

2. Tier-2 Supplier [Accessing OEM Data]

User Story: *As a tier-2 supplier, I want to request access to an OEM's real-time spindle-load dataset so I can improve the resiliency of my components.*

- The tier-2 supplier enters the portal and searches for data labelled "spindle load telemetry" within the Automotive sector.
- The portal identifies the OEM owning the dataset, the intermediary DSSP managing it, and what interoperability protocols are required.
- The supplier's own regional provider validates their identity and, through the shared ID infrastructure, grants access across the two Data Spaces without a second onboarding
- A compatibility check is performed to ensure the supplier's DSSP can establish secure communication with the OEM's connector, suggesting the compatible federator alternatives (D-Connect, Metaportal).

- Once approved, a federation-compliant contract template is offered, outlining compensation, duration, and usage restrictions, ensuring fast-tracked legal alignment.

3. Small Machining Shop [Onboarding]

User Story: *As a small machining shop, I want to join the federation through a regional provider so I can share milling-machine-health data with diagnostics services operators.*

- The shop locates a local Data Space Service Provider via the federation's map-based UI, with tailored onboarding guides for SMEs.
- The DSSP offers tooling to integrate the shop's machines, whether they use OPC-UA, legacy PLCs, or simple CSV logs, into a federation-compliant connector.
- A shared federation ID is issued, making the shop discoverable across all relevant Data Space use cases (e.g., Machine Tool, Industrial Diagnostics).
- The shop's datasets are published with purpose-label metadata (e.g., "milling machine maintenance"), and access policies are applied via standard templates.
- Diagnostics providers across the federation now see this small shop's data in the federated catalogue, even across sectors, making it far more visible than in a siloed local system.

4. Small Machining Shop [Improving Equipment Efficiency]

User Story: *As a small machining shop, I want to benefit from federation-enabled analytics solutions to improve the efficiency of the milling machines I own.*

- The shop easily identifies federation-certified analytics providers that offer tailored machine-health monitoring services.
- Federation identity and compatibility checks simplify onboarding processes, quickly connecting shop equipment data streams to analytics providers.

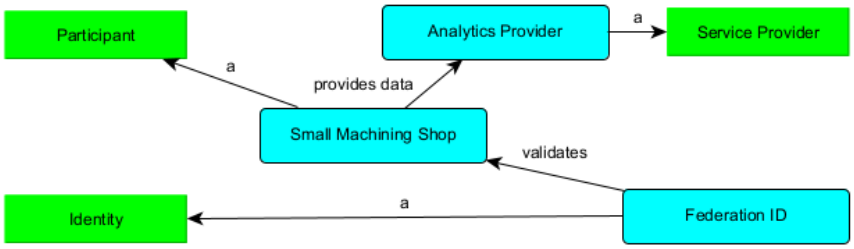


Figure 18. Small Machining Shop user story diagram.

5. Machine Manufacturer [Monitoring Machined Piece Tolerances]

User Story: *As a machine manufacturer, I want to aggregate tolerance-compliance data from the milling machines I have sold, across all customer sites, so I can refine machine design and proactively recommend process adjustments.*

- Using the federation Sovity portal solution, the manufacturer subscribes to anonymised dimensional-tolerance datasets published on each customer's Data Space, without needing those customers to join the manufacturer's own Space.
- A single federated identity and policy framework lets every customer approve or deny the data-sharing request in their local Space, while the manufacturer receives the streams through one connector instead of multiple bilateral integrations.

6. Repair Service Specialist [Updating a DPP]

User Story: *As a repair service specialist, I want to update a DPP after repairing a product to ensure accurate maintenance history.*

- The repair specialist scans the product's identifier and retrieves the associated DPP metadata via the federation's resolution service, which may aggregate data from multiple providers and locations.
- If authorized by the original manufacturer, the specialist writes repair details (e.g., replaced parts, timestamps, serial numbers) into the appropriate section of the DPP and in a traceable manner.
- The updated DPP information becomes available across the federation: to buyers, authorities, insurers, and service providers, enhancing transparency and reducing lifecycle data fragmentation.
- This ability to write back through federation-compliant channels ensures that repair history becomes part of the persistent data record, even if multiple actors or tools are involved.

7. Data Space Service Provider (DSSP) [Onboarding the Federation]

User Story: *As a regional or domain-specific Data Space Service Provider, I want to join the SM4RTENANCE Federation so that my clients can access and contribute to a wider variety of data from many industry verticals.*

- The DSSP accesses the federation's meta-portal and expresses interest via the provider onboarding interface.
- The DSSP undergoes technical and legal evaluation by the federation's onboarding authority, including checks for support of EDC/IDS connectors, DAPS, and semantic compatibility (e.g., OPC-UA, AAS).
- A federation identity is issued, and compatibility tools are provided to align the DSSP's catalogue with the federated schema (e.g., purpose-labelled datasets, policy templates).
- The DSSP then becomes a certified interface layer for regional machine shops, OEMs, or analytics providers, i.e., becomes an option to onboard and operate through. Then, the DSSP can provide tailored onboarding packages aimed at simplifying the process for their clients entering the SM4RTENANCE ecosystem. Consequently, organizations ranging from small and medium-sized enterprises (SMEs) and original equipment manufacturers (OEMs) to artificial intelligence (AI) service providers can access and publish data products across various domains without the need to develop custom integrations.
- From now on, any participant managed by this DSSP gains automatic visibility and identity propagation across the federation. The DSSP platform ensures secure, standardized data exchange and operations,

supporting compliance with legal and regulatory requirements. This encourages trust development among stakeholders, enabling collaborative business partnerships within the Data Space.

- DSSP enables businesses to create comprehensive data chains that trace material flows and enhance supply chain resilience. For example, the circular economy and carbon dioxide (CO2) monitoring are both supported by the tracing of parts and components from primary materials to their recycling stages.

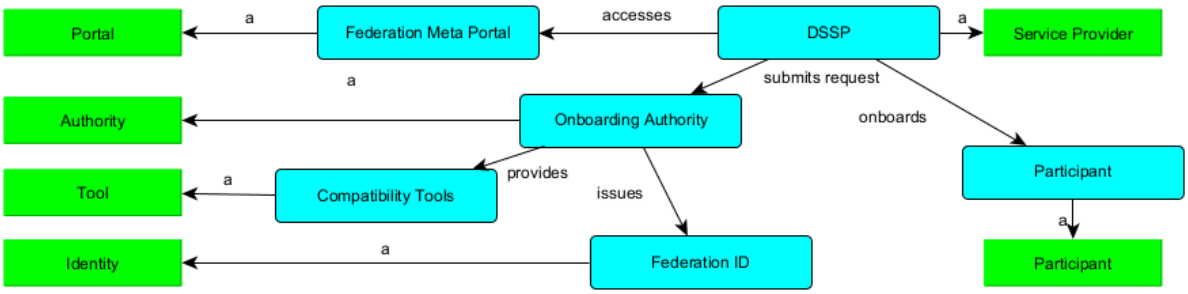


Figure 19. Front end workflow for DSSPs that intend to join the Federation.

8. Research Centre [Accessing Cross-sector Data]

User Story: *As a research centre, I want access to datasets from across different industry-specific Data Spaces within the federation, so I can conduct interdisciplinary research on federated learning methods.*

- The research centre accesses the federation frontend and searches for datasets tagged with predictive-maintenance-related purposes (e.g., vibration analysis, thermal imaging, etc.) across diverse manufacturing sectors.
- Federated identity management grants seamless authentication, providing access to immediate visibility and request capabilities for datasets residing in various federated Data Spaces without multiple onboarding processes.
- Standardized policy frameworks simplify the negotiation of usage rights, speeding up research cycles.
- Semantic interoperability ensures that datasets from different domains become easily integrable.

9. Industry Association [Benchmarking Industry Practices]

User Story: *As an industry association, I want to access aggregated datasets from sector-specific industry partners and establish guidelines and best practices for improved day-to-day operations.*

- The association logs into the SM4RTENANCE Portal, browsing industry-specific data catalogues of use to conduct benchmarks.
- Federation-wide data governance frameworks guarantee secure and anonymized data handling, preserving participating companies' competitive information.
- The association publishes benchmark reports and best-practice recommendations for any same-vertical participant in the Federation.

The following examples of user stories involve contributors that do not regularly operate or take part in the data exchange dimension themselves through the Federation, but provide infrastructure or verify that the ecosystem itself functions in a secure manner.

10. Sensor Provider [Wide-scope Hardware Compatibility]

User Story: *As a sensor provider, I want to validate my hardware for federation-wide compatibility standards so that my customers can confidently integrate my sensors at their Adapter level.*

- The provider uses federation-defined testbeds and certification programs to validate compatibility of sensor hardware and firmware with federation protocols and semantic standards.
- Through federation-driven collaboration, sensor providers receive guidelines and assistance for aligning product designs and communication standards (OPC-UA, MQTT) with federation interoperability requirements.
- Customers, such as manufacturing SMEs and DSSPs, easily identify and select federation-certified sensors, simplifying their data integration process and data ingestion into the federation.

11. Cybersecurity Expert [Ensuring Federation Compliance]

User Story: *As a cybersecurity expert, I want to audit and validate federation-wide data-exchange processes to support trust and reliability across the ecosystem.*

- Security assessments cover authentication and authorization mechanisms, data encryption standards, and access management policies, identifying potential vulnerabilities and recommending improvements.
- Federation-level reporting and alert systems enable proactive dissemination of security findings. By proactively identifying vulnerabilities and implementing robust security protocols such as encryption, access control, and authentication cybersecurity experts significantly reduce the possibility of breaches, downtime, and reputational damage.
- Cybersecurity Experts assist in aligning federation operations with legal frameworks, including the General Data Protection Regulation (GDPR), the EU Cybersecurity Act, and industry-specific standards. This alignment minimizes legal exposure and accelerates certification processes.

4.4 SM4RTENANCE services to support the federation of manufacturing data ecosystems

SM4RTENANCE Data Space will provide the required technical and semantic interoperability to support the federation of Data Spaces around the Portal.

Code	Interoperability Services	Release 1	Release 2
IF-01	Identity Federation		
IF-02	Virtual Data (Product) Catalogue		
IF-03	Data Space Service Monitoring		
IF-04	Data Products & Vocabularies		
IF-05	Virtual Business ID		
IF-06	Federated Browser		
IF-07	Data Space Protocol		

Table 4. SM4RTENANCE federation interoperability services.

4.4.1 *SM4RTENANCE federation services: 1st release*

Identity Federation

The Identity Service Federation enables the creation, management, maintenance, monitoring, and validation of identity information for participants and/or components within the SM4RTENANCE Data Space. This service also provides proof that other participants can use for authentication and authorization purposes.

Virtual Data (Product Catalogue)

Product catalogues offer a comprehensive directory of available services, including predictive maintenance tools, Digital Twins, Data applications and computing resources, allowing users to easily locate and access these resources.

Data Space Services Monitoring

Monitoring services play a pivotal role in ensuring transparency, accountability, and operational coherence across the federated Data Space ecosystem. Within a single Data Space, monitoring functions already serve to track transactions, enforce policies, and provide real-time visibility into system performance and reliability. However, in a federated context, these functions become even more critical due to the heterogeneity and distributed nature of the participants, governance layers, and technical infrastructures involved.

The envisaged services will ultimately cover three complementary dimensions:

- Advanced oversight mechanisms that go beyond clearing, enabling the system to detect anomalies, policy violations, or inefficiencies across interconnected nodes;
- Services capable of analysing evolution of the federation (e.g., onboarding of new members, changes in trust relationships, activity patterns), which is essential for adaptive governance;

- Multilevel reporting services, generating dashboards and insights adapted to various stakeholders — from technical operators to governance boards and regulators — to support decision-making, compliance monitoring, and performance evaluation.

These services will rely on APIs and real-time information aggregation pipelines. In a federated environment, they also contribute to interoperability and trust-building, by providing verifiable and auditable information about how data, policies, and services are used across the ecosystems.

Ultimately, monitoring functions are a cornerstone for operational transparency and a precondition for sustainable scalability of the federation. They ensure that each ecosystem can operate autonomously while remaining accountable to shared governance rules, making it possible to align local behaviours with global objectives.

4.4.2 SM4RTENANCE federation services: vision for the 2nd release

The second release will mainly focus on providing additional services to support value creation and seamless flow of data and participants within the future federation. Improvements and evolution of first release services, like the support of decentralized identities, are also envisaged.

Identity Federation - DIDs/DAPS

A Decentralized Identifier (DID) is a new type of globally unique identifier designed to enable verifiable, decentralized digital identity without relying on any centralized registration authority or identity provider.[11]

DIDs are particularly significant for establishing trust in a zero-trust environment. When a participant seeks to access data or services within the Data Space, it presents a DID-based identity along with one or more Verifiable Credentials. Self-sovereign identity (SSI) is an advanced digital identity model that empowers individuals and entities to fully own, control, and manage their digital identities without reliance on any intermediary or central authority

A Dynamic Attribute Provisioning Service (DAPS) is an infrastructure component used primarily in the International Data Spaces (IDS) ecosystem to issue dynamic, up-to-date attribute information about participants and connectors. It functions as an attribute server that issues OAuth2 access tokens, called Dynamic Attribute Tokens (DATs), which contain signed claims representing current attributes of the requesting IDS connectors or organizations. DAPS provides a trust anchor that enables participants to safely verify and grant permission to each other without the need for centralised data control.[12]

Data Products & Vocabularies

Data products are valuable assets that deliver both monetary and non-monetary benefits derived from data. They should address the needs of consumers and serve a clear purpose. Data products are presented to users in a consumable format, allowing for easy discovery and self-service consumption. These products adhere to specific

[11] https://www.w3.org/TR/did-1.0/
[12] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-g/components/identityprovider/daps

data product specifications. The process of productizing data involves transforming raw data into consumable and marketable data products.

Vocabulary services

Vocabulary services provide definitions for metadata representation, vocabularies, and ontologies. Vocabulary providers define metadata structures that describe data consistently. This consistency ensures that all participants in a Data Space can interpret and use the data uniformly. Vocabularies facilitate the organization easier to find, integrate and analyse data from diverse sources.

Virtual Business Partner ID

A Virtual Business Partner ID in Data Spaces refers to a unique digital identifier assigned to participants (business partners) within a Data Space. This ID facilitates sovereign, secure, and interoperable data exchange and governance across organizational boundaries. Gaia-X verifies the compliance of organisations requesting a Virtual Business Partner ID inside its ecosystem using an extensive trust and labelling framework. This framework establishes clear criteria and verification processes to ensure adherence to its core principles, including openness, transparency, data protection, security, and portability.

Federated browser/ Data Space Brokerage Services

Data Brokers or intermediaries serve as neutral third parties that connect individuals and companies with data users. While they may charge fees for facilitating data sharing between the parties, they cannot directly utilize the data they intermediate for financial gain. Data intermediaries must adhere to stringent requirements to maintain this neutrality and prevent conflicts of interest.[13]

Within the broader category of service providers in Data Spaces, intermediaries and operators facilitate data sharing and enable trusted data transactions. These services can include technical offerings, such as federation, participant agents, or, occasionally, value creation services, as well as business and organizational services.[14] **The preparatory work for the second release will assess the feasibility of deploying this service before the end of the project.**

The Data Space Brokerage Service plays a crucial role in facilitating data discovery and interoperability by managing metadata repositories and offering transparent, standardized access to information regarding the data and services available in the Data Space. This promotes secure, sovereign, and effective data sharing among participants.

Dataspace protocol

[13] https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

[14]https://dssc.eu/space/BVE2/1071253470/Intermediaries+and+Operators#3.3.3.-Intermediary-business-and-revenue-model-characteristics

The long-term ambition of SM4RTENANCE and its federation is to ensure compatibility with any Data Space that operates Dataspace-Protocol-capable connectors. The Dataspace Protocol is on track to become recognized as an ISO/IEC standard for secure and trusted data exchange. While the EDC basis is currently the most widely used for developing or deploying DSP-capable connectors within the EU Data Space ecosystem, the federation will leave room for wider connector compatibility.

By design, the SM4RTENANCE infrastructure is meant to remain open and flexible, avoiding any form of vendor or technology lock-in. This means that, as the ecosystem evolves and new versions of the Dataspace Protocol emerge, they should be able to integrate seamlessly into the federation. Supporting a wide range of compliant connectors goes beyond being a base requirement for technical neutrality, as it also paves the way towards innovation and openness across different industrial sectors and Data Space initiatives.

4.5 First Release Demonstrator

The project is advancing toward the creation of a federated ecosystem of industrial Data Spaces, designed to support cross-organizational data exchange in Industry 4.0 application domains, for instance: predictive maintenance, digital product passports, battery diagnostics, and supply chain optimization. A central aim is to enable participants in one Data Space to browse and evaluate data from another, even when not formally onboarded as members. This requires going beyond data catalogue interoperability and into a robust framework for mutual identity recognition.

In order to support external engagement and guide onboarding, the project is developing a Federation Portal, which will function as the primary access point for external partners and stakeholders. While currently at a design-only stage, the Portal already reflects the organizational structure and intended user experience of the federation. It will eventually allow users to browse federated data offerings, understand participation requirements, and initiate trust relationships across Data Spaces. The next project phase will involve building a working prototype and connecting it to the federation's evolving identity and catalogue infrastructure.

One pathway builds upon the MX-Port architecture this model promotes a lightweight and modular integration of machines into Data Spaces using OPC-UA and its companion specifications. All components involved are freely available as open-source software. The MX-Port solution enables secure, real-time machine communication and supports trusted data exchange through decentralized trust anchors. In a recent demonstration, the approach was used to share Energy Consumption, instantaneous Power, and the associated CO_2 footprint of manufacturing equipment via a Digital Product Passport. This capability highlights the potential of the MX-Port model to support sustainability use cases and regulatory compliance in addition to operational monitoring. The architecture's effectiveness has been showcased in real-world industrial environments, such as during the 2025 Hannover Messe, and is further reinforced by its extensive, and growing, library of domain-specific OPC-UA companion specifications, that seek to bolster interoperability across a wide range of machinery and production systems.

Dawex and Schneider Electric will lead a demonstration involving the Data4Industry-X Data Space, itself aligned to the Manufacturing-X initiative. The data exchange platform, powered by Dawex technology and integrated with Gaia-X Digital Clearing House services supports multiple industrial data protocols, including OPC-UA via Prosyst's Unified Data Collector, the Dataspace Protocol, AAS, and EDC Connectors. This approach is backed by concrete industrial use cases from Schneider Electric and Valeo, which illustrate the platform's flexibility in predictive maintenance and AI-driven CO_2-emissions forecasting.

A third decentralized approach for the mid-term demonstration is based on the DConnect confederation option. The demonstration will be carried out collaboratively by SQS, TXT, and PRIMA. Catalogue cross visibility, and identity cross-verification will be showcased, the interaction rounded up with a data set transaction across different Data Spaces.

In parallel with the evolution of these federation strategies, progress made at the individual, pilot scale, will be presented in detail. carrying out data transfers between their onboarded participants, some of which involve off-consortium organizations.

Looking forward, these developments represent steady and structured advancements toward realizing the envisioned federated industrial data ecosystem. With tangible advancements both at the overall scale and use case level, and a clear pathway for external access through the Federation Portal, the project is well positioned to demonstrate federation actions in the coming months.

5. Path towards the second release

This section outlines the strategic direction, methodological framework, and collaborative plan to evolve the SM4RTENANCE Data Space Services from the first implementation release to a consolidated and mature platform at M30. This next phase will consolidate the lessons learned, extend functional coverage, scale federation capabilities, and ensure operational alignment with external Data Spaces and European infrastructure initiatives.

5.1 Strategic vision

The strategic objective of the M30 release is to transition SM4RTENANCE from a proof-of-concept stage to a scalable, standards-based platform that aligns with the vision of the Common European Manufacturing Data Space. This evolution is driven by the following high-level goals:

- **Maturity**: Refine, stabilize, and extend the core services delivered in the first release to meet industrial-grade quality, performance, and resilience requirements.
- **Interoperability**: Enable semantic and technical interoperability with other Data Spaces and federated infrastructures (e.g., D4IX, Catena-X), leveraging shared vocabularies and protocol standards.
- **Trust and Compliance**: Reinforce mechanisms for identity assurance, policy enforcement, and usage control, aligning with Gaia-X Trust Frameworks, DGA requirements, and GDPR obligations.
- **Ecosystem Integration:** Position SM4RTENANCE for integration into broader European initiatives such as SIMPL, and the Gaia-X Federation Services ecosystem.

Strategically, the 2nd release must provide the technical and governance foundations to enable long-term sustainability, cross-sectoral expansion, and industrial adoption. This includes the ability to support a multiplicity of data sovereignty models, legal frameworks, and sector-specific data governance schemes.

5.2 Targeted capabilities by the second release

The portal evolution must result in a coherent, modular, and production-grade infrastructure capable of:

- **Multi-party Federation**: Onboarding multiple organizations as autonomous data providers and consumers, each with the ability to govern access policies, contractual terms, and identity verification.
- **Semantic Interoperability**: Supporting cross-domain vocabularies, ontology mapping, and real-time metadata harmonization across catalogues.
- **Policy and Usage Control:** Implementing fine-grained, verifiable, and enforceable usage policies using ODRL, EDC Policy Engine, or similar mechanisms.
- **Operational Monitoring and Logging:** Providing end-to-end observability, including trust monitoring, data access logs, audit trails, and SLA monitoring.
- **Dynamic Onboarding and Trust Services**: Automating the onboarding process of participants, services, and assets, with decentralized identity mechanisms and continuous trust evaluation.
- **Cross-Data Space Discovery:** Enabling federated search and discovery across SM4RTENANCE and external Data Spaces, with DSP-compliant interfaces and compatibility with Gaia-X registries and clearing houses.

This capability set ensures that the SM4RTENANCE platform can support real-world use cases involving complex stakeholder constellations, compliance constraints, and multi-provider integration.

5.3 Methodological Approach

To achieve these objectives, SM4RTENANCE will follow a proven methodological approach combining agile software development, iterative co-design, and pilot-driven validation.

- **Agile Architecture Evolution**: Technical partners will adopt an agile architecture governance model, with bi-weekly syncs, sprint-based backlog refinement, and quarterly architecture reviews. The architecture will evolve incrementally based on pilot needs, external feedback, and compliance assessments.
- **Component Ownership**: Each core component (e.g., Identity Federation, Vocabulary Service, Broker, Marketplace UI) will be maintained by a lead technical provider, with clear interface specifications, issue tracking, and continuous integration workflows.
- **Open Specification Alignment**: The architecture will continuously align with evolving standards from IDSA, Gaia-X, W3C. Contributions and pull requests to open-source dependencies (e.g., EDC, DAC) will be prioritized where relevant.
- **Co-development with Pilots**: Each pilot will serve as a live sandbox for feature evolution. Pilot leads will coordinate closely with technical teams to define user journeys, document integration gaps, and prioritize features based on real-world constraints.

5.4 Data spaces-Driven Validation Strategy

SM4RTENANCE's validation methodology follows a two-tiered model:

- **Internal Pilot Data Spaces:**
  - Each domain pilot (weaving, metrology, robotics, textile, machine tools) will test specific capabilities such as asset onboarding, identity delegation, digital twin registration, and data consumption.
  - Pilots will be used to validate user experience, onboarding time, access control logic, latency, and compliance behaviour.
  - KPIs will be tracked using structured evaluation sheets, and feedback will be logged via issue trackers integrated into GitLab or similar tool
  - Weekly pilot-tech syncs will ensure agile response to blockers and configuration needs.

- **External Pilot Data Spaces:**
  - A dedicated stream will focus on testing interoperability with external Data Spaces, notably D4IX and Underpin
  - Interoperability scenarios will include: cross-registration of offerings, vocabulary negotiation, identity handshake across different trust frameworks, and federated search.
  - Technical exchanges will be organized quarterly with the D4IX technical team, supported by compatibility testing environments (e.g., DSP sandbox, Gaia-X compliance tooling).

- Metrics such as interface compatibility, discovery latency, and semantic alignment success rates will be reported.

This dual validation strategy ensures both depth (intra-pilot integration) and breadth (cross-ecosystem interoperability), which are both essential for a successful 2nd release.

5.5 2nd release milestones

Key milestones include:

- M22: Architecture checkpoint and feature prioritization.
- M24: Release 1.1 – onboarding enhancements and federated catalogue improvements.
- M26: Release 1.2 – policy enforcement upgrades, monitoring integration.
- M27: Cross-Data Space testbed ready; scenarios executed.
- M29: Final validation sprints; regulatory audit checks.
- M30: Consolidated platform release, full documentation, KPI evaluation, validation

Each release will be accompanied by technical notes, changelogs, and open documentation updates

The 2nd release is a decisive milestone for SM4RTENANCE and its ambition to contribute meaningfully to the European Data Space ecosystem. It operationalizes a modular and standards-aligned architecture, validated through real-world trials and interoperable with external initiatives. Through disciplined governance, agile co-development, and pilot-led validation, SM4RTENANCE will deliver a credible, extensible, and trustworthy platform. This work lays the technical and organizational foundation for future sustainability and scale-up toward a Common European Manufacturing Data Space aligned with the EU's strategic data vision.

6. Conclusion

The development and initial deployment of the SM4RTENANCE Data Space Services represent a critical step toward the realization of sovereign, interoperable, and trusted data sharing infrastructures for the European manufacturing sector. As outlined throughout this deliverable, the SM4RTENANCE platform operationalizes key principles from the European data strategy by providing modular, standards-aligned services that enable collaborative data ecosystems to emerge around industrial use cases such as predictive maintenance, digital twins, and asset lifecycle optimization.

At the heart of this effort lies a foundational commitment to regulatory compliance, technological openness, and semantic interoperability. The first release of SM4RTENANCE integrates essential components such as federated identity management, catalogue federation, self-description validation, and policy-based data usage control, each of which is designed to uphold the core values of the Data Governance Act (DGA) and the Data Act. These legislative frameworks require data intermediaries and participants to ensure neutrality, transparency, and enforceable rights over data access and use. SM4RTENANCE addresses these obligations concretely by embedding verifiable credentials, distributed access control mechanisms (e.g. via EDC and ODRL), and audit-ready monitoring components.

The broader ambition of the project is not only to provide a set of technical services, but to demonstrate how federated governance and data sovereignty can be practically implemented in industrial environments. The European manufacturing landscape is typified by heterogeneity in systems, standards, and business models. SM4RTENANCE responds to this fragmentation by offering a framework for multilateral data collaboration, enabling large enterprises, SMEs, and public actors to engage in structured data transactions without compromising control, security, or compliance.
In alignment with the Data Act, which introduces obligations for data holders to make certain data accessible to third parties under fair, reasonable, and non-discriminatory conditions (FRAND), SM4RTENANCE provides the enabling infrastructure to support such data portability and transparency requirements. By integrating contractual transparency, usage policy enforcement, and dynamic consent management, the platform lays the groundwork for trusted data exchanges that are compliant by design and respectful of provider-defined constraints.
From a semantic perspective, the inclusion of vocabulary services, RDF-based metadata models, and dynamic interoperability frameworks (e.g. IMF, DSIF) ensures that the SM4RTENANCE ecosystem can bridge the gap between data heterogeneity and machine-readable understanding. This is particularly critical in manufacturing, where data often comes from proprietary operational technologies (OT), legacy systems, or domain-specific ontologies that must be harmonized to support cross-organizational analytics and services.
Furthermore, SM4RTENANCE explicitly embraces the federated Data Space model advocated by Gaia-X and the Data Spaces Support Centre (DSSC). By implementing distributed identity frameworks (DIDs, DAPS), decentralized service registration, the platform supports a decentralized trust fabric that reduces vendor lock-in and enhances scalability. This approach is essential for enabling data value chains to form across company boundaries, national jurisdictions, and industrial verticals.
The application of these capabilities is deeply rooted in the practical needs of the manufacturing domain. Predictive maintenance, asset traceability, sustainability reporting, and cross-factory optimization are all reliant

on timely, trusted, and semantically interoperable data access. SM4RTENANCE provides the architecture, services, and governance scaffolding to support these use cases, ensuring that manufacturing stakeholders can operationalize data-driven innovation while complying with legal and commercial constraints.

Looking forward to the M30 release, SM4RTENANCE will evolve into a more scalable and production-ready platform, validated through rigorous trial testing (both internal and external) and aligned with ongoing European interoperability efforts such as SIMPL, D4IX, and the Gaia-X Digital Clearing Houses. The iterative co-design methodology, cross-pilot validation strategy, and commitment to open standards will remain central to this process.

In conclusion, the SM4RTENANCE Data Space infrastructure is not simply a technological prototype; it is a concrete demonstration of how Europe's Data Space vision can be translated into operational capabilities that serve industrial, regulatory, and economic objectives. It provides the foundational elements of a Common European Manufacturing Data Space that is secure, compliant, modular, and future-proof, ready to scale with the ambitions of the European Data Economy.

7. Appendix

7.1 Gaia-X alignment

Data Spaces can leverage the Gaia-X Trust Framework to onboard participants by verifying their compliance with the Data Space Rulebook and issuing corresponding proofs of membership to facilitate trusted data exchange.[15]

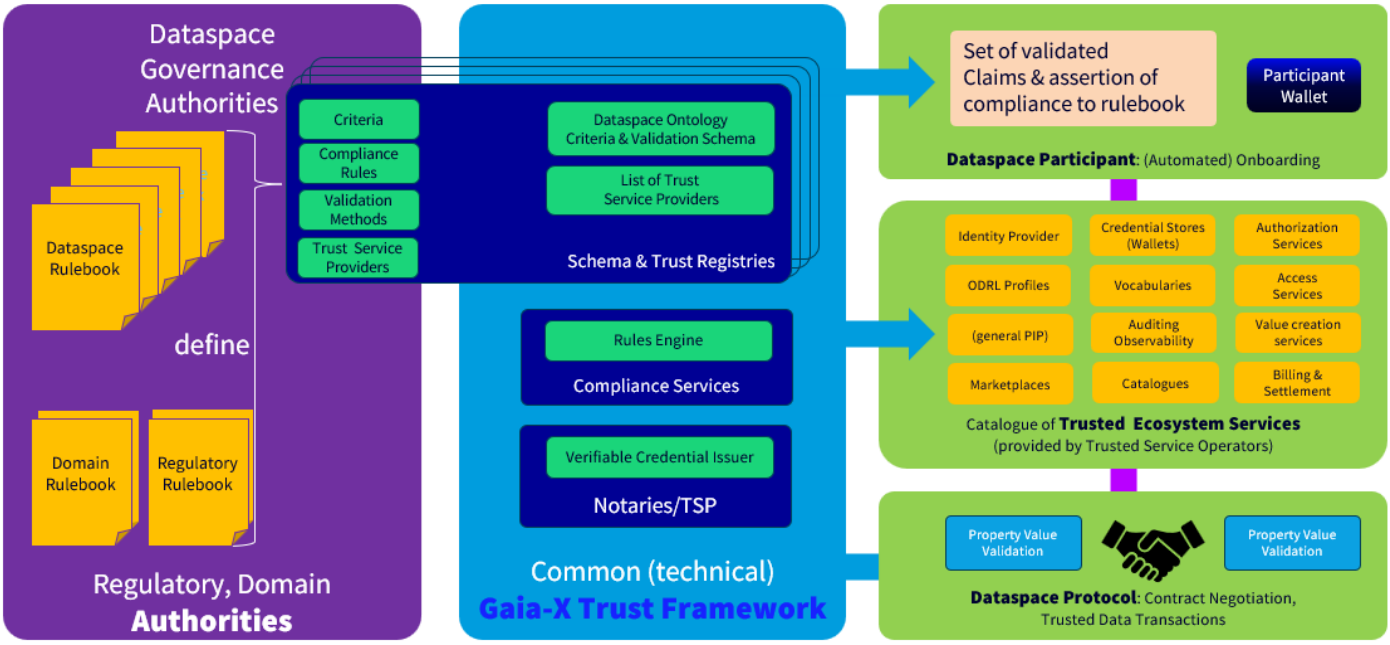


Figure 20. Data Space architecture enabled by the Gaia-X Trust Framework.

The Process Flow is as follows:

1. Governance Authority establishes rulebook, criteria, validation methods and a list of Trusted Service providers to sign the requested claims
2. Participants undergo compliance assessment using defined validation methods
3. Trust Service Providers sign compliance claims
4. Rules Engine validates compliance
5. Compliance credentials are issued and stored in participant wallets
6. Participants use credentials for trusted data exchange

[15] https://gaia-x.eu/wp-content/uploads/2024/05/An-Introduction-to-the-Gaia-X-Trust-Framework_2024-V4.pdf

Gaia-X Compliance

Gaia-X Compliance is applicable to **all** Gaia-X Service Offerings. A Gaia-X Credential will be provided for all entities defined within the Gaia-X conceptual framework.[17]

- Participant, including Consumer and Provider
- Service Offering
- Resource

Gaia-X Digital Clearing House

The operationalization of the Gaia-X Framework is supported by the Gaia-X Digital Clearing House (GXDCH), which functions as a one-stop hub for automated verification and compliance with Gaia-X regulations. This shared governance mechanism is crucial for enabling cross-dataspace interoperability.[16]

Each GXDCH is required to provide public services that implement the compulsory elements necessary for achieving Gaia-X compliance, operating under the exclusive governance of the GAIA-X AISBL (*Association Internationale Sans But Lucratif*). Any Gaia-X adopter (whether a user, provider, or federator) can utilize any GXDCH to obtain compliance, join a federation, or become a federator, as well as access additional services.

The GXDCH is designed for future evolution, allowing for enhancements in its components with each release. GXDCH combines mandatory and optional components.

Mandatory Components

Gaia-X Compliance Service: Validates participants' adherence to Gaia-X Policy Rules using Verifiable Credentials (VCs) and Verifiable Presentations (VPs).

Gaia-X Registry: Manages trusted credential issuers and defines credential structures

Gaia-X Notarization Services: Verifies organizational identities provided by participants credentials (e.g., via commercial registers) to prevent fraud

Optional components

Wizard: A UI for signing Verifiable Credentials in a Verifiable Presentation on the client side.

Wallet: An application for storing and presenting Credentials to third parties, also known as an Agent, Credential Registry, or Identity Hub.

Catalogue: An instance of the Federated Catalogue using the Credential Event Service.[17]

[16] Data Spaces Business Alliance. *Technical Convergence V2.* April 2023. Available at: https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf

[17] https://gitlab.com/gaia-x/lab/gxdch/-/blob/main/README.md?ref_type=heads#gaia-x-digital-clearing-house

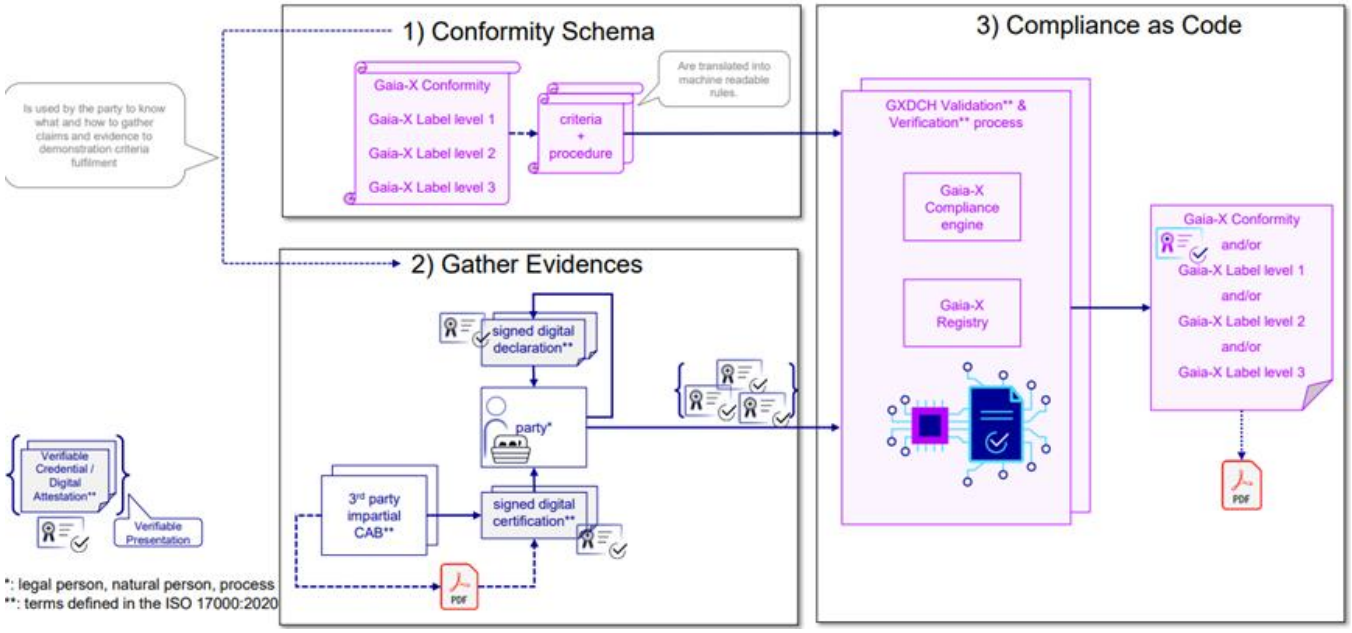


Figure 21. Procedure for Gaia-X Compliance.

Gaia-X Compliance Levels

Gaia-X introduced the **Standard Compliance**, along with three optional label levels, ranging from **Label Level 1** (the lowest) to **Label Level 3** (the highest). These levels are represented by what are known as labels. This system enables participants to adapt the level of security and trust to their specific requirements.

The **Trust Framework** (Standard Compliance**)** is a set of rules that define the minimum baseline for participation in the **Gaia-X** Ecosystem. These rules ensure a common governance and the basic levels of interoperability across individual ecosystems while allowing users to maintain control over their choices.[18]

The Gaia-X **Labelling Framework** is grounded in a set of core principles, starting with high-level objectives that are refined through specific labelling criteria. A Gaia-X Label is a mark of confidence that signifies the fulfilment of various criteria related to transparency, data protection, security, interoperability, portability, sustainability, and European control. These principles promote consistency across the ecosystem, enabling scalability, extensibility, composability, and modularity. They are also aligned with existing standards and incorporate both self-assessment and independent verification by Conformity Assessment Bodies (CABs).

Each level expands upon the previous one, addressing specific criteria such as data protection, cybersecurity, and geographical restrictions. A Gaia-X Standard Compliance and Gaia-X Label attestation may be requested for any product or service offering.

Gaia-X Standard Compliance and Gaia-X Label level attestations verify compliance at the time of assessment; however, they do not guarantee continuous adherence. Domain experts can extend them to meet the specific requirements of a particular industry, and they offer traceability for contract execution.

The compliance levels are as follows:

Gaia-X Standard Compliance: This is a universal set of standards designed to apply to all types of providers worldwide.

[18] https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.04/#fn:digitalsov

Gaia-X Label Level 1: This entry-level compliance guarantees adherence to standard data protection and security regulations in accordance with European laws.

Gaia-X Label Level 2: This level signifies enhanced data protection and security standards that comply with European laws and are primarily based on established certifications.

Gaia-X Label Level 3: This is the highest compliance level, designed for services that require exceptional data handling, security, and legal control. It is exclusively for European providers.[19]

Property	Standard Compliance	Level 1	Level 2	Level 3
Declaration of Service or Product	✓	✓	✓	✓
Signed with verified method	✓	✓	✓	✓
Automated validation by GXDCH	✓	✓	✓	✓
Automated verification by GXDCH	✓	✓	+	+
Data Exchange Policies	✓	✓	✓	✓
Certified Label Logo		✓	✓	✓
Data protection by EU legislation		✓	✓	✓
Manual verification by CAB			✓	✓
Provider Headquarter within EU				✓

Figure 22. Design Principles for Gaia-X Standard Compliance and Labels [20].

*: *not all criteria can be automated.

+: means automated verification of the evidence issuer (Standard & Conformity Assessment Bodies **CAB**)

Gaia-X Infrastructure

Gaia-X establishes an interconnection between service providers and service users, fostering trust through a technological framework that embodies the principles of transparency, openness, interoperability, and data reversibility.[21]

[19] https://gaia-x.eu/wp-content/uploads/2024/09/Compliance-Document_Marketing-Summary-2024.pdf
[20] GAIA-X European Association for Data and Cloud "Gaia-X Compliance Document - 24.06 Release"

[21] Trust Framework architecture - Gaia-X Architecture Document - 25.05 Release

The Gaia-X Architecture is designed to effectively support a diverse range of service offerings through a sovereign and adaptable interconnection of infrastructure and data ecosystems, facilitating the flexible exchange of data among various participants. Consequently, interconnection services represent a distinct category of resources[22]

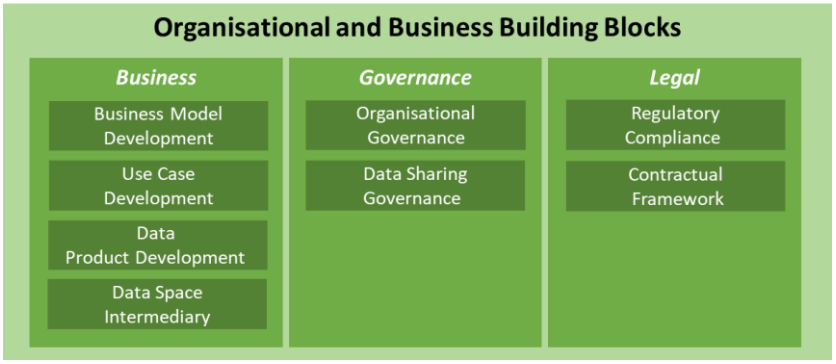
The Infrastructure Ecosystem focuses on computing, storage, and interconnection elements. In terms of assets and resources, these elements are categorized as nodes, interconnections, and various software assets. They encompass a spectrum of services, from low-level offerings like bare metal computing to highly sophisticated solutions such as high-performance computing. Interconnection services facilitate secure and efficient data exchange among different providers, consumers, and their services. Gaia-X enables integration of services across multiple ecosystem providers.

Network, compute, and storage services are always combined to provide a cloud or edge service that is presented to the user. Network services are always necessary for users to access compute and storage services. Even in the case of platform or application services, which abstract the underlying network, compute, and storage services, the network remains essential for enabling user connectivity to these services. This becomes especially important when several providers deliver distinct parts of the services. Applications may be merged from different infrastructures found within the same data centre but run by different providers, within the same city or metropolitan area, across different locations in the same country, or even across different countries and regions. For instance, computing and storage may be provided by different infrastructures.

Gaia-X aims to ensure a secure, interoperable, and scalable digital ecosystem by addressing the specific requirements for networking and interconnection. These requirements are satisfied through three key building blocks that focus on self-description model, inter-cloud provider measurements that describe connectivity between nodes/providers and interconnection and network services based on internet, QoS attributes and metrics.

7.2 DSSC alignment

SM4RTENANCE adheres closely to the DSSC Blueprint Framework, which provides a structured foundation for designing interoperable, sovereign, and federated Data Spaces. The architecture distinguishes clearly between business and organizational building blocks (such as business model, participation management, and regulatory compliance) and technical building blocks, including data models, trust framework, and value creation services. This separation ensures that SM4RTENANCE delivers the necessary technical capabilities while at the same time supports robust, transparent, and trustworthy governance across its pilots.



[22] https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/Introduction_and_scope/

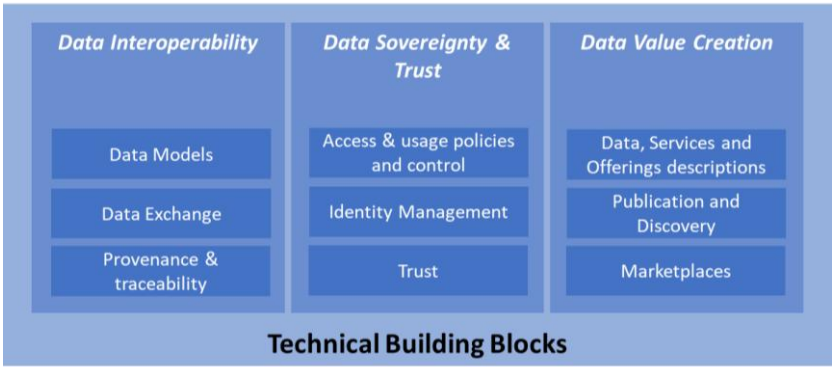


Figure 23. Data Space Support Centre (DSSC) Building Blocks.

Each pilot within SM4RTENANCE could follow a DSSC-compliant architectural pattern, allowing for a tailored yet harmonized implementation across different industrial contexts. This includes the adoption of reusable DSSC patterns to ensure alignment in terms of capabilities, interoperability requirements, and policy enforcement mechanisms. As part of this approach, SM4RTENANCE will define a common semantic vocabulary and architectural method that supports domain-specific customizations while maintaining coherence with the overarching DSSC Reference Architecture.

By doing so, SM4RTENANCE cross-domain interoperability, simplifies integration, and contributes to the maturity and validation of the DSSC Blueprint through concrete, real-world deployments. This commitment ensures that each pilot serves as both a standalone solution and a building block within a federated, European-wide Data Space ecosystem.

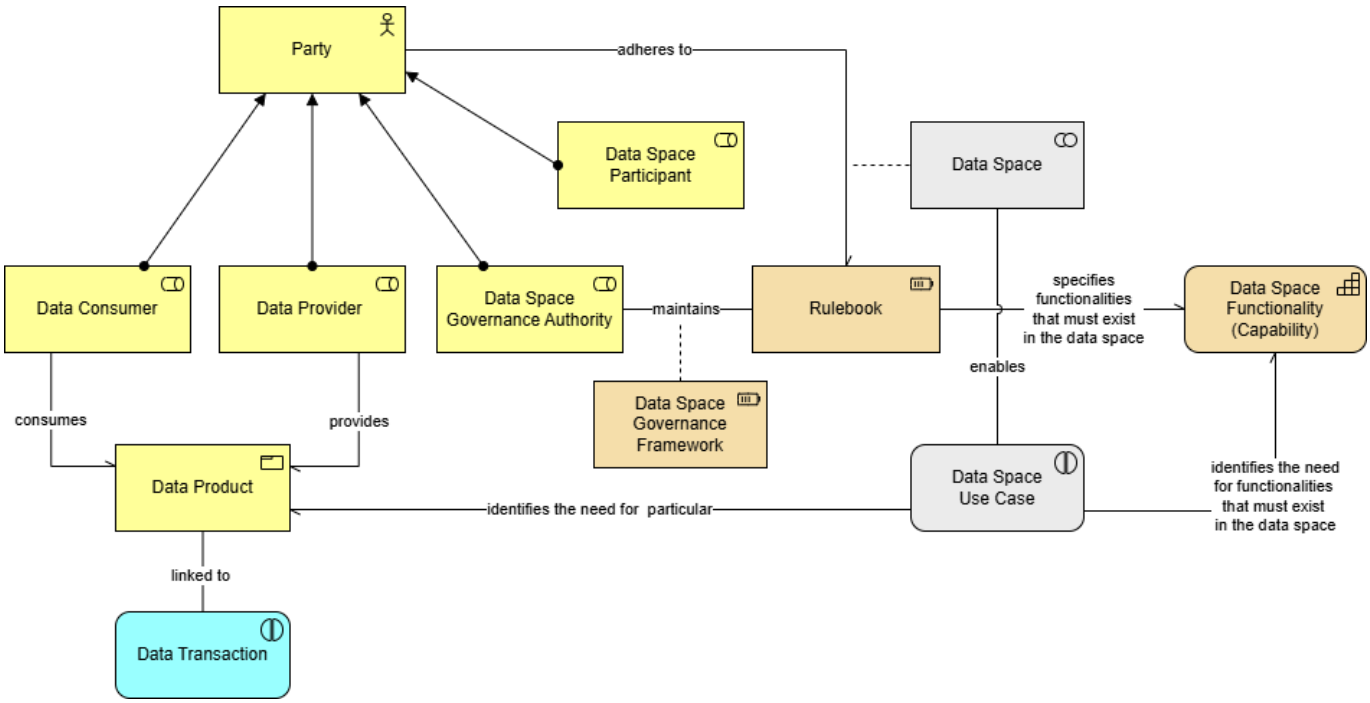


Figure 24. DSSC architecture for Data Spaces concepts and roles.