SM4RTENANCE

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

Title	D2.1 - SM4RTENANCE Data Space blueprint & Data Space harmonisation specifications
Document Owners	Jeremy Decis (DAWEX)
Contributors	Marcelo Ambrosio (Innovalia) Carmen Polcaro (Innovalia) Zisis Kyroudis (Atlantis Engineering) Vasiliki Vlahodimitropoulou (OTE) Ariane Yonta (DOMINA) Maximilian Wagner (VDMA)
Dissemination	PUBLIC
Date	28/04/2025
Version	1.0

Digital Europe Grant Agreement N.101123490

Document Fiche

Authors	Dawex
Reviewers	Domina
Work package	WP2
Task	Task 2.5 Asset 4.0 Data Spaces blueprint design & building block selection
Nature	Document
Dissemination	PU
Keywords	Data space, blueprint, federation, harmonization, interoperability, standards, architecture, infrastructure, data sharing

Disclaimer

This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of its content. This document may contain material, which is the copyright of certain SM4RTENANCE consortium parties, and may not be reproduced or copied without permission. All SM4RTENANCE consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.
Neither the SM4RTENANCE consortium as a whole, nor a certain party of the SM4RTENANCE consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered by any person using this information.

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

Abbreviations and Acronyms

Acronym	Meaning
AAS	Asset Administration Shell
AI	Artificial Intelligence
API	Application Programming Interface
BIM	Building Information Modelling
BPN	Business Partner Number
BSI	Federal Office for Information Security
CA	Certificate Authority
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CES	Credential Event Service
CSA	Coordinate and Support Action
CSV	Comma Separated Values
DDTR	Decentralized Digital Twin Registry
DGA	Data Governance Act
DID	Decentralized Identifiers
DIH	Digital Intelligence Hub
DISP	Data Intermediation Service Providers
DPP	Digital Product Passport
DS	Data Space
DSIF	Data Space interoperability Framework
DSP	Data Space Protocol
DSSC	Data Space Support Center
DT	Digital Twin
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EDC	Eclipse Dataspace Components
EHDS	European Health Data Space
EIF	European Interoperability Framework
EOSC	European Open Science Cloud
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	European Union
FAIR	Findable Available Interoperable Reusable
FTP	File Transfer Protocol
GXDCH	Gaia-X Digital Clearing House
GXFS	Gaia-X Federation Services
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IATP	Identity and Trust Protocol
IDS	International Data Spaces
IDTA	Industrial Digital Twin Association

IEC	International Electrotechnical Commission
IP	Intellectual Property
IRS	Item Relationship Service
ISO	International Organization for Standardization
IT	Information Technologies
JOSE	JavaScript Object Signing and Encryption
JSON	JavaScript Object Notation
KIT	Keep It Together
LLM	Large Language Model
MDS	Mobility Data Space
MQTT	IoT communication standard
MX	Manufacturing X
NDA	Non-disclosure Agreement
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OIDC4VC	Open ID Connect for Verifiable Credentials
OIDC4VP	Open ID Connect for Verifiable Presentations
OPC	Open Platform Communications
OSP	Onboarding Service Providers
PKI	Public-key infrastructure
RAM	Reference Architecture Model
RAMI4.0	Reference Architecture Model for Industry 4.0
SAMM	Semantic Aspect Meta Model
SFTP	Secure File Transfer Protocol
SHACL	Shapes Constraint Language
SIMPL	Secure IoT Middleware Platform
SME	Small and Medium Enterprise
SOC	State of charge
TDT	Trusted Data Transaction
TF	Task Force
TS	Technical Specification
VC	Verifiable Credential
WP	Work Package
eIDAS	Electronic Identification And trust Services
W3C	World Wide Web Consortium

List of partners

Short name	Legal name
AFS	AFNET SERVICES
ATLA	ATLANTIS ENGINEERING AE
AVL	AVL LIST GMBH
BAIDATA	ASOCIACIÓN PARA DESARROLLO DE LA ECONOMÍA 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	ASOCIACIÓN DE EMPRESAS TECNOLÓGICAS INNOVALIA
ITEMA	ITEMALAB S.R.L
MADE	MADE SCARL
NTTDES	NTT DATA SPAIN, SL
NTTDSL	NTT DATA SPAIN SOLUCIONES TECNOLOGICAS SL
OTE	ORGANISMOS TILEPIKOINONION TISELLADOS OTE AE
PIA	INDUSTRIE 4.0 OSTERREICH – DIE PLATTFORM FUR INTELLIGENTE PRODUKTION
PIAC	FRATELLI PIACENZA S.P.A
PRIMA	PRIMA INDUSTRIE SPA
SCSN	STICHTING SMART CONNECTED SUPPLIER NETWORK
SOVITY	SOVITY GMBH
SQS	SOFTWARE QUALITY SYSTEMS SA
SYXIS	SYXIS VS

TNO	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO
TOP-IX	CONSORZIO TOP-IX - TORINO E PIEMONTE EXCHANGE 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)

List of figures

List of tables

1 Executive Summary

This deliverable will present the SM4RTENANCE blueprint based on the analysis of embryonic Data Spaces from CATENA-X, MANUFACTURING-X, BAIDATA, SCSN, DFIX already existing in the EU Data Space ecosystem. The objective will be to identify what is missing to achieve the federation of Data Spaces and their harmonization, to progress towards a unified manufacturing Data Space ecosystem.

The Data Spaces Support Centre (DSSC) is the main European body responsible for providing general guidance to support the development of Data Spaces. The ambition of the SM4RTENANCE Blueprint is to align with the DSSC Blueprint v.1.5, published in October 2024. Alignment with the DSSC Blueprint aims to support the interoperability and openness of the SM4RTENANCE architecture, ensuring a reliable foundation with broad access to existing Data Spaces services and infrastructure. The Blueprint will serve as an essential tool for guiding and coordinating the remaining development work required to achieve the project objectives as SM4RTENANCE progresses. The blueprint will provide the starting point for continuous joint development and collaborative innovation in the establishment of a data sharing infrastructure that will support manufacturing across Europe for years to come.

2 Introduction

2.1 Purpose and scope of the deliverable

This deliverable is part of *Work Package (WP) 2 Data Space ecosystem industry commons*, which spans 18 months, i.e., the entire first half of the SM4RTENANCE project, ending halfway through the Data Space Alignment phase.

This deliverable has been built in the context of the *T2.5: Asset 4.0 Data Spaces blueprint design & building block selection M6-M24 (Leader DAW, Contributors*, that will address the specification of the DSSC reference technical building blocks. Based on the technical requirements identified in T2.1, this deliverable will design the SM4RTENANCE blueprint, will select the building blocks and will specify the operational infrastructure and components that will be required to implement the SM4RTENANCE Data Space. This deliverable will be a starting point for the continuous assessment of DSSC reference blueprint, SIMPL implementations and SM4RTENANCE requirements to maintain a common blueprint to ensure Data Space continuity across SM4RTENANCE Data Spaces. This document is structured as follows

- Introduction to the concepts of Data Space and to the specificities of the manufacturing domain
- Analysis of the current EU initiatives and assets for supporting Data Spaces standardization,
- Analysis of existing manufacturing Data Spaces and the challenges to be addressed to achieve Data Spaces harmonization,
- Definition of the governance principles for Data Spaces federation and harmonization,
- Proposition of a SM4RTENANCE architecture aligning with the DSSC Blueprint and common EU standards and initiatives

2.2 Relation to other WPs and tasks

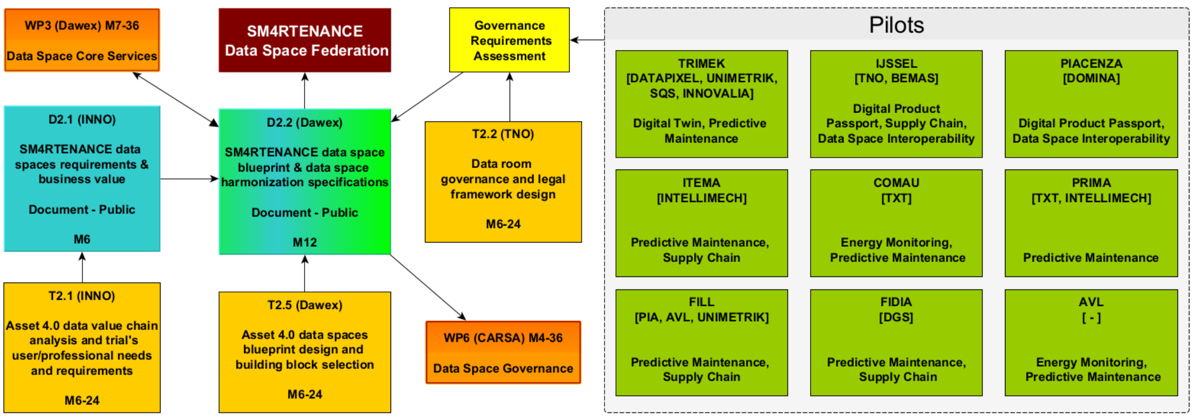

Figure 1. Deliverable 2.2 links to other Work Packages, Tasks, Deliverables and activities.

The overarching theme across this deliverable is establishing the SM4RTENANCE blueprint in alignment with existing Data Spaces and related initiatives, while exploring the challenges to interoperability and how well positioned the existing projects are towards it. These activities fall under T2.5, and materialize in this report, both of them led by Dawex.

Nevertheless, this deliverable is also interrelated with structures on different hierarchical levels of the SM4RTENANCE project. It has a mutual feedback link with WP3 (two-tone orange block in Figure 1) in relation to the definition of the architecture and blueprint of the SM4RTENANCE Data Space (red block in Figure 1). Work Package 6 is expected to recollect the governance requirements reported in this deliverable, which originate from the work in T2.2, specifically, the series of interviews with the Pilots under the umbrella of the Governance Requirements Assessment.

3 Introduction to Data Spaces in the manufacturing domain

3.1 Definition

According to DSSC Glossary a Data Space is an " *Interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants*. ".

According to DSSC Glossary a Data Space is an "A distributed system defined by a **governance framework** that enables secure and trustworthy **data transactions** between **participants** while supporting trust and **data sovereignty**. A Data Space is implemented by one or more **infrastructures** and enables one or more **use cases**".[1]

The DSSC rely on the definition of a Data Space, which borrowed from the recently published CEN CENELEC workshop agreement on Trusted Data Transactions:

This definition includes several elements

Interoperability. To share data, participants in a Data Space need to ensure they're technically, semantically, legally, etc., interoperable. The Data Space provides common governance principles, standards, practices, and enabling services. As you will see later, these are bundled into what is often called a 'rulebook' or 'governance framework'.

Services. All kinds of services are needed to form these frameworks, such as identifying and onboarding participants or making data findable. Each participant also needs services to connect their own data sources with the Data Space and vice versa.

Trust. Trust enables participants to make informed decisions about how, when, and with whom to share data.

[1] https://dssc.eu/space/Glossary/176554052/2.+Core+Concepts

Note that there currently is no formal/legal definition of a Data Space; in different context the term is defined slightly differently. In the definition above for example the term 'framework' is used, but of course Data Spaces have instances as well.

Data Spaces aim to achieve:

- **Data Sovereignty**: Ensuring that data providers retain control over their data, including who can access it and under what conditions.
- **Interoperability**: Enabling seamless integration and use of data from various sources by supporting different data formats and systems
- **Innovation and Collaboration**: Promoting data-driven innovation and collaboration across sectors, leading to new business models and services.
- **Security and Privacy:** Providing robust security measures and compliance with data protection regulations to maintain the confidentiality and integrity of data.
- **Economic Growth**: Enhancing the value derived from data, which can drive economic growth and competitiveness.
- **Public and Private Sector Collaboration**: Facilitating cooperation between public and private entities to address common challenges and leverage shared data for the public good.

Data spaces should be built around key concepts. The DSSC considers the Participants, Data Products, Services, and Rulebooks as the core concepts of every Data Space[2].

Table 1. Data Space components according to DSSC Blueprint 1.5.

Component	Description
Data Provider	A data provider is an entity that owns or controls data and makes it available within the Data Space for other participants to access or use. Data providers retain sovereignty over their data, meaning they can set specific terms and conditions on how their data can be accessed, shared, and utilized by others in the Data Space. They are responsible for ensuring the quality, accuracy, and compliance of their data with relevant standards and policies.
Data Consumer	A data consumer is an entity that accesses and utilizes data made available within the Data Space to gain insights, perform analyses, or support decision-making. Data consumers agree to abide by the terms and conditions set by data providers, including usage limitations and compliance requirements.
Service Provider	A service provider offers technical, analytical, or support services to enable the functionality of the Data Space. This can include providing infrastructure, data processing tools, security, and interoperability solutions that facilitate data exchange. They can also create additional value by providing data related services, for example by helping data providers to enhance their data products. Service providers play a crucial role in

[2] https://dssc.eu/space/Glossary/176554052/2.+Core+Concepts

	supporting the Data Space's operations, ensuring data is accessible, secure, and meets participants' performance needs.
Data Space Governance Authority	The governance authority oversees and manages the Data Space, ensuring compliance with the rulebook and maintaining a secure, trustworthy environment for data sharing. It establishes the Data Space's governance model, enforces adherence, and resolves disputes among participants. The governance authority is essential for building trust within the Data Space, and to oversee that participants adhere to agreed-upon rules and ethical standards.
Rulebook	The Rulebook as a comprehensive set of guidelines, standards, and agreements that govern the operation and management of a Data Space. The goal of the Rulebook is to establish trust, transparency, and interoperability among Data Space participants, and ensure that they adhere to a common Data Space governance framework. The Rulebook typically addresses legal, technical, organizational, and operational aspects of data sharing to facilitate a secure and efficient data ecosystem. It defines the roles and responsibilities of all involved parties, ensuring that data sovereignty and privacy are maintained. By adhering to these rules, participants can operate within a trusted environment, where they know their data is protected, and all parties comply with established standards, fostering collaboration and enabling the efficient and secure exchange of data.
Participant Agent Service	These are services required for an individual participant to join a Data Space. For example: storing and exchanging a verifiable credential sharing which data is made available and publishing it in a catalogue specifying and enforcing access and usage policies integrating with actual data sources or data processing services
Federation services	These are services that facilitate the interplay of participants for all kinds of data sharing. For example: issuing verifiable credentials to participants of a Data Space, indicating that they're a participant in the Data Space, confirming an identity or complying with a specific policy providing a shared catalogue of available participants and data products in the Data Space providing policy information that participants can use to assess whether someone can be granted access (e.g. personal consent) providing services for provenance and observability Some of these services must comply with specific EU legislation, such as eIDAS or the EU Data Governance Act. This provides additional assurance to the users of such services, e.g., prohibiting the re-use of data by these services for purposes other than facilitating the data sharing between participants.
Value creation services	These are services operating within the Data Space that support value creation. For example, an AI service that can analyse data or a visibility service providing tracking and tracing functionality. Depending on each Data Space's use cases and business model, many such services can exist.

Data Product	A data sharing unit, bundling resources (data and/or data services) and metadata that describes the license terms, the resources, and other information in a machine-readable way. While the content of data products may vary, we talk of a package of resources and all information that a potential data product consumer needs, to make a decision whether to consume the data product or not. A data product typically includes • the resource, that can be data and/or data service, • the description of the resource, • its allowed purposes of use, • quality, format, frequency, duration and other requirements the data product fulfils, • access and control rights (e.g., attribution, Intellectual Property Rights, liabilities, geographical limitations, usability for training LLMs), • delivery options (e.g., APIs, SMTP, web interface, mapping tools), • information about data provenance and lineage, • pricing and billing information, • other information (e.g., ethical considerations), • and metadata describing all these above. Data products are offered to Data Space participants in a consumable form, to be discovered and consumed by data product consumers on a self-serve basis. Data products comply with a data product specification. Productising data means transforming data into consumable and marketable data products
Data Transaction	Data transaction refers to a unique immutable, i.e. unmodifiable unit of data access or exchange, logged, treated in a coherent and reliable way independent of other data transactions. A data transaction requires trust between participants, regulatory compliance, contractualization, licensing, technical exchange management and traceability. There are 2 kind of data transactions **Data transaction in a distributed mode** - Data transactions in a distributed mode rely on a network topology where nodes are exchanging data with each other peer-to-peer. Distributed systems are suited for use cases where trust in participants is pre existing, allowing direct transfer between parties. **Data transaction in a managed mode** - A data transaction in a managed mode refers to a data transaction where an intermediary acts as a trusted third party. The data flows from the data provider to the acquirer via the third party, which manages trust, cataloguing and traceability. Managed systems are suited when trust must be enforced by a third party.

3.2 The overall context in EU and the key challenges of the manufacturing domains

Driven by the European Commission, more and more Data Spaces have been or are being deployed in a wide range of sectors. The following table summarizes the current and upcoming Data Space landscape, including organizations, projects and Data Spaces, operational and under development. As the list is constantly evolving, it should not be seen as exhaustive

Table 2. Data Space initiatives, projects and implementations.

Name	Category	Field	Description
AgriDataSpace [3]	Project	Agriculture	Focuses on data sharing in agriculture to improve farming practices, enhance sustainability, and address food security challenges.
ATLAS	Project	Agriculture	Provides a platform for agricultural data sharing, promoting precision farming, resource efficiency, and sustainable agricultural practices.
BAIDATA [4]	Organization	Data Economy	Supports the development of public-private data ecosystems through research, development and training activities. Focuses on regional Data Space pilot projects.
Catena-X[5]	Operational Data Space	Manufacturing and Automotive	Provides an open, scalable data ecosystem for the automotive industry, aiming to improve efficiency, innovation, and collaboration among manufacturers and suppliers.
Data4Industry[6]	Data Space in development	Manufacturing	Data exchange solution tailored for the industrial sector, engineered to enhance data and information exchange across global organizations, subsidiaries, and suppliers, with a focus on boosting competitiveness and reducing carbon footprints.
Energy Data Space [7]	Data Space in development	Energy and Utilities	Facilitates data exchange in the energy sector, promoting smart grid development, renewable energy integration, and energy efficiency.

[3] https://agridataspace-csa.eu/
[4] https://baidata.eu/en
[5] https://catena-x.net/en/1
[6] https://www.data4industry-x.com/
[7] https://energy.ec.europa.eu/publications/common-european-energy-data-space_en

EU Data SP4CE[8]	Preparatory action	Manufacturing	Initiative aimed to establish a framework for secure, fair, and cost-effective data sharing across manufacturing ecosystems within the EU.
European Health Data Space (EHDS) [9]	Data Space in development	Health	Aims to facilitate the secure exchange of health data across Europe to enhance research, improve personalized medicine, and support health systems.
European Open Science Cloud (EOSC) [10]	Data Space in development	Research and Academia	Provides a platform for the sharing of scientific data and resources across Europe, fostering collaboration and accelerating research and innovation.
Factory-X [11]	Project	Manufacturing	Focuses on creation of an open and collaborative data ecosystem for the manufacturing sector that enhances both horizontal and vertical integration within the manufacturing supply chain.
Finance Data Space [12]	Data Space in development	Financial Services	Supports the secure sharing of financial data to improve services like credit scoring, fraud detection, and personalized financial products.
Gaia-X[13]	Organization	Cross-Sector	Aims to create a federated and secure data infrastructure for Europe, ensuring that data sharing across various sectors adheres to European standards and values.
Green Deal Data Space [14]	Data Space in development	Green Deal Objectives and Sustainability	Supports the achievement of Green Deal objectives by facilitating data sharing related to environmental sustainability, climate action, and green technologies.
Manufacturing-X [15]	Initiative	Manufacturing	Aims to enhance data-driven innovation and collaboration in the manufacturing sector by creating a common Data Space for industrial data sharing.
Mobility Data Space (MDS) [16]	Operational Data Space	Transportation and Mobility	Enhances data sharing in transportation to optimize traffic management, public transport, and smart mobility solutions.

[8] https://www.fiware.org/project/eu-data-sp4ce.html
[9] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
[10] https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science/european-open-science-cloud-eosc_en
[11] https://factory-x.org/
[12] https://www.european-financial-data-space.com/
[13] https://gaia-x.eu/
[14] https://green-deal-dataspace.eu/
[15] https://www.plattform-i40.de/IP/Navigation/EN/Manufacturing-X/Manufacturing-X.html
[16] https://mobility-dataspace.eu/

Public Administration Data Space [17]	Data Space in development	Public Administration	Aims to improve data sharing and collaboration within and between public sector organizations to enhance public services and governance.
SCSN [18]	Operational Data Space	Supply Chain and Logistics	The Smart Connected Supplier Network (SCSN) facilitates data sharing across supply chains to improve efficiency, traceability, and collaboration among logistics partners.
Skills Data Space [19]	Data Space in development	Education and Skills	Focuses on sharing data related to education and skills to support lifelong learning, workforce development, and alignment of skills with labour market needs.

Data spaces are designed to enable secure, efficient, and interoperable data exchange among a range of stakeholders. However, realizing these goals involves navigating various complexities. Data spaces are facing structural challenges that still ampere the realization of their objectives. The identification of these structural challenges should support the analysis of the limits of the current models, and the definition of SM4RTENANCE strategy for achieving the harmonization and federation of Data spaces.

1. Data Security and Privacy

Challenge: One of the foremost concerns in managing data is safeguarding it from unauthorized access and potential breaches. Organizations must implement robust security measures to protect sensitive information from cyberattacks, hacking attempts, and other security threats. Additionally, they need to navigate and comply with various privacy regulations, which dictate how personal data should be handled, stored, and shared. Ensuring compliance while maintaining high levels of security can be complex and resource-intensive.

2. Interoperability

Challenge: Achieving seamless interoperability between diverse systems, applications, and platforms is critical for effective data management. This involves enabling different technologies to communicate and exchange data efficiently, despite variations in data formats, standards, and protocols. The lack of standardization can lead to data silos, integration issues, and inefficiencies. Solving interoperability challenges requires adopting universal standards or creating middleware solutions that can bridge gaps between disparate systems.

3. Data Quality and Provenance

Challenge: Ensuring data quality involves maintaining the accuracy, consistency, completeness, and reliability of data throughout its lifecycle. Poor data quality can lead to erroneous insights, flawed decision-making, and operational inefficiencies. Additionally, tracking data provenance—knowing

---

[17] https://reform-support.ec.europa.eu/document/download/d622cef5-8ff9-404d-8301-ee133c2d0192_en?filename=Session%202%20-%20Data%20Spaces%20for%20Public%20Administrations.pdf
[18] https://www.mcb.eu/fr/SCSN
[19] https://www.skillsdataspace.eu/

the origin, changes, and history of data—is crucial for validating its authenticity and reliability. This challenge necessitates rigorous data management practices, validation techniques, and provenance tracking mechanisms.

4. Scalability and Performance
Challenge: As data volumes and data transaction loads increase, it is essential to ensure that the data infrastructure can scale accordingly without compromising performance. Scalability involves designing systems that can grow and handle larger amounts of data and higher transaction rates efficiently. Performance challenges include maintaining fast data processing speeds, low latency, and high availability, even under heavy load. Addressing these issues often requires advanced architecture, optimized algorithms, and scalable cloud solutions.

5. Cost and Resource Management
Challenge: Managing the costs associated with data infrastructure, including storage, processing, and maintenance, is a significant concern. Organizations must balance the need for robust data solutions with budget constraints and resource availability. This includes expenses related to hardware, software, cloud services, and compliance requirements. Efficient resource management involves optimizing infrastructure usage, leveraging cost-effective solutions, and planning for future growth without overspending.

6. Governance
Challenge: In order for Data Spaces with different legal forms and structures to work together, it is necessary to define general rules for collective operation. These rules concern the business model (between territorial Data Spaces or platforms), the governance, decision-making and escalation processes, and the organisation that will be responsible for steering this governance. It should be noted in this context that the Data Governance Act, which came into force in September 2023, defines the obligations and responsibilities of organisations that offer data exchange services (known as Data Intermediation Service Providers, or DISPs). These regulations will be monitored in France by ARCEP. Thus, any strategy for interoperability within and between Data Spaces will need to devise clear governance processes, at both 'local' and 'federal' levels, and envisage the creation of a governance organisation. More specifically, the interoperability of business models will need to be worked on in depth. For example, if access to platform A is subject to subscription conditions and charges for the use of services, it will be necessary to determine under what conditions other platforms, and their users, can access platform A's products and services.

4 The EU normative Data Space Ecosystem

Data spaces are part of a whole broader strategies, towards data-driven ecosystems, supported by key initiatives, which aim to create a federated data infrastructure supporting Data Spaces across different sectors. Gaia-X, IDSA, DSSC, OpenDEI, Manufacturing-X, are key initiatives to Europe's strategy for developing Data Spaces, and they play a critical role in ensuring digital sovereignty, data interoperability, and innovation across the continent.

Digital Sovereignty: These initiatives ensure that Europe maintains control over its data, reducing dependency on non-European cloud providers and tech giants. This is crucial for Europe's independence in the digital economy.

Security & Privacy: Europe places a strong emphasis on the protection of personal data, and these initiatives help create infrastructures that are compliant with the GDPR (General Data Protection Regulation) and other security standards.

Interoperability: By fostering standards and protocols (like the ones from IDSA and SIMPL), these initiatives facilitate interoperability across different systems, allowing seamless data exchange between sectors and countries.

Economic Innovation: Data-driven innovation is key to Europe's future economic growth. These initiatives support the creation of an open, secure, and scalable environment for data exchange, driving new business models and opportunities across industries.

Boosts Digital Transformation for Industry 4.0: They support the digitalization of industries by providing an ecosystem where industrial data can be securely shared and analysed. This is essential for the modernization of traditional industries and moving towards Industry 4.0.

Together, they ensure that Europe is well-positioned to lead in the global digital economy while safeguarding its values and interests.

4.1 Gaia-X

Gaia-X, a not-for-profit Association that was established in 2021, unites a variety of organisations (such as large companies and SMEs, developers and users of technology, industrial players, and academic members) to achieve one common goal: to enhance the European data economy by enabling the creation of common Data Spaces, in full alignment with the EU's data strategy. Gaia-X is committed to the development of a common standard for a digital ecosystem that is open, transparent, and secure. This standard will serve as the foundation for a new data infrastructure that ensures the safe and trustworthy exchange of data.

Gaia-X aims is to provide the European Single Market with unparalleled opportunities for innovative data-driven business models, thereby reducing the reliance on non-controllable technologies and reflecting Europe's need for data and cloud sovereignty. The association is open to everyone and aligns with the European values of human-centricity, transparency, openness, and sovereignty. Gaia-X mission is to design and implement a data sharing architecture that includes common data sharing standards, best practices, tools, and governance mechanisms. Additionally, it represents a federation of cloud infrastructure and data services that is firmly established in the European Union, with the commitment of all 27 EU Member States. This overarching mission serves as the driving force behind the Gaia-X architecture.

Based on the principles of European data and cloud sovereignty, Gaia-X intends to build a federated open data infrastructure. Gaia-X seeks to create a digital governance system that can be implemented on any existing cloud or edge technology platform, thereby enabling data and service transparency, controllability, portability, and interoperability.

The Gaia-X vision is expressed through the creation of two ecosystems: data and infrastructure, which are interconnected by federations. The three conceptual pillars for the achievement of this vision are[20]:

- Gaia-X Compliance: Decentralized services that foster objective and measurable trust.
- Data Spaces / Federations: Interoperable and portable cross-sector datasets and services
- Data Exchange: Established contract rules for access and data usage

The objective of this framework aims to enable the portability, exchange, and sovereignty of services and data among providers, thereby opening the European Data Market to enhance competitiveness and ultimately foster growth and social equality. This vision will only become a reality if all three pillars are fully realized.

The initiative publishes technical specifications to allow constructions of European Data Spaces

- Gaia-X **Architecture Document**
- Gaia-X **Data Exchange Document**
- Gaia-X **Policy Rules Conformity Document**

The Gaia-X Architecture document describes the essential concepts for building the Gaia-X data and infrastructure ecosystem. It integrates the necessary Providers, Consumers and Services to facilitate this interaction. These services include securing identities, implementing trust mechanisms, and controlling the data use, exchange and compliance, all without the need for individual agreements.

Architecture Document 24.04[21]
A new milestone was reached with the publication of the Gaia-X Architecture Document 24.04

A particular element to highlight in the document is the section mapping the Gaia-X Architecture, the Gaia-X Digital Clearing Houses components, specifications on Federated Catalogues, and enhancements to Identity, Credential, & Access Management, as well as major updates for Data Exchange Conceptual and Operational Models.

Data Exchange document 23.11[22]
The release of the Gaia-X Data Exchange Document 23.11 is a major update to the Data Exchange Services specifications and paves the way for a secure and trustworthy data economy.

[20] https://gaia-x.eu/gaia-x-framework/

[21] https://gaia-x.eu/news-press/announcing-the-latest-release-of-the-gaia-x-architecture-document-24-04/
[22] https://docs.gaia-x.eu/technical-committee/data-exchange/23.11/dewg/

Major updates to the Data Exchange Conceptual and Operational Models were released and technical ontologies for Data Product, Data Transaction, Policies & Data Product Usage Contracts, and Data Usage Descriptions have been introduced, based on open standards like DCAT-V3 and ODRL.

This document serves as guiding principles to all organizations looking at creating data ecosystems and Data Spaces which have become a fundamental component of business competitiveness and economic sovereignty.
The Gaia-X Compliance document consolidates the previous deliverables "Policy Rules & Labelling Document" and the "Gaia-X Trust Framework", and introduces the new criteria for Data Exchange services within the Gaia-X framework among other significant advancements.

By encompassing in the document Data Exchange services criteria, this defines what it means to be compliant to Gaia-X when conducting data exchanges.

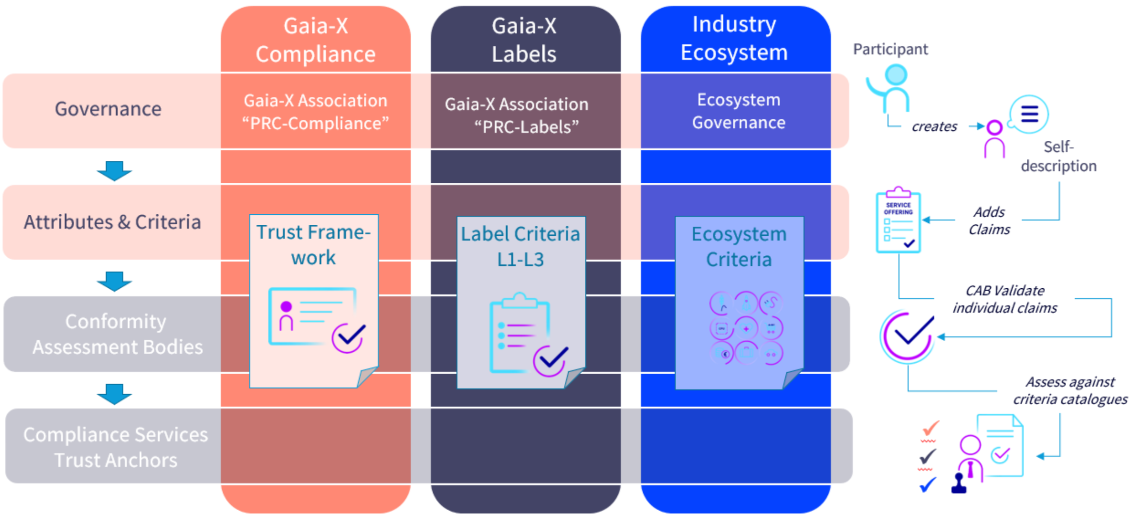

Figure 2. Gaia-X Compliance - Enable Trust & Governance 23

The Gaia-X Trust Framework is a comprehensive set of rules that define the minimum requirements for participation in the Gaia-X ecosystem. These rules offer a common governance structure and ensure basic interoperability among the individual ecosystems, thereby allowing control over decisions to be maintained.

The Gaia-X Trust Framework implements the requirements defined by Gaia-X, as described in the Policy and Labelling Document and the Architecture Document. The Architecture Document specifies the standards and protocols that ensure seamless interoperability among various systems,

[23] https://gaia-x.eu/gaia-x-introduces-the-compliance-document-to-enable-and-increase-trust-security-and-european-sovereignty-in-digital-ecosystems/

facilitating the exchange of information and enabling the utilization of that information in mutually beneficial ways.

The Trust Framework defines verifiable credentials and linked data representations as fundamental components of its future operations. Trusted information will be retrieved in machine-readable formats, and where such formats are unavailable, Gaia-X will implement procedures to convert trusted information into machine-readable formats. This conversion is essential for the federation of trusted assertions within the Gaia-X ecosystem and for the development of mechanisms to re-evaluate the validity of claims within the trust framework.

The GXDCH (Gaia-X Digital Clearing House) serves as a node of verification of the Gaia-X rules, and it is an essential part for the operationalisation of Gaia-X in the market. It acts as the entry point for achieving Gaia-X compliance and becoming part of the Gaia-X ecosystem. GXDCHs are non-exclusive, interchangeable nodes operated by market participants, functioning as Gaia-X federators. They operate and execute the mandatory and optional Gaia-X Framework services necessary for compliance and facilitate the onboarding of any Gaia-X adopter. The Gaia-X framework outlines the software assets, technical requirements, and functional specifications necessary for compliance with Gaia-X standards. This framework guarantees the distributed and decentralised characteristics of Gaia-X compliance, which is not centralised by the Gaia-X Association.[24]

The Gaia-X concept of sovereignty includes the autonomy and self-determination necessary for users to make informed technological decisions. All providers in Gaia-X are obligated to provide **Gaia-X Credentials**, formerly known as Self-Descriptions, which are standardised, machine-understandable metadata that describe their service offerings and themselves. Gaia-X Credentials are the common language used by participants in a Gaia-X ecosystem to communicate with one another.[25] The Gaia-X Conceptual Model, as published in the Gaia-X Architecture Document, outlines the relationships between all entities in the Gaia-X ecosystem. "Provider," "Service Offering," and "Resource" are the most critical entities. A Provider is defined by Gaia-X as a participant who "operates resources and creates service offerings." A Service Offering is a digital service that can be ordered. Services may be derived from resources or may be dependent upon other service offerings from third parties. Providers use metadata to describe themselves, their service offerings, and the resources that comprise them. The Self-Descriptions are comprehensible to the Federation Services that oversee the Self-Descriptions throughout their lifecycle, as well as by consumers, including humans and the automated machine agents that support them.[26]

A federated technical architecture is not possible without an essential network infrastructure. Interconnection and networking are fundamental components for connecting and federating all of the different entities inside the ecosystem. Gaia-X creates an infrastructure ecosystem by establishing portability and interoperability between network and interconnection providers, Cloud Solution Providers (CSP), High Performance Computing (HPC), sector-specific clouds and edge systems. Mechanisms are developed to find, combine and connect services from participating providers in

---

[24] https://gaia-x.eu/gxdch/

[25] Conceptual Model - Gaia-X Architecture Document - 24.04 Release

[26] GXFS White Paper “Self-Description of Resources, Service Offerings and Participants within Gaia-X Ecosystems”

order to enable a user-friendly infrastructure ecosystem. Gaia-X supports distributed use cases, spanning from on-premises set-ups, cloud hosted infrastructure through to facility to edge cases.

Building the Data Space Industry 4.0 on Gaia-X
A cloud/edge infrastructure is the backbone of Data Space Industry 4.0 and associated business models. This paves the way for data and service hosting and processing that is both sovereign and transparent. Many different stakeholders are working together on the European project Gaia-X to build a federated cloud architecture that will allow for the development of Data Spaces across different industries. Currently, the architecture for the Data Space Industry 4.0 is being developed in close collaboration with the European Gaia X Foundation as well as the national Gaia hubs. Thus, industrial requirements can be included into the Gaia framework and vice versa.[27]

4.2 DSSC

The Data Spaces Support Centre (DSSC) is a key implementation initiative of the European Data Strategy delivered through the Digital Europe Program. One of the objectives of the DSSC is to accelerate the deployment, scaling and adoption of Data Spaces in Europe. In attaining that objective, the DSSC aims to fully respect European values, and supporting the European economy and society.
The DSSC is fostering the development of Common European Data Spaces through exploring the needs of Data Space initiatives. Additionally, it defines common requirements and establishes best practices to accelerate the formation of sovereign Data Spaces. Herewith, the DSSC contributes to realizing the vision of a genuine European single market for data.

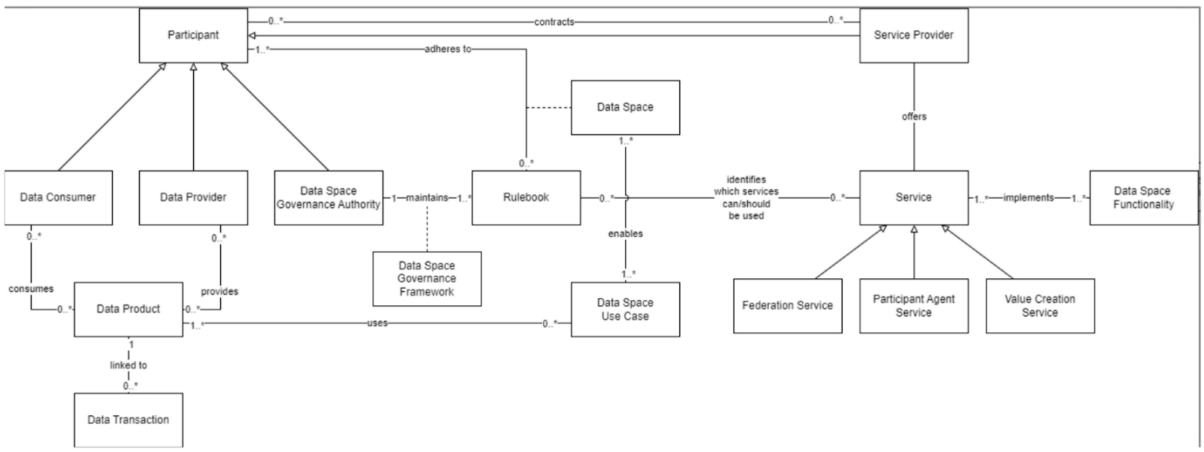

Figure 3. DSSC core conceptual model of a Data Space.

[27] Federal Ministry for Economic Affairs and Climate Action Platform Industrie 4.0 Position Paper “Creating the Data Space Industrie 4.0”, Available online: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/PositionPaper-DataSpace.pdf?__blob=publicationFile&v=1

4.2.1.1 The Data Space Support Centre

The DSSC has several offerings they provide to Data Spaces and Data Space initiatives[28]. The main ones we focus on in this report are the *Building Blocks*, and the *Glossary*. Both of these are part of the DSSC blueprint. The building blocks are meant to break down the Data Space into smaller manageable pieces. The building blocks are the "*basic units or components that can be implemented and combined with other building blocks to achieve the functionality of a Data Space*"[29]. Figure 4 provides the latest rendition of the DSSC Building Blocks, which comes out of Blueprint version 1.5. The DSSC Glossary is meant to establish "*consistent and coherent terminology for DSSC communication and publications*"[30]

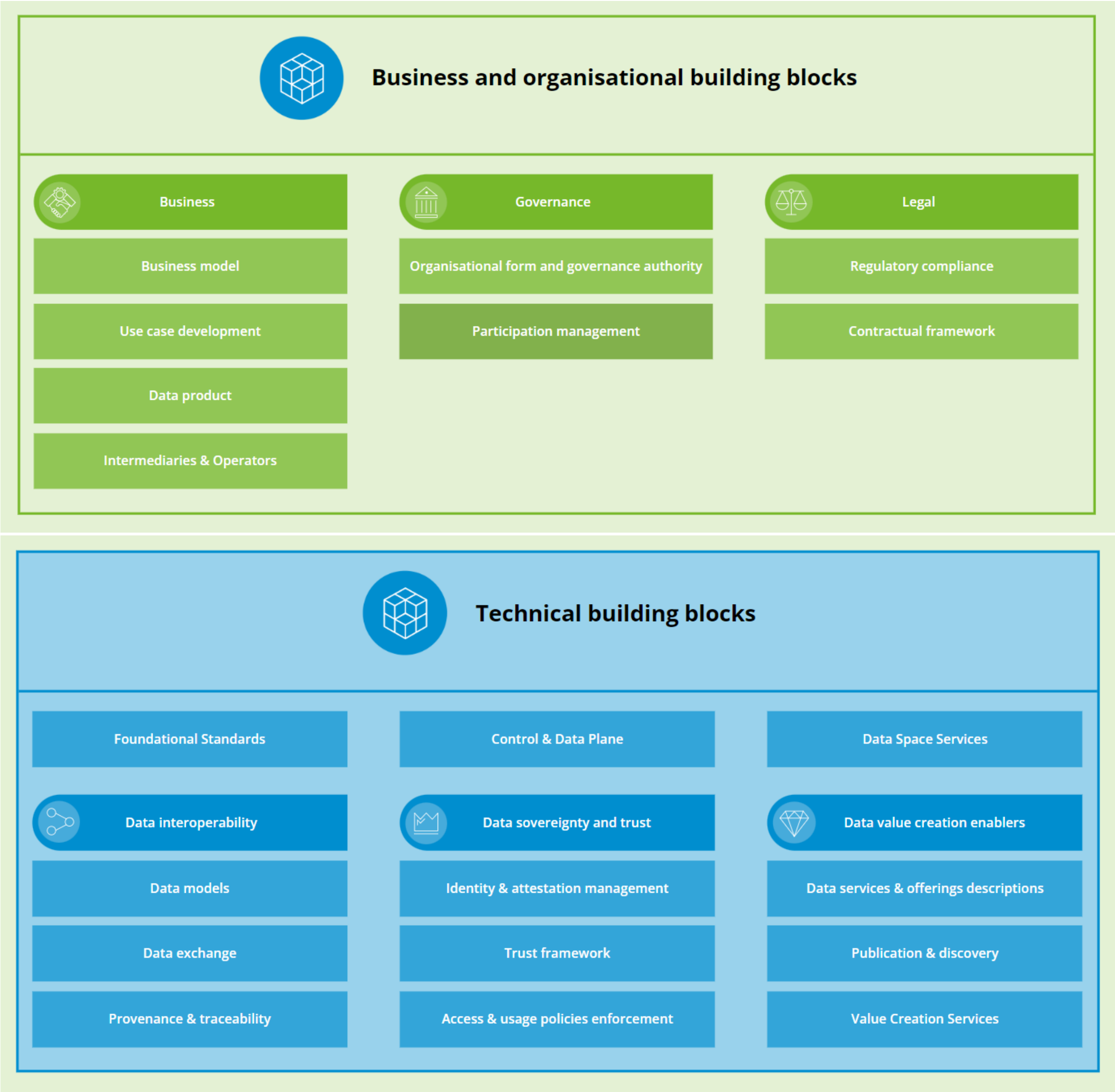

Figure 4: DSSC building block blueprint v1.5

[28] The full DSSC offerings: https://dssc.eu/page/knowledge-base
[29] https://dssc.eu/space/bv15e/766064046/Building+Block+Overview
[30] https://dssc.eu/space/bv15e/766061530/Introduction+-+DSSC+Glossary

In Blueprint version 1.5[31] (most recent at the time of writing), the DSSC has identified **thirteen design principles** that correspond to seventeen building blocks that were analysed in D2.1 across **six** fundamental pillars: **Business, Governance, Legal, Data Interoperability, Data Sovereignty and Trust, and Data Value Creation Enablers**. These principles are classified into two distinct categories: pillar-specific design principles and cross-pillar design principles. The pillar-specific principles offer direction for the design and operation of building blocks inside a single pillar, while the cross-pillar principles are relevant to building blocks spanning many pillars in the Data Space blueprint. Table 3 presents a comprehensive enumeration of the design concepts along with their respective categories.

Table 3. Data Space design core principle.

Category	No	Design Principles	Pillars
Pillar – Specific Design Principles	**1**	Reusability of Data	Data Value Creation Enablers
	2	Ensure Data Interoperability in Data Spaces	Data Interoperability
	3	Establish a fit-for-purpose contractual framework	Legal
	4	Adaptable Data Space governance framework	Governance
	5	Pursuit of Quality by Design	Data Value Creation Enablers
Cross-pillar Design Principles	**1**	Incentives and synergies between Data Space participants	Business Data Value Creation Enablers
	2	Discoverability, Availability, and Accessibility of Data	Business Data Sovereignty and Trust Data Value Creation Enablers
	3	Transparency	Governance Data Interoperability Data Sovereignty and Trust Data Value Creation Enablers
	4	Establishing Trust and Security in Data spaces	Legal Data Sovereignty and Trust
	5	Ensure compliance with EU legal framework and norms	Legal Governance Data Sovereignty and Trust
	6	Ensure Participants Rights in Data Sovereignty	Governance Data Interoperability Data Sovereignty and Trust
	7	Promote Participation Through Inclusivity	Governance Data Value Creation Enablers

[31] https://dssc.eu/space/bv15e/766061169/Data+Spaces+Blueprint+v1.5+-+Home

	8	Promote environmental sustainability	All Pillars

Pillar Specific Design Principles

Reusability of Data

The reusability of data adds significant value, as it allows access to shared data for reuse by multiple participants, domains, and use cases. Data product owners must describe their data effectively to facilitate its use in different contexts. The reusability of data design principle supports this process by providing guidelines and sharing best practices to ensure data serves new users and use cases beyond its original purpose. This promotes reusability, breaking down traditional data silos and enabling shared access for stakeholders, leading to more informed strategies. Several guidelines and mechanisms are implemented that encourage data reuse, including the promotion of reuse, the regulation of reuse through policies, the establishment of data sharing agreements and open licensing frameworks, and the assurance of traceability. Thorough documentation and metadata should accompany data, making it easier to find, understand, and re-use.

Data Interoperability in Data Spaces

Interoperability significantly improves collaboration among diverse organizations and systems, thereby promoting the creation of more comprehensive and valuable datasets. The implementation of standardized data handling techniques enhances the quality and consistency of data, which in turn increases its reliability for analysis and decision-making. Adopting common standards, data models and communication protocols ensures that different systems can understand and exchange data effectively. These standards might include data formats, API interfaces, and communication protocols. Metadata is the backbone of data interoperability. By providing essential information about data, metadata enables organisations to share, reuse and analyse data effectively, fostering innovation and collaboration.

Establish Fit-for-Purpose Contractual Framework

Data spaces facilitate secure data exchange between providers and recipients. A customized contractual framework is crucial for efficient and secure transactions. The objective of this design principle is to provide guidelines and mechanisms for creating a flexible, enforceable, and standardized contractual framework that facilitates data-sharing transactions and the establishment of Data Spaces. This framework should be clear, enforceable, and standardized, promoting trust and data sovereignty. The framework must be dynamic enough to enable the Data Space to evolve, incorporating rules for onboarding and offboarding participants, renewing governance standards, and updating technologies. Contracts should be legally and technically enforceable, assigning responsibility for breaches and controlling data access.

Adaptable Data Space Governance Framework

The Data Space Governance Framework is a comprehensive set of principles designed for the management and oversight of a Data Space. It outlines the roles, functions, and responsibilities of the governance authority and the participants. The framework must be flexible, adaptable, and future proof, enabling rapid changes and decision-making to address emerging challenges while remaining relevant as regulations and technology evolve. Scalability is vital for accommodating growth without sacrificing efficiency. Achieving a balance between adaptability and scalability is essential, with thoughtful implementation that considers regulatory and ethical standards. This framework is intended to evolve in response to user needs and the dynamics of the data ecosystem.

Pursuit Quality by Design

Quality is crucial in Data Spaces for generating value from products, services, and metadata. The Data Space governance authority sets minimum quality standards focusing on accuracy, completeness, timeliness, consistency, validity, availability, performance, and reliability. The design principle aims to provide guidelines for producing high-quality data sets, services, and metadata, building confidence, encouraging collaboration, and promoting data sharing among stakeholders. The Data Space governance authority must define quality characteristics, establish metrics, and set KPIs to promote collaboration and data sharing, balancing ambition with practicality through continuous assessment and validation processes.

Cross Pillar Design Principles

Incentives and Synergies Between Data Space Participants

The objective of this design principle is to promote synergies among participants, which will result in mutual advantages such as value generation and monetisation. It lays the foundation for the business and data value creation enablers that are the building blocks of the Data Space blueprint, providing guidelines for creating synergies and incentivising engagement. This is crucial for sustainable development, data sharing, and collaboration, as it establishes compelling incentives for active participation.

Ensure Compliance with EU Legal Frameworks and Norms

Compliance with EU legal frameworks is crucial for the effective operation of a Data Space, ensuring alignment with regulations such as the General Data Protection Regulation (GDPR), the Data Governance Act, and the Data Act. Adhering to these laws guarantees data privacy, security, transparency, and equitable access for all participants, fostering trust and successful collaboration in data sharing. This design principle provides guidance and mechanisms that ensure compliance with applicable EU laws while safeguarding fundamental rights and promoting fair competition.

Discoverability, Availability, and Accessibility of Data

The potential of shared data resources is maximized by three key factors: discoverability, availability, and accessibility. Discoverability refers to the ease with which stakeholders can locate the necessary data, fostering collaboration and innovation across various sectors. Availability ensures data is accessible when needed, enabling timely decision-making and efficient operations. Accessibility focuses on how users interact with data, enhancing user-friendly interfaces and formats tailored to different skill levels.

Transparency

Trust and collaboration among participants are based upon transparency in Data Spaces. The governance framework should prioritise transparency in the decision-making, responsibilities, and onboarding and offboarding processes. Evaluation processes should be conducted with clarity and transparency, guaranteeing that the criteria and justification behind decisions are easily accessible. This will facilitate understanding and effective participation of prospective participants.

Establishing Trust and Security in Data Spaces

Data spaces are crucial for the operation of digital transactions, as they rely on the trustworthiness and reliability of participant information. Risks such as identity theft, broken authentication, compromised access control, sensitive data exposure, and Distributed Denial of Service (DDoS) attacks can undermine trust among participants. To mitigate these threats, Data Spaces must implement robust security measures and adhere to best practices that protect sensitive information while maintaining trust.

Ensure Participants Rights in Data Sovereignty

The design principle outlined here focuses on two key aspects: data sovereignty for participants and the policies that govern data usage and access. The primary objective is to provide comprehensive guidelines and mechanisms that enable Data Space initiatives to design, develop, and operationalize processes, activities, and collaborations that uphold participants' rights regarding data sovereignty.

Promote Participation Through Inclusivity

The design principle of inclusive governance, fairness, and equality is crucial for Data Space initiatives. It ensures equitable initial conditions and access to data and services based on specific policies, contracts, and consents. Active involvement of all voting members in building a Data Space and its governance framework is essential. This democratic approach recognizes diverse perspectives and priorities within the Data Space, promoting inclusive governance. The governance authority should maintain open communication throughout the governance lifecycle.

Promote Environmental Sustainability

Data spaces play crucial role in promoting environmental sustainability in sectors such as agriculture, healthcare, energy, and smart cities by facilitating data sharing among stakeholders. They enable the collection and dissemination of information that can have a beneficial effect on the environment such as reducing carbon footprints.

4.3 IDSA

The International Data Spaces Association (IDSA) has defined a data sharing framework (IDS)[32] that includes a reference architecture, open-source building blocks, and a certification process for the development and operation of Data Spaces.

[32] https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/1_introduction

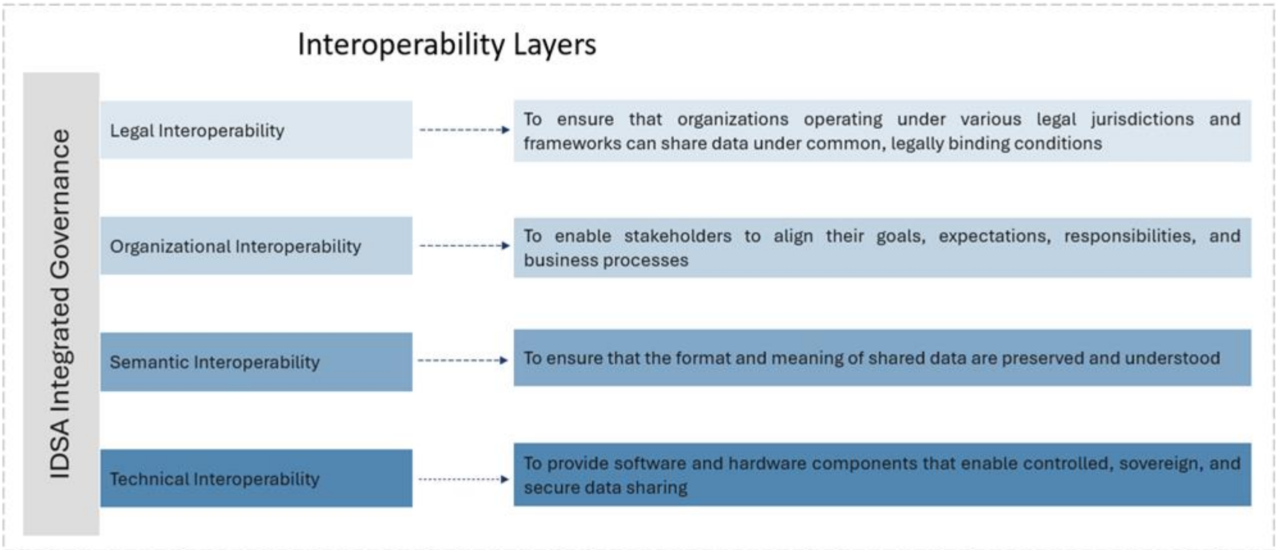

Figure 5. IDSA Interoperability Framework based on EIF.

The IDS Reference Architecture Model[33] (IDS RAM) defines the main components and requirements for developing a Data Space. It provides a standardised vocabulary and framework for the design and implementation of Data Spaces, ensuring both technical and semantic interoperability between different Data Space implementations. This includes standards for data connectors, data models and security measures, as well as rules for data governance.

The IDSA Rulebook fulfils multiple purposes concerning the development and functioning of Data Spaces. The objective is to define precisely which regulations are compulsory and which are optional guidelines and propose a roadmap for developing a common framework and best practices for Data Spaces.[34]

It is important to highlight that there are two types of interoperability when considering interoperability in Data Spaces. Intra Data Space interoperability refers to the ability of individual participants within a single Data Space to effectively exchange and use data. Inter-Data Space interoperability enables participants to access data from multiple Data Spaces.

The European Commission developed the European Interoperability Framework (EIF), which offers guidelines for addressing interoperability challenges. There are four layers of interoperability: technical, semantic, organisational and legal. Furthermore, the four layers also include a background layer, "interoperability governance," and a cross-cutting component, "integrated governance."[35]

The four levels of interoperability can also be applied to Data Spaces, as described below.

[33] https://internationaldataspaces.org/offers/reference-architecture/
[34] https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/1_introduction
[35] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/solution/eif-toolbox/6-interoperability-layers

Technical Interoperability

Technical interoperability is a critical requirement in Data Spaces and should be implemented by data connectors in accordance with specifications and standards. The Dataspace Protocol (DSP) acts as the foundation for technical interoperability in Data Spaces. This protocol is developed to enable the interoperable sharing of data between entities that are governed by usage control. It relies on web technologies and provides a set of specifications. The interaction of Participants in a Data Space is carried out by Participant Agents, called Connectors. [36]The connector is a software installed by the participating company or a platform thereby providing technical access to the IDS ecosystem. A data connector must cover multiple levels of interoperability, such as the general interaction between the connectors to describe the data assets and their associated endpoints, the definition of policies for access control and usage control, as well as the negotiation of these policies and contracts. While most interactions take place between Connectors, some interactions with other systems are required.

Semantic Interoperability

Semantic interoperability is the term used to describe the ability of information technology systems to exchange data with a shared and clear meaning. This is an essential prerequisite for federated data networks, including IDS and Data Spaces in general. Semantic interoperability requires that data providers and consumers within the network explicitly refer to a common vocabulary when describing their data offerings or requirements. It enables the exchange of data between entities by utilizing data information models or semantic meanings that are understood. When interacting systems assign the same meaning to an exchanged data item, the data remains consistent across systems, regardless of individual data formats. This consistency of meaning can be achieved by referencing to established standards or agreements concerning the format and meaning of data, or by employing shared vocabularies in a dynamic manner, either in schema form and/or through an ontology-driven approach.

The semantic models utilized in a Data Space are essential for ensuring interoperability. This encompasses semantic models for the data intended for sharing within the Data Space, as well as semantic models that describe the Data Space itself, including its policies, participants, and processes.

Organisational Interoperability

Organizational interoperability focuses on how various organizations collaborate to achieve their mutually agreed-upon objectives. Within the framework of Data Spaces, organizational interoperability involves the processes, policies, and governance structures that enable data sharing, including the definition of roles, responsibilities, and formal agreements. A well-governed Data Space

[36]IDSA, September 2024, **Data Connector Report**: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Data-Connector-Report-84-No-16-September-2024-1.pdf

requires an accurate definition of organisational processes. All participants in a Data Space must conform to same processes.[37]

Legal Interoperability

Legal interoperability refers to the ability of organizations operating under diverse legal frameworks, policies, and strategies to collaborate effectively[38]. In the context of Data Spaces, legal interoperability pertains to the recognition of the legal equivalence of contracts and contractual terms across different data ecosystems.

The IDS Identity Concept

The International Data Spaces is a trust framework that enables the exchange of trusted data between data providers and consumers within a Data Space across companies. The IDS Connector, a specific data endpoint that is certified against security criteria, is required for participants to transfer data between various systems, applications, or platforms. It fulfils two critical functions: it enforces cybersecurity measures and usage policies to safeguard trust and provide Data Exchange Services.

Identity is at the core of any Data Space, ensuring that all participants can be authenticated and authorized securely. The International Data Spaces provide federated identity management in accordance with contemporary standards, building trust and enabling participants to make autonomous and informed decisions.

Identity and Access Management (IAM) is a critical security domain that encompasses a variety of technologies and business processes. Its primary objective is to ensure that authorized individuals and devices can access necessary resources at the appropriate times and for legitimate purposes, thereby preventing unauthorized access and fraud. The key components of IAM involve user authentication, authorization, and the management of user roles and permissions.

The IDS Identity Provider offers an authentication service for all participants in the Data Space. It provides capabilities to create, maintain, manage, monitor, and validate identity information for these participants. This functionality is particularly crucial for establishing a network of trust within the IDS. The Identity Provider in the IDS consists of three interconnected components: Certificate Authorities (CAs) are responsible for issuing and managing technical identity claims, the Dynamic Attribute Provisioning Service (DAPS) provides temporary tokens containing up-to-date information

[37] https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/3_interoperability

[38] https://joinup.ec.europa.eu/collection/digital-skills-public-sector/solution/interoperable-europe-academy/legal-interoperability-ex-ict-implications-eu-legislation

about connectors, and the Participant Information Service (ParIS) offers business-related information of IDS Participants in both machine- and human-readable formats.

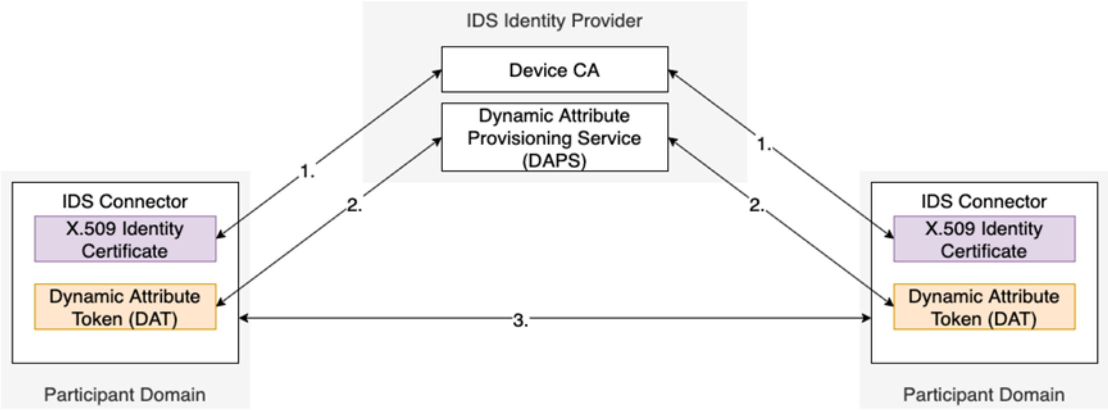

Figure 6. Interaction between IDS connectors and Identity Components s[39].

4.4 OpenDEI

The OPEN DEI Initiative was a European Union-funded project launched in June 2019 and concluded in early 2023. Its participants were based in four European Member States: Belgium, Germany, Italy, and Spain. Its primary goal was to support the EU's Digital Transformation strategy by developing common data platforms and unified architectures for key sectors, including manufacturing, agriculture, energy, and healthcare. Through aiming to bridge gaps, encourage collaboration, and enhance communication among various Innovation Actions, OPEN DEI sought to maximize the impact of the EU's digitalization efforts.

A central focus of OPEN DEI was Platform Building, which involved comparing existing reference architectures and open-source implementations to establish a unified industrial data platform. This initiative was essential for creating a standardized digital infrastructure that could support diverse industrial applications across Europe. The project also concentrated on Data Ecosystem Building, aiming to create an innovation and collaboration platform through a European network of Digital Innovation Hubs (DIHs). This included contributing to an industrial skills catalogue and observatory, which were designed to bolster digital capabilities and foster collaboration within the industry. Another significant objective was Large Scale Piloting, which involved developing a digital maturity model and creating assessment methods and benchmarking tools. These tools were intended to guide industries through their digital transformation processes, helping them measure progress and navigate their migration journeys effectively. Standardisation was another key focus of the OPEN DEI initiative. The project conducted cross-domain surveys, promoted and implemented standards, and built alliances with existing EU and standard-developing organizations. This work aimed to ensure

[39] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/perspectives-of-the-reference-architecture-model/4_perspectives/4_1_security_perspective/4_1_2_identity_and_trust_management

that digital transformation efforts were supported by robust, widely accepted standards that facilitated interoperability and integration across different sectors.

The project assigned Task Forces (TF) to address specific challenges in digital transformation. TF1 (Data Sharing Spaces) established design principles for cross-sectoral Data Spaces, while TF2 (Data-Powered Business Ecosystem Building) developed reference models to guide data-powered digital transformation. TF3 (Digital Platforms, Pilots, and Standards) focused on creating tools and knowledge for platform architecture, and TF4 (Digital Transformation & Business Impact) analysed the adoption drivers and barriers for platforms and assessed their business impact. Of particular importance were the Task Force 1 contributions, focused on defining the foundational principles for Data Spaces, crucial for the future data economy. Under the coordination of the International Data Spaces Association, Task Force 1 developed an extensive position paper that detailed the design principles, building blocks, and governance structures necessary for effective and sovereign data sharing. This document, crafted with input from over 40 experts across 25 organizations and 13 Horizon 2020 projects, was the first comprehensive approach to establishing these principles. It aimed to ensure that Data Spaces could be built on a solid foundation of interoperability and governance, addressing both technical and organizational needs.

Throughout its tenure, OPEN DEI made substantial contributions in the manufacturing domain. The project successfully completed the activities outlined for its working groups (WGs). These groups generated significant knowledge about technical and standardization aspects of the digitalization process. They facilitated collaboration and cross-fertilization between various projects within the digital platform area and with projects from other domains. This collaboration provided a comprehensive overview of the manufacturing sector's progress towards digitalization. Another contribution of OPEN DEI was the creation of an Open Source Software catalogue, an extensive list of available software tools classified into 19 categories, including security and containerisation. The catalogue was designed to provide valuable tools for the daily work of projects, pilots, and use cases within the scope of the initiative. It served as a resource for selecting appropriate open source tools for development and architectural design, supporting the broader objectives of the project.

Evolving from the OPEN DEI, the Data Spaces Support Centre (DSSC) was launched in 2022 to build on the project's legacy. The DSSC expanded the scope of the work initiated by OPEN DEI to encompass a broader range of industries and societal perspectives. It continued the project’s efforts by serving as a central hub for Data Space initiatives, facilitating connections and supporting the development of interoperable and secure data-sharing systems. The DSSC aimed to act as a "help desk" for Data Spaces, assisting organizations in navigating the complexities of data governance and ensuring that the principles established by OPEN DEI were applied effectively across various domains.

4.5 EU DATA SPACE 4.0

EU DATA SP4CE developed a robust and sustainable data-ecosystem approach for the European manufacturing sector. The initiative established a governance model that supported hierarchical and non-hierarchical structures, enabling flexible collaboration among industry leaders, SMEs, and research organizations (see Fig. 7). Through this collaborative approach, the project addressed data sharing challenges and ensured interoperability across diverse stakeholders.

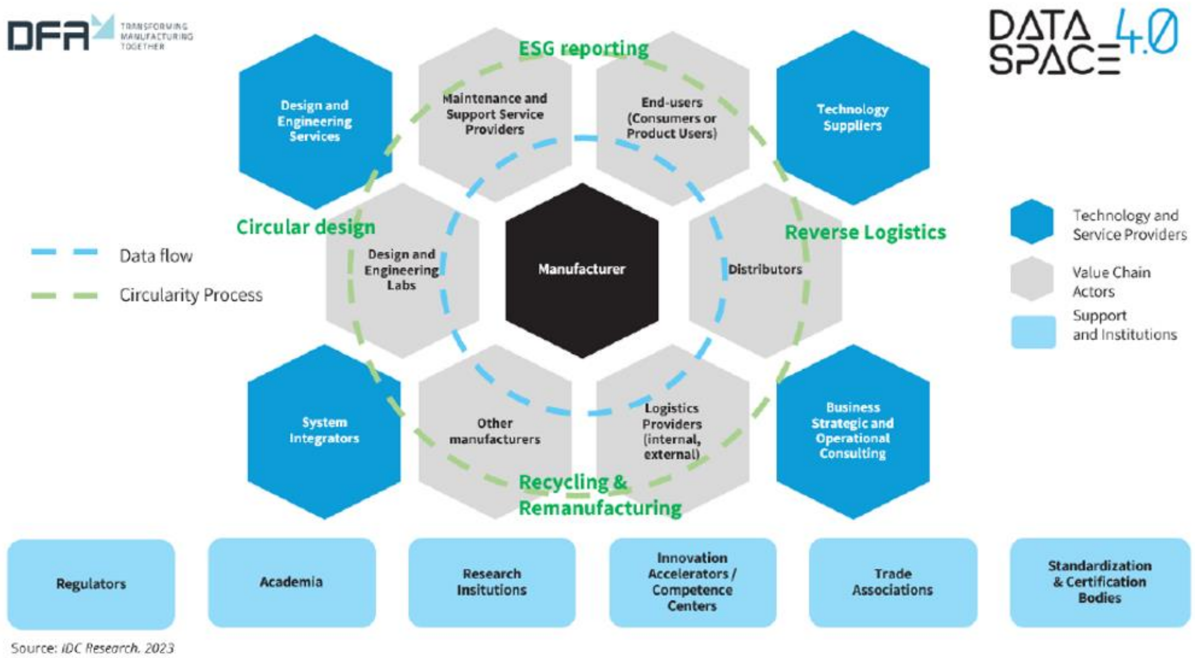

Figure 7. Collaborative scene around the manufacturing scene in the Data Space context.

The project aligned its framework with EU regulations, including the Data Governance Act, Data Service Act, and Data Act. It provided a detailed inventory of data platforms and developed certifiable blueprints for Data Space 4.0, establishing the technical foundation for interoperable systems. This effort facilitated the deployment of digital value chains, which were operationally feasible and scalable across the manufacturing sector. In addition, EU DATA SP4CE advanced sustainable business models tailored to the manufacturing industry, which emphasized economic viability while offering tangible benefits to stakeholders. Workshops and maturity assessment tools were implemented to guide organizations in integrating Data Spaces into their workflows. The project also prioritized high-quality data assets through a structured smart data model repository for Industry 4.0. Clear digital platform roadmaps supported applications such as predictive maintenance, collaborative asset management, and agile supply chain solutions. Aligning these efforts with the Data Space Support Centre further ensured scalability and global deployment of the Data Space model.

4.5.1 Manufacturing Data Space Value Journeys

Along the path of the digital transformation, organizations have to embark on both, a *Data Value Journey* and a *Business Value Journey*. The former involves identifying actors within the Data Value Chain, such as manufacturing companies, OEM providers, suppliers, and operators. These actors have access to extensive datasets generated by systems operating at various levels, including Engineering Technology (ET), Operational Technology (OT), Information Technology (IT), and Industrial IoT (IIoT). Often underutilized, these datasets achieve their full potential when shared through trusted mechanisms, such as Trusted Networks, Data Marketplaces, or Open Data portals. Data sharing unlocks the Business Value Journey, where organizations leverage federated edge-cloud ecosystems to access and utilize high-value datasets.

Existing digital manufacturing platforms are extended to support collaborative data sharing while maintaining control over internal systems. This enhanced connectivity gives rise to new industrial services and solutions that leverage expanded datasets, including predictive maintenance, asset management, and circularity applications. The federation of sovereign digital platforms amplifies data-sharing capabilities, enabling advanced processes and solutions within European Data Spaces.

4.5.2 Manufacturing Data Space Design Approach

A Data Space dedicated to the manufacturing-industry scenario integrates or streamlines various aspects of the manufacturing lifecycle, including:

- **Design**: Product Lifecycle Management and Engineering Data Product Lifecycle Management
- **Simulation**: Process Simulation
- **Supply Chain**: Optimization
- **Execution**: Manufacturing Execution Systems enabled by dynamic asset management and predictive/prescriptive maintenance
- **Aftersales**: Improved services with access to reliable data from the data value chain

Deploying and operating a Manufacturing Data Space requires a blueprint tailored to the unique requirements of each ecosystem. These ecosystems face several challenges, including varying Data Space needs, incompatible implementations of building blocks, and a lack of widely adopted certification programs and standards.

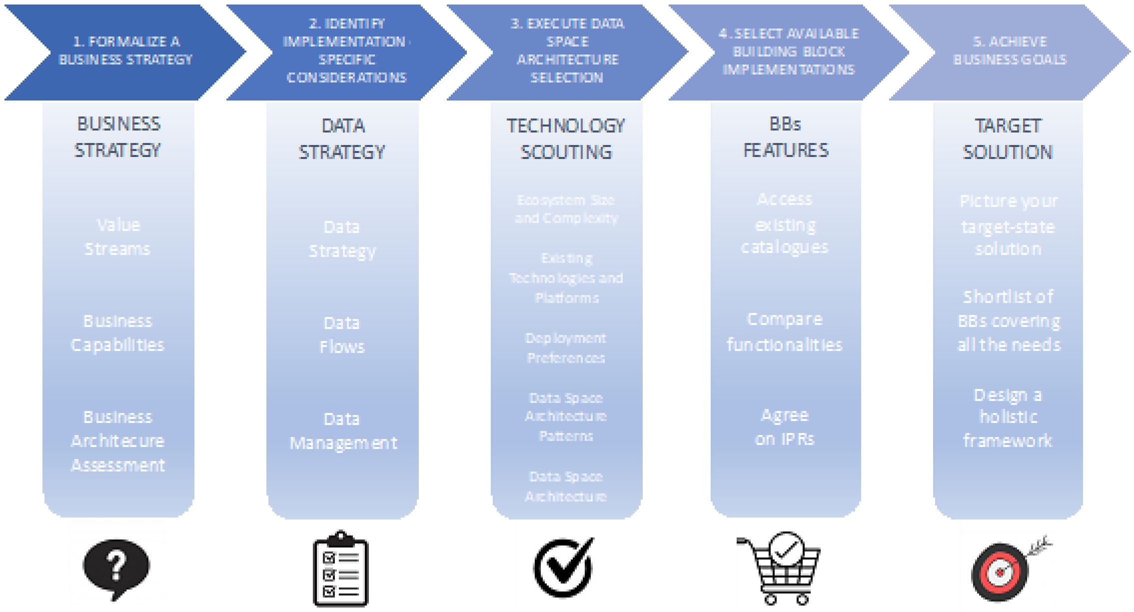

Figure 8. Five-step model design approach.

The 5-step-model design approach (see Fig. 8) is driven by clear business strategies and technology/BB mapping towards specific applications enablement. This approach is intended to support data-driven ecosystems development and identification of solutions that have a business value in the Data Space context.

4.5.3 Data Space 4.0 Reference Certification Programme Framework

The Data Space 4.0 Reference Certification Programme Framework (RCPF) ensures interoperability, security, and trust within data ecosystems. The framework is grounded in reference standards and open specifications, providing transparent compliance information. It adopts a modular approach, ensuring functional and technical interoperability without imposing strict limitations on functionality. Certification addresses both technology and participants, recognizing the distinct roles of data consumers, providers, service providers, and application developers. The framework differentiates between core components with cross-domain applicability and domain-specific applications, balancing certification and qualification processes.

Considerations for redundancy reduction, compatibility and cost efficiency were made while devising the principles that should guide certification design. The framework incorporates mutual recognition mechanisms, to ensure compatibility and trust across different ecosystems, making the certification model more scalable and sustainable. This ultimately aims to simplify adoption of Data Spaces within the European manufacturing sector. More specifically, the certification principles established in EU DATA SP4CES were :

- **Transparency and Compliance**: Provide clear information on compliance with reference standards and specifications.
- **Modular Approach**: Ensure functional and technical interoperability through a modular approach.
- **Interoperability and Security**: Validate and certify technology for interoperability and secure operation.
- **Role-Based Certification**: Certify participants based on their roles (data consumer, provider, service provider, etc.) and associated risks.
- **Differentiation between Core Components and Domain-Specific Applications**: Distinguish between cross-domain certification and domain-specific qualification.
- **Alignment with Market Standards**: Comply with market standards, such as ISO 27001, to ensure trust and reduce costs.
- **Mutual Recognition of Certifications**: Consider mutual recognition of certifications and standards to facilitate data sharing.

It is expected that certification programs emerging from SM4RTENANCE should have the above considerations as their baseline.

4.5.4 Community outreach efforts

The EU DATA SP4CE project has addressed the needs of diverse users and applications while proactively managing intellectual property rights (IPR) derived from the initiative. A strategic approach to dissemination and exploitation has ensured broad outreach, raising awareness in the manufacturing sector and empowering the Industry 4.0 community. Efforts to position the project as a central resource for addressing data and Data Space challenges have resulted in synergies with various projects, groups, and initiatives operating at industrial, manufacturing, digital, and data-driven levels across Europe. The project has also joined forces with international initiatives such as IDSA and FIWARE to contextualize manufacturing challenges within broader digital trends. Through these efforts, EU DATA SP4CE has supported SMEs and industrial organizations in adopting Data Space technologies, focusing on dataset prioritization and benchmarking embryonic and manufacturing Data Spaces.

As part of its knowledge transfer strategy, EU DATA SP4CE has actively organized, participated in, and engaged with global events to transfer expertise on Data Spaces to targeted audiences. A notable achievement has been its role as a moderator of the Thematic Working Group (TWG) on Data in Manufacturing within the European Digital Innovation Hubs (EDIH) Network. With over 80 EDIHs and 170 participants, this effort has built a thriving community supporting SME digital transformation. Tailored strategies have empowered SMEs, reaching 25% of the European manufacturing market, and provided guidelines and procedures for the effective transfer of Data Space 4.0 assets.

In parallel, EU DATA SP4CE's involvement in community-building events across Europe and beyond has contributed to the development of a Multi-Stakeholder Governance Framework and Federated

Data Ecosystems. Engaging a broad spectrum of stakeholders has enriched the governance framework with diverse perspectives, strengthening collaboration across the manufacturing supply chain. Collaboration with leading organizations in the Data Space field, including IDSA, DSSC, and GAIA-X, has expanded the project's audience while advancing critical objectives. Participation in Global Data Spaces Roundtables has further integrated EU DATA SP4CE into European discussions on Sustainable Business Models for the Data Economy and the development of Manufacturing Data Space Building Blocks and Blueprint Certification. Key events such as the DSSC Summits and Data Spaces Symposiums have been instrumental in aligning the project with prominent Data Space initiatives.

EU DATA SP4CE's growing presence at Hannover Messe Fairs (2022–2024) has established the project and its partners as credible sources of information for SMEs, organizations, and communities. With full representation in public panels, parallel sessions, and exhibitions, the project has amplified awareness of Data Spaces and strengthened the connection between manufacturing stakeholders and data-driven technologies, advancing the adoption of Data Spaces across Europe and internationally.
The outcomes of the project and its deliverables are available on https://manufacturingdataspace-csa.eu/ .

4.6 Manufacturing-X

Manufacturing-X is a common initiative from economy, politics and science aiming to create an international, interoperable data ecosystem that enables digital innovations for greater resilience, sustainability and competitiveness. Based on the initiative Manufacturing-X is also a German funding scheme from 2024-2026. Leveraging the globally recognized "Industrie 4.0" brand, Manufacturing-X builds on the foundational work done by the Plattform Industrie 4.0 network. This initiative has addressed key issues such as interoperable and secure data interfaces, trustworthy data infrastructure, innovative data-based business models, and legal considerations for data usage.
Manufacturing-X is characterized by:

- data-based networking of industry value chains – across industries and borders
- creating a space for innovation for resilient, competitive and climate-neutral production
- covering the entire life cycle of products and means of production – from the extraction of raw materials to recycling
- enabling of new, data-based business models and application solutions
- paving the way for scalable, industry-standard applications – for large companies and for SMEs
- is based on Gaia-X and stands for secure, open and sovereign data exchange

In the Manufacturing-X data ecosystem, companies can share and use data while still retaining control over their data. Companies can individually determine who has access to their data, for how long, and how it may be used. This concept of data sovereignty enables all players in value networks to work together in a spirit of trust and promotes the willingness to share data. Manufacturing-X paves the way to a data-based economy.

The Manufacturing-X initiative aims to create cross-industry data ecosystems with maximum interoperability. These should help to enable effective and efficient value creation for a resilient, sustainable and competitive industry. The following tasks are planned for this:

- definition of common standards for the implementation of Manufacturing-X for industry
- establishing technologies to enable data to be shared securely and confidently along entire value chains
- defining which technical, legal and organizational requirements must be created for this,
- making the initiative known to economic actors in particular through accompanying communication
- promoting concrete use cases, such as process improvements through data fusion from different sources or quality improvement through the use of machine, material and processing data.

The focus is on the implementation of practice-relevant added value, e.g.:

- efficient and fast traceability of supplied parts
- ESG reporting in complex supply chains
- decarbonization across various processing stages
- circular economy from design to disposal
- product passport management
- capacity management within and across sectors
- complex quality assurance and damage analysis

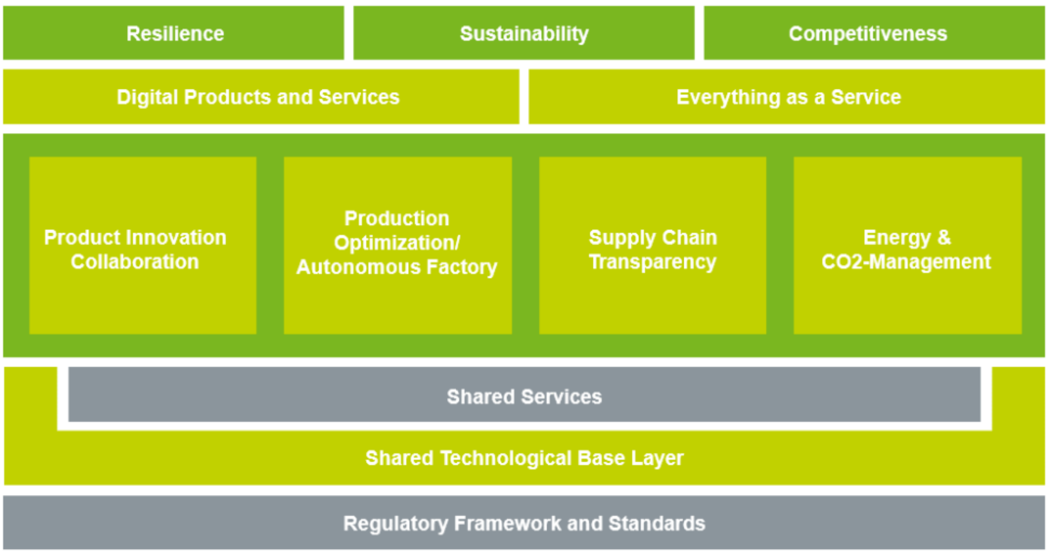

Figure 9. Manufacturing-X holistic approach[40]

[40] https://www.plattform-i40.de/IP/Redaktion/DE/Standardartikel/ManufacturingX_Framework.html

The Manufacturing-X initiative is based on a holistic approach to developing and promoting the next evolutionary stage of industrial production. The overarching strategic objectives, which focus on a resilient, sustainable and competitive industry, are fundamental to this. To this end, Manufacturing-X deals with cross-sector use cases for the collaborative use of data in order to leverage economic and ecological potential. To achieve this, uniform standards must be defined, which must be operated and lived in a fundamental technical infrastructure in order to ensure interoperability and sovereignty. Manufacturing-X is thus based on a common technical, organizational and legal framework and contributes to future development in cooperation with European and international legislators.

Developing a unified system architecture is of fundamental importance for establishing interoperable data ecosystems across various industry sectors. This architecture must provide not only technical interoperability but also a consistent legal, economic, and organizational framework that facilitates efficient collaboration among stakeholders. Key fragments of this architecture will be defined through various flagship projects and later integrated into a comprehensive basic system architecture via a multi-project approach. Standardization will be a critical component of this architecture, involving the specification of necessary standards, identification of relevant national and international bodies, and coordination of these processes within the Manufacturing-X community.

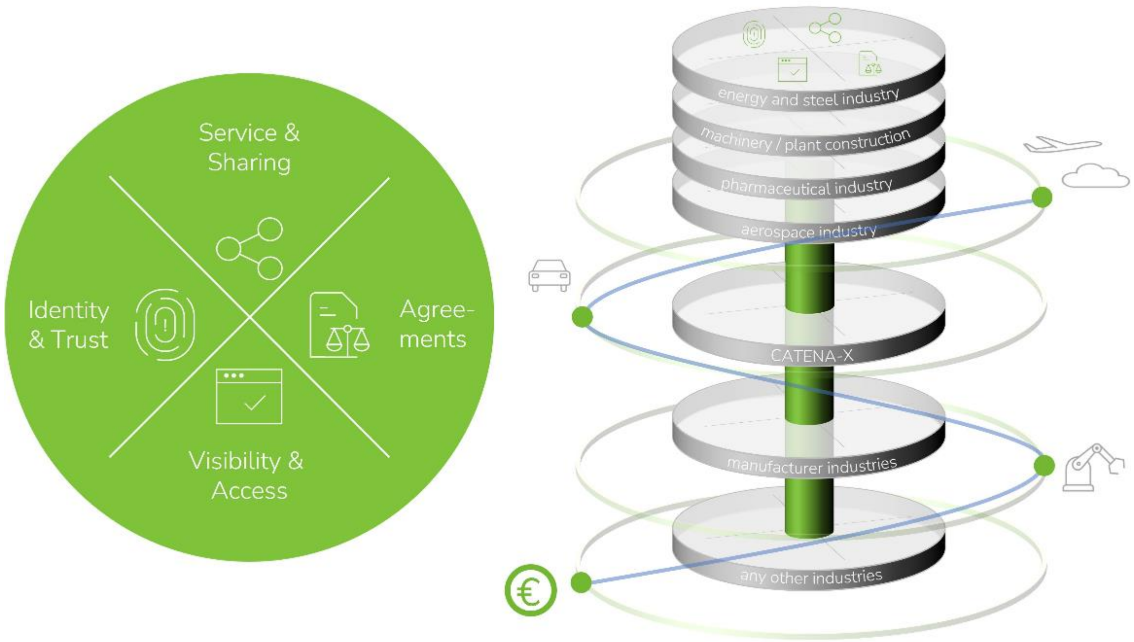

Figure 10. Four core elements to ensure interoperable data sharing between industries (© Plattform Industrie 4.0)

An overarching technical architecture for Manufacturing-X is the key to creating interoperability. To this end, common central elements of the technical and organizational architecture are being developed that guarantee interoperability not only within an industry, but also across industries. The architecture aims at the technical integration of existing and future systems within production Data

Spaces. The requirements for these four core elements, the so-called building blocks, for the industry-specific use cases show certain similarities. Therefore, these four core elements can be developed across industries using a collaborative approach.

- "Identity & Trust" concerns security aspects of data sharing processes. Data is only shared between partners who trust each other and where the sender and recipient can be clearly identified.
- "Visibility & Access" encompasses standardized technologies and mechanisms for multilateral data sharing, for example, through the use of interoperable interfaces, in order to enable a high level of efficiency in the use of shared data.
- "Service & Sharing" includes the provision of central services for the efficient design and implementation of data sharing processes; for example, a uniform registry service is used to search for and find decentralized data sets.
- "Agreements" provides the basis for central services for uniform contract management in the multilateral sharing of data. Among other things, the focus is on establishing legal certainty in multilateral data sharing and on aspects of monetizing data flows.

To advance the Manufacturing-X initiative effectively, parallel efforts are necessary to establish the organizational and coordination structures required for its success. The first step involves leveraging the Plattform Industrie 4.0 network to create a core group of central stakeholders, including representatives from companies, associations, research institutions, and the public sector. This group will serve as the nucleus for forming and leading the Manufacturing-X community. The core group will utilize the established processes and frameworks of Plattform Industrie 4.0 to foster collaborative dialogue and develop robust management structures for Manufacturing-X. These structures will be essential for orchestrating the Manufacturing-X community, ensuring effective coordination among stakeholders, and driving the creation of a Data Space Industrie 4.0. The Steering Committee Manufacturing-X (SC4MX) is the central body in the Industry 4.0 platform for all Manufacturing-X activities. Aiming for bundling and coordinating all activities related to this topic regarding mechanical and plant engineering industry, the VDMA founded the Manufacturing-X Forum.

The Manufacturing-X funding scheme creates the necessary structures for collaboration that would not come about under purely market-driven conditions. It also promotes the transfer of project results to industry at large and supports internationalization. The first projects under the funding framework started at the beginning of 2024 and will run until 2026. Current Manufacturing-X projects include:[41]

- Factory-X
- Aerospace-X
- DAVID
- Decide4ECO
- HealthTrack-X

[41] https://www.bmwk.de/Redaktion/DE/Dossier/manufacturing-x

- Robot-X
- Semiconductor-X
- Scale-MX

In the coming years, the entire value chain will be increasingly integrated and supported by digitalization – from product, production and process design to on-site customer service and a circular economy. No country, initiative or company can achieve this alone. International Manufacturing-X (IMX) will realize a federated, decentralized and collaborative data ecosystem for smart manufacturing to support greater resilience, sustainability and competitiveness. The International Manufacturing-X Council (IMXC) is a joint effort by partners from science, politics and industry to advance the development of IMX. Open collaboration, inclusion, transparency and equal treatment of all partners within this ecosystem are key. The IMXC will jointly define an agenda, decide on a roadmap for implementing aspects and determine responsibilities.

5 The strategy of Data Spaces in the manufacturing sector for interoperability and federation

5.1 Data For Industry-X (D4I-X)

Data4Industry-X is the Data Exchange solution for Industry to improve competitiveness & reduce carbon footprint. DFIX supports:

- A Trusted, secure, compliant and sovereign data exchange environment
- Fostering a competitive and sustainable European industry, also supported by useful data impatriation from all plants across the world
- Innovation and operating services on distributed data
- Consolidation and reporting on CO2 emissions of each shop floor to take their reduction to the next level
- Implementing Gaia-X de facto standard, interfacing with OPC UA protocol, and using Eclipse Dataspace Components
- cross-border, cross-company, cross-factory industrial data exchanges

The D4I-X Data Space will

- Set-up and govern data exchanges in the manufacturing industry, for productivity, competitivity and sovereignty
    - Intra-company for large, multi plants groups
    - Inter-companies for value chain optimization
- Demonstrate in automotive and nuclear sectors, addressing specific manufacturing challenges:
    - End-to-end data privacy and security
    - Scalability, and standardisation of data exchanges
    - Carbon footprint management
    - Readiness for Data Governance Act and Data Act

Initially targeting the automotive and power generation industries, Data4Industry-X is supported by the French government's France 2030 initiative and the European Next Generation program. Leading partners such as Dawex, Schneider Electric, Valeo, CEA, and Prosyst contribute their technological and industrial expertise to develop a solution that complies with European data regulations, including the Data Act and Data Governance Act.

The solution leverages Gaia-X de facto standards to create a trusted, secure, and sovereign data exchange environment. It uses the Eclipse Dataspace Component framework for interoperability between Data Spaces and the UDC (Unified Data Collector) Prosyst solution to retrieve and exchange industrial data via the OPC UA protocol. By enabling cross-border, cross-company, and cross-factory data exchanges, Data4Industry-X plays a determining role in advancing digital transformation and fostering innovation within the industry.

Data4Industry-X also supports new digital business models, such as pay-per-part and remote monitoring, which rely on efficient and secure data exchanges. These models reduce costs, improve service delivery, and ensure manufacturing processes are more responsive to real-time data inputs. The solution is particularly valuable in industries focused on sustainability, as it enables better energy management and CO2 footprint reduction.[42]

DFIX's Approach for interoperability

DFIX's interoperability strategy is based on the objective of removing the main technical and technological limitations to the syndication of distributed data from heterogeneous systems identified through DFIX's work. More specifically, the ambition is to define programmatically applicable syndication, structuring and communication systems, enabling data to be collected and/or processed in a distributed manner, with a view to the interoperability of services between the Edge layer and the federated platform layer.

A generic framework will be defined for structuring data and services in a uniform and consistent way, thereby guaranteeing the interoperability of services in a complete architecture, which will be a distributed environment, between the Edge layer and the federated platform layer for transparent data transfer and contextualisation, implementing Gaia-X de facto standard, interfacing with OPC UA protocol, and using Eclipse Dataspace Components. Finally, this work will be carried out while ensuring that solutions can be deployed and applied programmatically, particularly in terms of data access and usage rights.

5.2 Catena-X

The digital transformation of the automotive industry is significantly reliant on the collaboration of all stakeholders along the automotive value chain. Nevertheless, this vision is complicated, as companies at various phases of the automotive value chain frequently have their own IT systems to manage their data. A common language is required for all participants in order to guarantee that these complicated volumes of data can be sent, received, and processed seamlessly at all stages of the value chain which is based in common standards and frameworks.

With the Catena-X, massive amounts of data may be integrated and exploited collaboratively. The exchange of data and information on the network is regulated by the Catena-X data ecosystem standards. They are the foundation for assuring that the technologies, data, policies, and processes employed are developed and operated in accordance with compliant regulations. The technological and industrial requirements of the automotive industry are the foundation of all standards developed for the Catena-X data ecosystem.

Catena-X signifies a transition towards a future where the automotive industry is increasingly data-driven and interconnected. Catena-X emphasises the importance of responsible, transparent, and

[42] https://www.dawex.com/en/news/data4industry-x-bridging-industrial-data-ecosystems
https://www.dawex.com/en/news/dawex-schneider-electric-valeo-cea-and-prosyst-join-forces-to-create-data4industry-x

sustainable supply chains, which are crucial for managing disruptions that may affect global supply networks. The operating model of Catena-X is aligned with the principles and values of Gaia-X and the International Data Space Association (IDSA) to build the first open and collaborative data ecosystem for the automotive industry. Gaia-X is the foundation for the overall Catena-X trust framework and provides the basis for a federated, interoperable Data Space with trusted identities. Catena-X demonstrates the potential of data sharing guided by the architectural principles of the International Data Spaces Association (IDSA). By adopting an open ecosystem approach, it fosters industry-wide collaboration beyond traditional boundaries. Interoperability and openness are essential components of this transformation, creating a foundation for collaboration that drives innovation and resilience across the automotive sector. Catena-X's commitment to sovereign data sharing is emphasised by the implementation of the Eclipse Connector, which enables organisations to preserve their data sovereignty while participating in a multi-cloud environment. The Eclipse Foundation guarantees that the Catena-X ecosystem benefits from a transparent and collaborative development process by hosting the official open-source development project. The Catena-X Association provides governance for the ecosystem within the automotive industry, representing various stakeholders to address common business needs. Additionally, it establishes the vision, mission, and guiding principles for the Catena-X Data Space through a governance framework based on the Catena-X statutes.

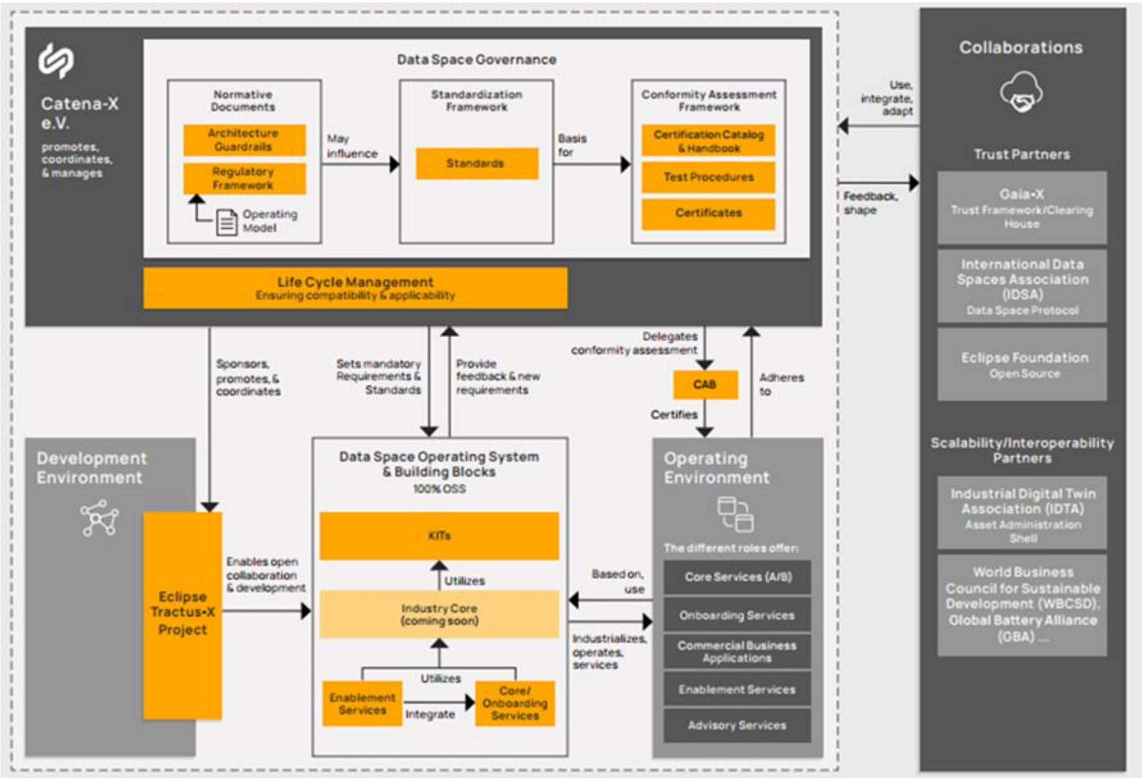

Figure 11. The Catena-X Data Space environment.

The global Catena-X Data Space is built on five mission-critical pillars.

- A dedicated role concept that encompasses all participants in the Data Space. The ecosystem is based on the principle of multiple, distinct roles for the creation of a functional and attractive Data Space.
- A service map of foundational software services, building blocks, and standards that constitute the **Catena-X Operating System** and **Business Foundation**.
- Procedures, processes, and foundational elements for a trusted, scalable, and compliant Data Space operation.
- Effective Data Space governance includes standards, legal frameworks, and certification, along with integrated and holistic lifecycle management to ensure compliance, interoperability, and compatibility.[43]

There are three components of the **Catena-X Operating System**: Core Services, Onboarding, and Enablement. The Enablement Services consist of a collection of decentralized services that facilitate participation in the Catena-X Data Space. To establish a connection to the Data Space and enable standardized interactions tailored to the specific needs of each use case, every participant is required to deploy and utilize the Enablement Services. These services ensure the strategic value proposition of data sovereignty and technical as well as semantic interoperability.

The foundational component of the Enablement Services is the Eclipse Data Space Connector, which is based on the Data Space protocol and the Identity Wallet. The Eclipse Data Space Connector enables each company participating in a data exchange to specify exactly how the data transfer should be organized and provides control over how data is shared and utilized, even across multiple cloud environments. The EDC is compatible with other connectors that also comply with the Data Space protocol, providing a foundation for interoperability. It consolidates all functionalities required for secure data exchange, including data provisioning, discovery, access policy definition and usage policy negotiation This framework ensures compliance with internal specifications and regulations regarding data sovereignty and facilitates the exchange of sovereign data and standardized technical connectivity. Data is exchanged only between partners, with no central data repository. Regardless of the commercial use case, all participants can use these tools to establish a fundamental connection to the Data Space.

In addition to generic data-exchange capabilities, enabling services include context-specific offerings such as the Asset Administration Shell (AAS), the Decentralized Digital Twin Registry (DDTR) and the Item Relationship Service (IRS).

Common accessibility and discoverability functionalities are offered by **Core services** for participants in the Data Space. Examples include Business Partner Number (BPN) issuers for maintaining business partner numbers and participant information, Identity and Access Management (IAM) solutions for managing identity and access, and discovery services for retrieving asset addresses in decentralized registries across the Data Space

[43]Catena-X Operating Model White Paper Released October 16, 2023, Released Version 2.1

The Onboarding Services are administered and executed by OSPs, facilitating participants' access to the Catena-X Data Space. An example of building trust is the adoption of the Gaia-X Digital Clearing House (GXDCH) and its integration into the Catena-X onboarding process. The GXDCH verifies compliance with Gaia-X rules. Gaia-X provides a framework for the verification and description of participants, their resources, and services. This framework enables the creation of verifiable information about participants, resources and services. This is crucial because Catena-X participants exchange business-critical data on a peer-to-peer basis and require assurance regarding the identity of those with whom they share data. Furthermore, Catena-X is one of many industry Data Spaces, and its participants will not only operate within Catena-X. To enable participants to connect with others in different Data Spaces, Catena-X employs the Gaia-X Trust Framework for identity and trust.

CATENA-X KITs, standing for Keep It Together, consolidate all essential resources and technical documentation required for the adoption of a Catena-X use case by all participants in the Data Space. KITs provide software components, standards, policies, and deployment scripts to accelerate the adoption and development of Catena-X use cases. To ensure interoperability and data sovereignty in Catena-X use cases, a minimum set of elements is required. This includes semantic models for data integration and understanding, logic and schemas for value calculation, API implementations for technical communication, and access and usage policies to uphold data sovereignty Standardised semantic models provide essential meaning to data and relationships to enable interoperability. API specifications outline the functional and expected behaviour of an API, including its endpoints, data formats, and interaction rules. Access and Usage Policies regulate the rights and conditions for data access and usage, thereby promoting data sovereignty. In addition to this minimum set, a KIT comprises several other elements.[44]KITs are open to everyone as part of the open-source Eclipse Tractus-X project, which facilitates participation in the design and development of a KIT. A comprehensive overview of the artifacts can be found on the Tractus-X project website.[45] The Tractus-X project adopts the Eclipse Foundation’s development process for using or contributing to the Catena-X operating system, including source code, semantic models, technical documentation, and deployment instructions. KITs have wide applicability and are not limited to the automotive value chain.

The Catena-X Association is actively engaged in every aspect of the Catena-X ecosystem. Its notable activities include publishing standards, providing certificates as part of its conformity assessment, and initiating programs to share knowledge and tools with the automotive industry, particularly targeting small and medium-sized enterprises (SMEs).[46] Furthermore, the Association is committed to operating in compliance with all applicable laws and regulations, recognizing the importance of transparency and accountability in its Data Space operations. To achieve this, it is continuously

[44] KITs 101 “An introduction to Catena-X KITs within the open-source Eclipse Tractus-X project” White Paper Released October 9, 2023, Released Version: 1.0

[45] https://github.com/eclipse-tractusx

[46] Data Space Governance 101 "Overarching principles and technology for a sovereign data space" Released October 9, 2023 Released Version: 1.0

developing a holistic governance framework that outlines the requirements and responsibilities of all stakeholders involved in its activities.[47]

5.2.1 Catena-X approach for interoperability

5.2.1.1 Catena-X Interoperability Framework[48]

Catena-X adopts a holistic approach to ensure compatibility and harmonization across the entire automotive value chain, in accordance with the European Interoperability Framework. This framework categorizes interoperability into four dimensions: technical, semantic, organizational, and legal. This allows participants in the Catena-X Data Space to create additional business value by connecting with partners outside their own network and engaging in multiple Data Spaces without additional technical, organisational or legal constraints.

5.2.1.2 Technical Interoperability

Technical interoperability refers to the compatibility of systems, interfaces, and protocols used for data exchange within the Catena-X Data Space. The minimum requirement for achieving interoperability with Catena-X is the adoption of the IDSA Data Spaces Protocol (DSP) and the Identity and Trust Protocol (IATP). The DSP functions as an industry standard that can be utilized to ensure the technical interoperability of multiple Data Spaces. The IATP defines the interaction between the wallets holding a participant's identification credentials and the connector and is presently being developed in collaboration with the Eclipse Tractus-X group. The EDC connector is responsible for validating the credentials of the parties participating in the data exchange and orchestrating the data exchange based on the defined access and usage policies associated with the data assets stored in the connector. The Tractus-X development environment, supported by the Eclipse Foundation, encourages the creation of interoperable free and open-source software components, such as the EDC fostering innovation and flexibility in system design and implementation.

5.2.1.3 Semantic Interoperability

The Catena-X Ecosystem utilizes semantic models based on the Semantic Aspect Meta Model (SAMM). The Semantic Aspect Meta Model (SAMM) is an open standard, and it is used to define the semantics of the different aspects of an asset represented by a digital twin. Aspect models are machine readable and other artefacts can be derived from them. The aspect model is the common basis for the http/REST API for accessing data via the standardised Digital Twin API of the Asset Administration Shell. Catena-X also employs the internationally adopted Asset Administration Shell (AAS) as one technical implementation. AAS is the standardized digital representation of the asset and corner stone of the interoperability between the applications managing the manufacturing systems. The

[47] https://catena-x.net/en/catena-x-introduce-implement/governance-framework-for-data-space-operations
[48] https://catenax-ev.github.io/docs/operating-model/why-understanding-the-catena-x-data-space#the-catena-x-data-ecosystem-architecture

ASS supports the standard-compliant exchange of data along the entire production life cycle. AAS ensures that different systems and platforms can communicate and understand each other, reducing integration effort and costs. Employing these models is the minimum requirement to achieve semantic interoperability with Catena-X. Within this context, standardization efforts led by the Association, in collaboration with industry partners like the IDTA, aim to establish shared vocabularies, ontologies, and data models specific to automotive domains and use cases.

5.2.1.4 Organizational Interoperability

Organisational interoperability entails the alignment of basic structures, processes and roles between the different stakeholders. The minimum effort required to achieve organisational interoperability with Catena-X involves identifying the Governance framework of Catena-X and its key roles. Utilizing Catena-X Core Service Providers (CSPs) and Onboarding Service Providers (OSPs) enhances access to the Data Space. The Catena-X Association plays a crucial role in fostering collaboration with other initiatives, such as the Gaia-X, the International Data Spaces Association (IDSA), and the Eclipse Data Space Working Group.

5.2.1.5 Legal Interoperability

Catena-X operates within a Regulatory Framework that defines rights, responsibilities and obligations governing the exchange and use of data. The Catena-X Regulatory framework for Data Space operations acts as a guiding foundation on which all Data Space participants can rely to ensure trust, interoperability and scalability. The Regulatory framework for Data Space operations is made up of individual components that each govern a specific level of the Data Space operations. The Data Space level provides the overall framework, the Use Case Level is for specific use cases, the Data Offering Level is for individual data offerings, and the Data Usage Level is for automated contract negotiations.

At the most basic level, contracts should allow for possible add-ons that enable sharing with partners from other Data Spaces, while ensuring that these external partners comply with the Catena-X regulatory framework. In order to allow for a seamless transition between Catena-X and other Data Spaces, compliance with the Catena-X Regulatory framework should be integrated at the Data Space level of those external Data Spaces.

5.3 Manufacturing-X Data Spaces

Current Manufacturing-X projects include:

Factory-X (find a detailed description in the following chapter)
In the lighthouse project “Factory-X”, 47 partners are working together under the leadership of Siemens and SAP. The primary goal is to create an open and collaborative data ecosystem for factory outfitters and operators based on Catena-X and concepts of the Plattform Industrie 4.0. The project aims to implement eleven use cases of the data ecosystem that are particularly relevant for the manufacturing industry. To this end, the following topics in particular will be considered:

- Cross-manufacturer data consistency for engineering, device information and condition monitoring
- Contribution to sustainability through carbon footprint and energy management, as well as digital solutions to support a circular economy
- Provision of digital solutions for "as a service" business models (e.g. marketplace/pay-per-part, remote control/monitoring)
- Traceability of materials, data and products along the entire supply chain
- Update and change management for devices in the field

In addition to the technical development, the consortium also plays an important role in the cross-project coordination of development activities and in building an international Manufacturing-X community.

Aerospace-X

Under the leadership of Airbus, the "Aerospace-X" consortium has been formed by 14 companies and research institutions. The main objectives of this funding project are to establish the digital ecosystem for the aerospace industry, to ensure digital continuity and to enable new forms of collaborative, data-based value creation.

The basic capabilities for cross-company digital collaboration with regard to basic technologies, data infrastructure, software services and regulatory requirements are to be developed on the basis of the production chains for the fuselage, cabin and engine. The focus is on the use cases of demand and capacity management, CO_2 emissions and regulations for the CO_2 footprint, circular economy and collaborative quality management.

Robot-X

Robot-X aims to digitize the product life cycle for robotic systems, connect the players involved and optimize the interaction process. The barriers to entry for small and medium-sized enterprises (SMEs) in robotic systems are often high due to high investment costs and complex development phases. The Robot-X project aims to help lower these barriers and also make it easier for SMEs to access customized robots and automation lines. This is to be made possible by model-based system development (MBSE) and the use of artificial intelligence (AI).

At its core, the project is concerned with building a networked Data Space for the harmonized exchange of digital twins of robotic components to enable data- and model-based system development using AI. The approach pursues an automated configuration of robotic systems based on a modular principle. To this end, different cross-industry application scenarios are being implemented in three use cases. These include the Drone Port – a drone take-off and landing device for use in defense and agriculture. In addition, the project is addressing the topic of industrial packaging for irregularly shaped production parts in industry, as well as composites processing, an autonomous precision grinding system for the aerospace industry.

Semiconductor-X

Semiconductor-X is developing digital twins for the semiconductor industry based on the Gaia-X/Catena-X architecture together with key industry players and research partners. These are designed to digitally map the planning-critical segment of the supply and value chain and are based on a generic software architecture with parameterizable data and reference models. AI-based analysis functions are used to overcome industry-specific challenges such as long production lead times, fluctuating process yields and a high number of variants. Digital twins are developed and networked for different application levels:

- Heterogeneous integration: secure and efficient data exchange between partners in a production chain, particularly when integrating semiconductor chips into complex IC packages
- Resilient network nodes: new digital services and cooperation models for optimizing operations and improving quality in the manufacturing process
- Sustainability assessment: developing methods for determining and optimizing the carbon footprint and energy and water consumption along the value chain

Decide4ECO

The Decide4ECO project is concerned with the consideration and evaluation of sustainability requirements and the achievement of sustainability goals. Since a large part of the resource consumption is already determined in the product planning and development, the project starts at this phase and develops digital solutions for decision support in development and production with regard to sustainability criteria. The evaluation should take into account the entire value chain and the entire product life cycle.

The data on which the sustainability analysis is to be based must be collected across the entire manufacturing and supply chain. The necessary data exchange along supply chains is to be implemented based on common standards in the Manufacturing-X data ecosystem, for which open interfaces and standards are being developed in the project. A standardized digital product passport is to be provided in the common data ecosystem and supplemented with information. The software solutions for assessing sustainability that are based on this should thus consider all relevant upstream and downstream processes and also be supplemented with predictive, AI-based impact analyses.

DAVID

DAVID is a cross-cutting project in the Manufacturing-X environment that ensures digital interoperability based on the Asset Administration Shell (AAS). It contributes to the development of open data ecosystems in industry by providing processes and means to validate the technological and semantic interoperability of MX projects. This enables cross-industry use cases.

The collaborative projects from the funding measure “KoPa 35c Module a2 - Digitization of Vehicle Manufacturers and Suppliers” are also part of the DAVID consideration.

DAVID provides content-related and methodological support for the MX projects, particularly with regard to the use of the AAS. In addition, the project coordinates the use of the AAS within Manufacturing-X, validates intermediate project results and ensures their standardization. Finally, an SME adapter is being developed in the project to make SMEs connectable to the Industrie 4.0 Data Space.

HealthTrack-X

Health Track-X aims to build an open and decentralized data ecosystem for the healthcare sector. All stakeholders should be able to maintain data sovereignty more easily, thus creating trust and increasing efficiency. The use of this data ecosystem should promote digital collaboration between stakeholders, thereby improving healthcare in Germany and Europe.

The development of architectural components and enabling technologies for the data ecosystem will be based on the results of Catena-X and closely coordinated with other Manufacturing-X funding projects. The solutions developed will be based on the Gaia-X principles for the sovereign and secure exchange of data.

The project aims to develop concepts and standards for a unified master data management system that allows physical goods and their paths along the supply chain to be digitally recorded and tracked. HealthTrack-X focuses on three use cases:

- Simplifying business processes by automatically providing digital documentation to accompany goods shipments.
- Common standards for carbon footprinting should enable a sustainability assessment of products along their supply chain and create incentives for sustainable business models.
- The digitally connected supply chain should also enable the early prediction of supply bottlenecks.

After the project is completed, the prototypical data ecosystem will be made available to all stakeholders for participation in the tested use cases and for implementing their own digital business models.

Scale-MX

With Scale-MX, Manufacturing-X Data Spaces have their own transfer initiative. The goal of the project is to gather learnings & experiences from all Manufacturing-X projects and to transfer the knowhow gained within the projects to the communities outside.

In the context of SM4RTENANCE, Scale-MX can be a anchor for information regarding Manufacturing-X.

5.4 Factory-X

Factory-X is a public funded and a lighthouse project in the context of the Manufacturing-X program. Spearheaded by Siemens and SAP it is aiming to create an open and collaborative data ecosystem for the manufacturing sector. Launched on February 1, 2024, and set to conclude by June 2026, Factory-X involves a consortium of 47 partners, including companies, associations, and research institutions, with an additional 10 associated partners. Building upon the principles of Catena-X and Platform Industrie 4.0, Factory-X focuses on creating a collaborative environment that enhances both horizontal and vertical integration within the manufacturing supply chain. The project focuses on 11 dedicated use cases that aim to enhance and integrate both horizontal and vertical aspects of the supply chain within industrial operations. These use cases are designed to extend the existing supply chain-oriented solutions by adding vertical integration, which directly connects and optimizes shop floor operations. Each use case is centred around specific business applications, which are carefully conceptualized, prototypically developed, and validated to ensure they address the unique needs of the manufacturing environment. To this end, the following topics in particular will be considered:

- Cross-manufacturer data consistency for engineering, device information and condition monitoring
- Contribution to sustainability through carbon footprint and energy management, as well as digital solutions to support a circular economy
- Provision of digital solutions for “as a service” business models (e.g. marketplace/pay-per-part, remote control/monitoring)
- Traceability of materials, data and products along the entire supply chain
- Update and change management for devices in the field

This holistic approach enables a seamless integration of processes across different levels of production, from supply chain management to on-the-ground operations, ultimately driving efficiency and innovation in industrial settings. All approaches and solutions developed in Factory-X will be based on existing open standards and concepts such as OPC UA, EDC, AAS etc., where possible and appropriate, to enable technical interoperability in a cross-industry, open data ecosystem. A key concern is to maintain interoperability between emerging domain-specific Data Spaces, as participants of a data ecosystem can also be from other industrial sectors, which is why Standardization is a key.[49][50]

One main technical challenge of the project is facing is the integration of IT (Information Technology) and OT (Operational Technology), which is crucial for improving efficiency and modernizing operations and faces several challenges. Cultural differences between IT and OT teams, with IT focusing on data management and cybersecurity, and OT prioritizing reliability and safety, require alignment of goals. Security is a major concern as OT systems were not originally designed with cybersecurity in mind, making them vulnerable when integrated with IT networks. Different technologies and protocols used by IT and OT, such as TCP/IP for IT and proprietary protocols like Modbus for OT, complicate interoperability and data sharing. Legacy OT systems, often decades old, pose additional challenges due to the need for costly and disruptive updates or replacements.

Standardized technology can address these issues by providing consistent frameworks and protocols. Interoperability standards like OPC UA and AAS facilitate seamless communication between IT and OT systems. Cybersecurity frameworks such as ISA/IEC 62443 offer structured protection for both environments. Standardized platforms and tools also enhance scalability and efficiency, reducing the need for custom integration work. By adopting these standards, organizations can bridge the IT-OT divide, ensuring smoother integration and improved overall performance and security.

[49] https://factory-x.org/projects/
[50] https://www.bmwk.de/Redaktion/DE/Dossier/Manufacturing-x/Module/projekt-factory-x.html

Therefore the Factory-X project approach is a standardized vertical integration (intra-shopfloor) and horizontal integration (e.g. IEC, Catena-X) to enhance technical capabilities and commercial offerings. Using the installed base unchanged protects investments and IP. The Factory-X integration architecture defines a finite and well-defined set of architectural building blocks that enable the integration of industrial applications without having to change their interfaces and/or information structures. An application may require an adapter to connect to the FX port. In addition, it supports the discovery of industrial applications according to defined criteria and their application-oriented composition according to business purposes. Integration Architecture provides a set of shared services with standardizes Interfaces.

The FX Port is a concept to enable interactions of business applications in a uniform way. Therefore it provides the necessary transformations e.g. of time, location and function as services with standardized interfaces.

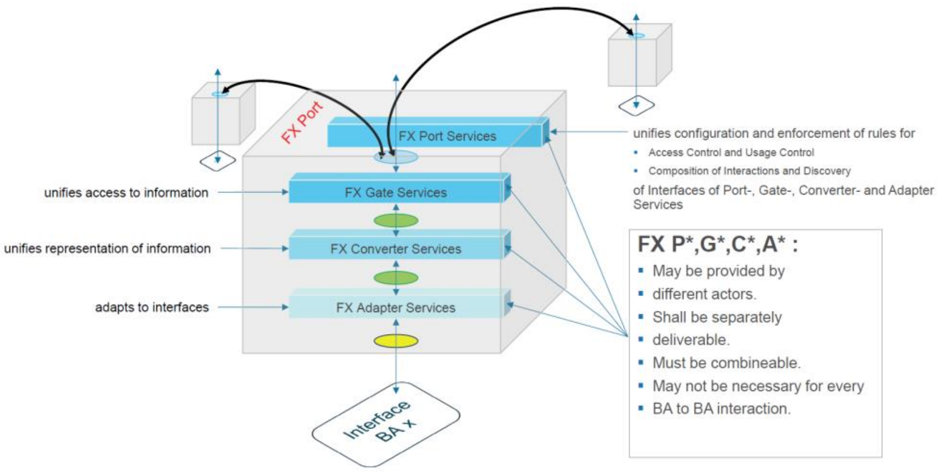

Figure 12. FX-Port generic concept for vertical and horizontal integration.

FX Services offered by the FX-Port are the following:

- FX Adapter Services adapt to the interfaces of Business Applications. If the required information for a use case is accessible through such an interface, the Business Application does not need to be modified.
- FX Converter Services converts and unifies the information representation to be understood by different FX applications. The information model of a FX application is transformed into a common information model agreed upon by FX Applications and also the other way around.
- FX Gate Services provide the necessary interfaces and related operations to standardize access to information.
- FX Port Services unify configuration and enforcement of rules for access control and usage control and for composition of interactions and discovery of interfaces of Port-, Gate-, Converter and Adapter Services.

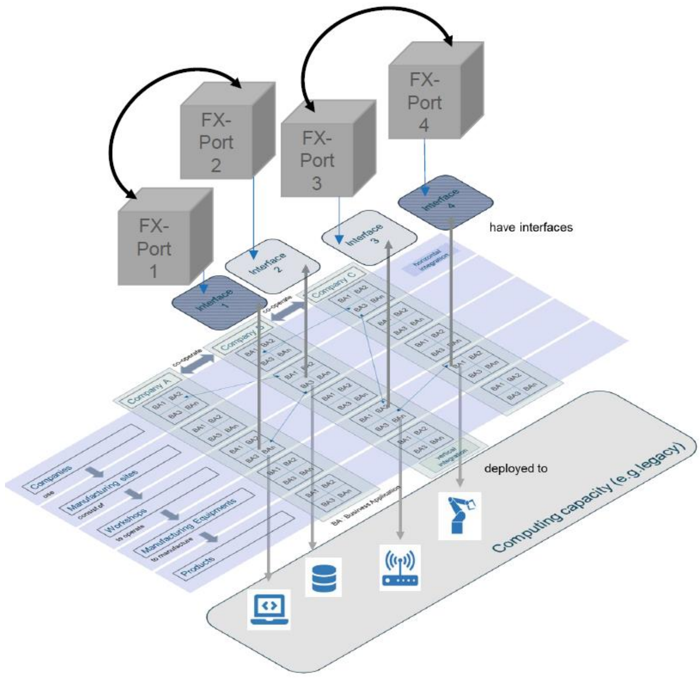

Figure 13. FX-Port as a concept to enable interactions of industrial applications in a uniform way.

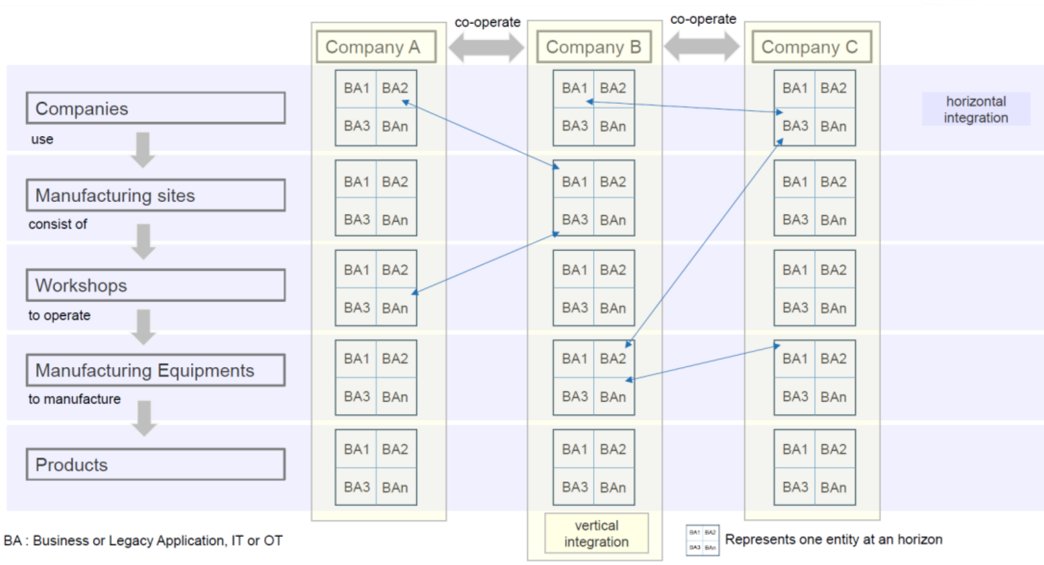

Figure 14. FX – generic view to vertical and horizontal integration.

The FX integration architecture will provide a set of shared services with standardized interfaces of FX-Ports.

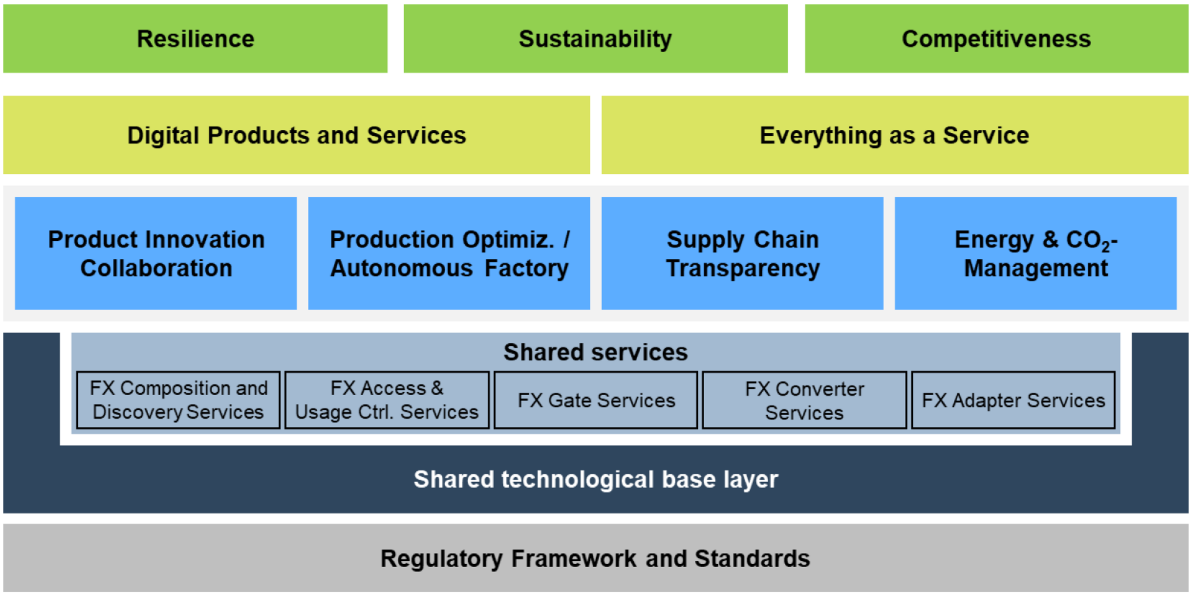

Figure 15. The Manufacturing-X holistic approach with set of shared services from the Factory-X project.

In addition to the technical development, the consortium also plays an important role in the cross-project coordination of development activities and in building an international Manufacturing-X community.

5.5 The Smart Connected Supplier Network (SCSN)

The Smart Connected Supplier Network (SCSN) is an ecosystem that has developed a standard for trustworthy information sharing, based on semantic technology to operate an open supply chain network, thereby ensuring optimal interoperability between the supply chain partners for the most prominent information streams. SCSN builds on the International Data Spaces (IDS) standard, which is a European standard for data sharing, enabling data sovereignty developed by the partners of the International Data Spaces Association (IDSA).

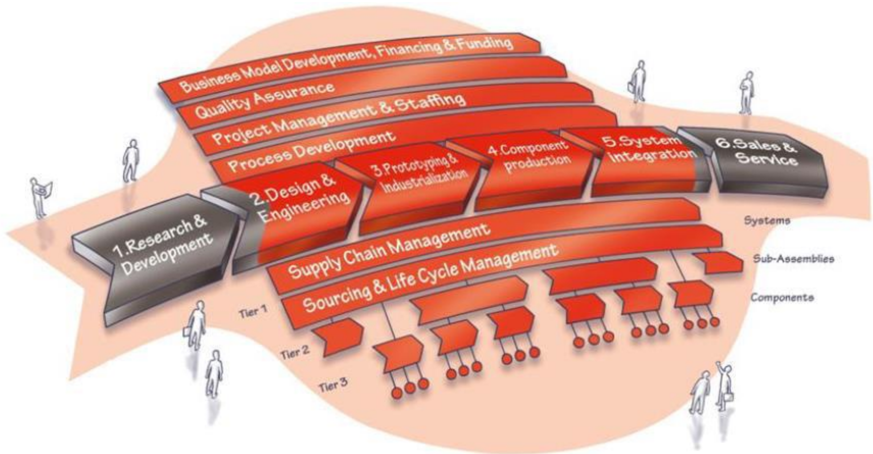

Figure 16. Open Supply Chain Network Scenario.

SCSN and IDS bring a “connect-once -reach the entire supply chain scenario” to manufacturing enterprises, different from traditional bilateral EDI connections or the use of centralized (cloud) platforms. SCSN simplifies data sharing in the supply chain by automatically generating SCSN-messages, directly into manufacturer's own ERP-systems. Given the strict agreements about the semantics of the messages, there can be no misunderstanding as all messages can only be interpreted one way. The semantic standard has been developed for the following prominent information streams:

- Invoices,
- Production schedules/planning,
- Orders;
- Logistic data;
- Certificates;
- Product specifications including 3D drawings;

Currently in development are the information streams below:

- Product measurement data,
- Asset Administration Shells,
- Digital Product Passports,
- Carbon Footprint Emissions Data,
- Service Orders (in the SM4RTENANCE project)

The three types of supply chain partners affiliated with the Smart Connected Supplier Network include:

- Manufacturing companies,
- Software companies offering ERP-systems,
- ICT Service Providers (intermediaries) who make the link with the SCSN network, and between the ERP systems.

To connect to the SCSN Network, manufacturing companies need to establish a single connection with one of the ICT Service Providers. This is usually done with the ERP system of the manufacturing company, using the SCSN semantic specification and/or translators for the specific ERP system. The ICT Service Providers communicate with each other using the SCSN semantics and the IDS technical standard, which enables each supply chain partner to continue using their own ERP system and their own ICT Service Provider. Since all ICT Service Providers involved in SCSN are interconnected, a manufacturing company can do business with any other manufacturing company, even when the other partner uses a different ICT Service Provider. There is no need to connect to every SCSN-connected organization separately. More importantly, manufacturing companies using SCSN, remain the owner of their data and decide autonomously which data will be shared with which connected enterprise in the network.

The infrastructure of SCSN is based on the International Data Spaces Reference Architecture Model 3.0 (IDS-RAM3) and adopts the four-corner model, generating the following functionalities om its foundation:

- Address Book based on the IDS Broker and Parls in order to publish and find the connected manufacturing companies.
- Identity Manager and DAPS in order to ensure trusted identities of all participants.
- The Service Providers facilitate end-user connectivity:
- Each service provider has a Hybrid IDS Connector to interconnect the end-users.
- The service providers integrate the connector with the end-users' IT systems such as ERP systems.

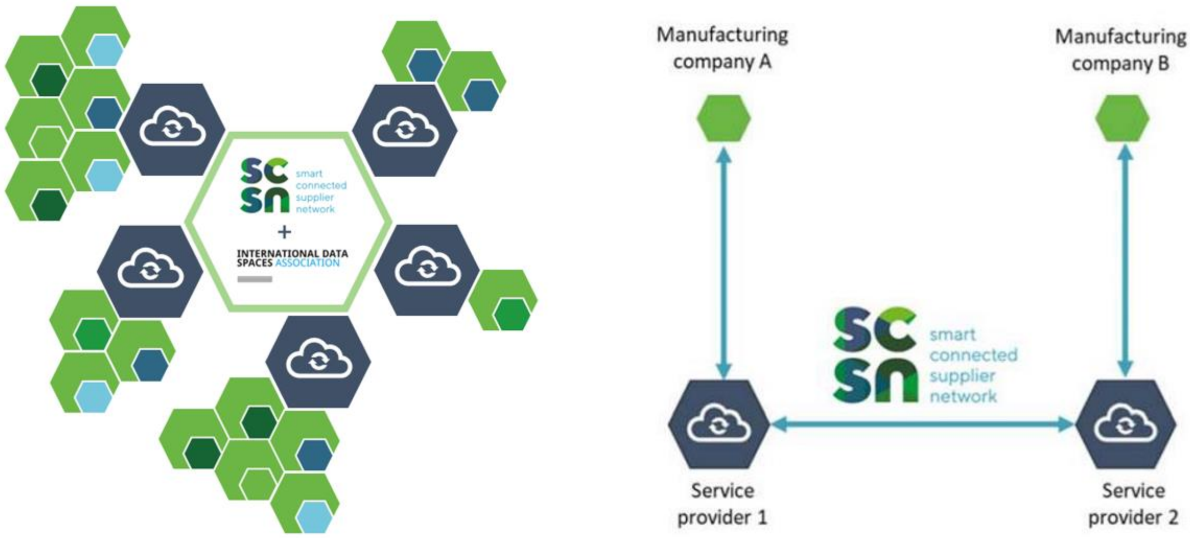

Figure 17. SCSN Open Supply Network 4 Corner Model.

This approach enables easier implementation for supply chain collaboration, as well as scaling it, enabling manufacturing companies to reduce the administrative burden, and helps them prevent errors. Furthermore, SCSN enables agility of the entire supply chain and a more successful risk management. This results in a reduced the time-to-market and time-to-money for manufacturing companies and suppliers, enabling them to respond quicker to changing market demands.
In order to continuously host, improve and maintain the SCSN standard, an increasing number of functionalities will be added over time, such as Product Carbon Footprint and Service Orders, based on market demands of the high-tech manufacturing industry.

5.6 Other Data Spaces initiatives

5.6.1 EuProGigant

The EuProGigant (European Production GigaNet) project, is implementing a common data infrastructure for the manufacturing industry in accordance with the principles of Gaia-X. The initiative aims to demonstrate the economic and technological advantages of Gaia-X's open, European multi-cloud infrastructure.[51]

[51] https://euprogigant.com/en/project/euprogigant-and-gaia-x/

The EuProGigant aims to create a location-independent, digitally connected production ecosystem, driven by the vision of a smart, resilient, and sustainable European manufacturing industry. EuProGigant develops an infrastructure and data ecosystem that complies to the principles and functionalities of Gaia-X, allowing businesses to exchange data and services securely and reliably and utilising an open edge-to-cloud architecture. This framework enables enterprises to establish connections for the provision of data and digital services while ensuring compliance with the principles of data sovereignty, personal data protection, and IT security. Industry partners will integrate the essential functionalities of Gaia-X into their digital products and services, facilitating interoperable usage across edge, on-premises, and cloud-based environments. Key functions include self-sovereign identity management, which governs the authentication and authorisation rights of users/devices and APIs for the organisational credential manager to adopt the Gaia-X Federation Services. These APIs enable comprehensive management of tenant credentials, optimising the processes of issuing, holding and verifying digital credentials. Additionally, there is a portal for browsing data and service offerings, a data exchange connector that enables self-sovereign controlled access to information and services, and Gaia-X Self-Descriptions that serve as graph-based descriptors for the interoperability of resources.[52]
As a result of the Gaia-X principles, a neutral virtual economic space is being established, facilitating the dissemination of intelligent services and supporting the European Commission's climate policy objectives and the Green Deal goals.

5.6.2 FLEX4RES

FLEX4RES offers an open framework designed to facilitate the reconfiguration of production networks, thereby supporting resilient value chains. It utilizes the Asset Administration Shell (AAS) to implement in-factory reconfiguration practices and incorporates a manufacturing platform based on state-of-the-art Gaia-X and IDS technologies to enable horizontal supply chain data exchange. This capability allows factories to swiftly adapt their operations in response to new requirements or challenges. A key concept in FLEX4RES is the Digital Twin, which serves as a virtual representation of the manufacturing network. This technology is essential for the planning and execution of reconfiguration processes in highly adaptable production systems and networks. The Digital Twin enables visualization and testing of modifications before they are implemented in real-world scenarios. A critical component of this framework is the integration of Self-Descriptions with linked, standardised information models, which promotes a consistent and transparent understanding of data across various systems.

[52] M.Weber , M.Weigold, T.Koch, “ The European Production Giganet – Towards a Green and Digital Manufacturing Ecosystem” In: Bleicher, F. (hg) (2022), "Smart and Networked Manufacturing", Wiener Produktionstechnik Kongress 2022, Band 5, 95-100. Wien: New Academic Press.

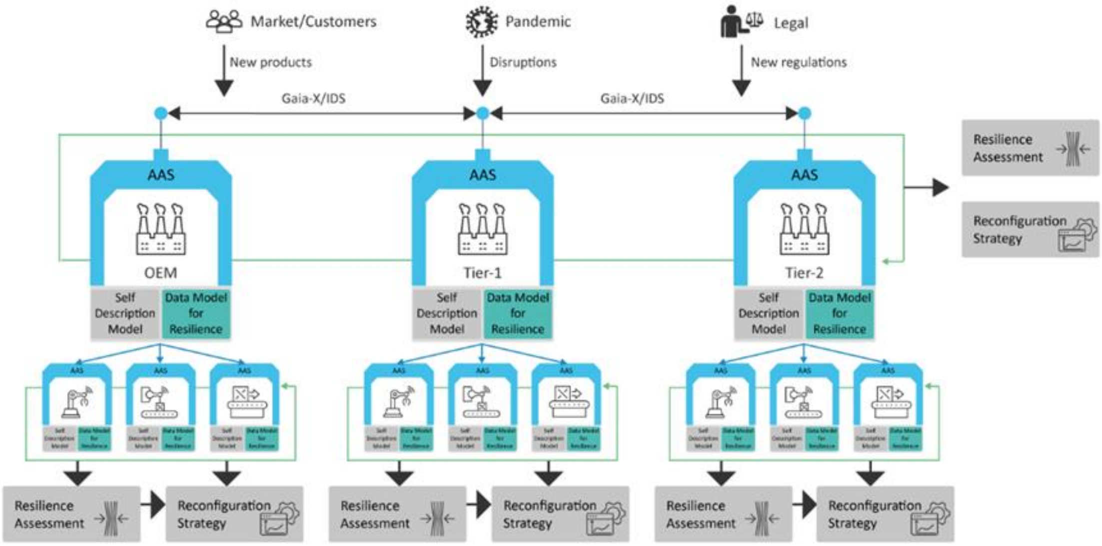

Figure 18. The Flex4RES concept.

As illustrated in Figure 18, an Asset Administration Shell (AAS) middleware platform is implemented at each Original Equipment Manufacturer (OEM) or tier-n supplier's site. The AAS middleware manages digital twin (DT) data in accordance with the AAS standard. This middleware software provides an Application Programming Interface (API) for accessing the properties, services, and events of AAS instances. To facilitate the exchange and sharing of information within a Data Space, it is essential to establish the appropriate IDS or Gaia-X connections through the components outlined in the Data Space reference architecture. A trusted application serves as a proxy to access the digital twin (DT) data stored in the Asset Administration Shell (AAS) middleware. Since the connector (e.g., an IDS connector) is designed to interpret specific messages, dedicated data applications are required to communicate with the DT information stored in AAS platforms. The connectors among original equipment manufacturers (OEMs) or suppliers utilize the IDS/Gaia-X infrastructure to exchange DT data with one another, as well as with resilience and reconfiguration services. Similarly, both services are provided through the Data Spaces infrastructure to enable the secure use of industrial data by service providers.

5.6.3 SIMPL

SIMPL is an open-source smart middleware platform designed to facilitate cloud-to-edge federations and support all major data initiatives funded by the European Commission. The Smart Middleware Platform will federate data, software, and infrastructure across the European Union, providing secure, resilient, energy-efficient, and accessible cloud-to-edge capabilities. It will enable EU stakeholders to collaborate and pool resources, thereby creating greater business value, enhancing resource utilization efficiency, and reducing costs and duplication of efforts. By leveraging the features offered by the Smart Middleware Platform, an open marketplace for EU resources will be established, facilitating the energy-efficient reuse of efforts achieved by other EU participants.

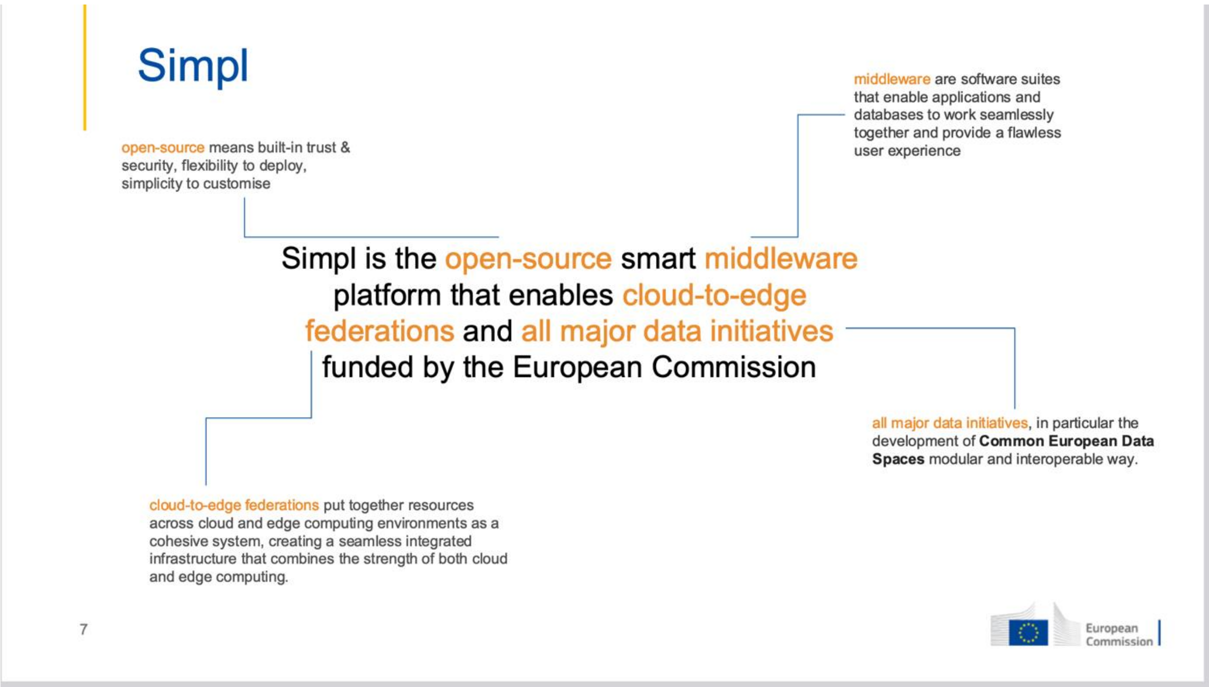

Figure 19. SIMPL key stakeholders' workshops, Brussels, July 4th, 2024.

The Smart Middleware Platform requires some centralised services within Data Spaces to support specific capabilities. However, it is important to note that these centralized services are assigned minimal responsibilities, as the primary objective of the Smart Middleware Platform is to achieve maximum decentralization.

Three types of centralized components were identified to support the distributed functionalities of the Smart Middleware Platform

Data, Infrastructure and application catalogues provide a cataloguing service that enables end users to discover shared services within the Data Space.

Vocabulary providers offer definitions for metadata representation, vocabularies, and ontologies.

Identity authorities manage the identities of participants in the Data Space and provide proofs that other participants can use for authentication and authorization.

The implementation of SIMPL assets is not yet possible. 2025 will see the acceleration of the developments and the first POCs. For being able to use mature and tested components, SM4RTENANCE will need to wait until 2026/2027, according to the planning shared by SIMPL. As the focus of SIMPL will not be on manufacturing, we should carefully assess the relevance of SIMPL assets with the specificities of the domain before implementing them.

The objective of SM4RTENANCE will thus be to build an architecture open enough, align with the EU standards and principles, to be ready for future implementation of SIMPL components.

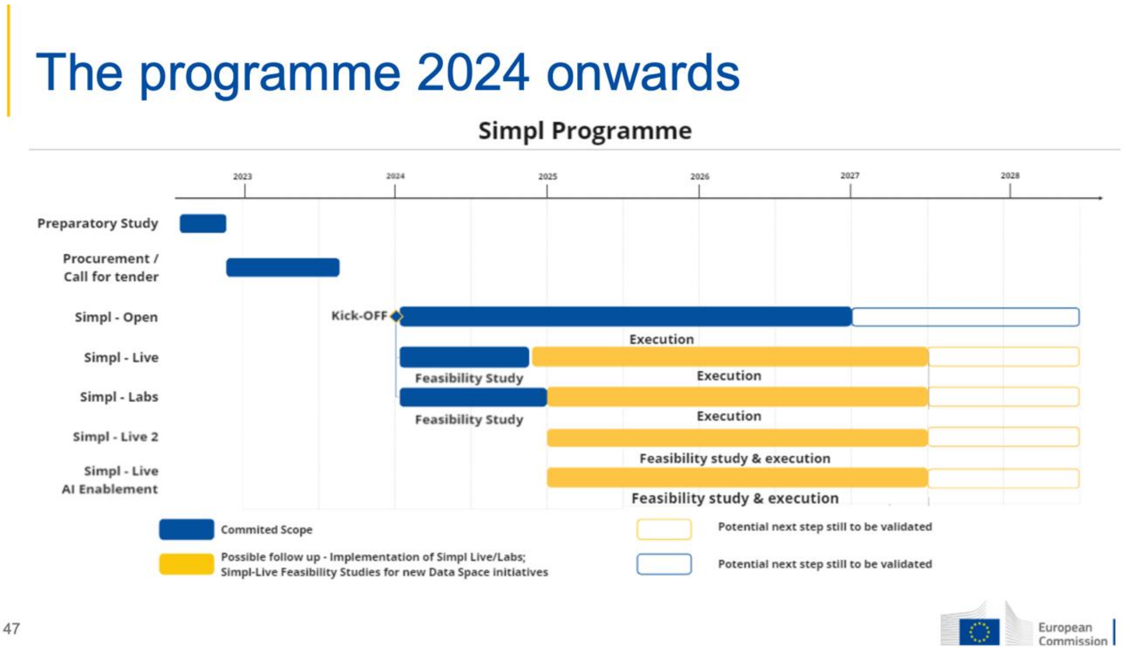

Figure 20. SIMPL key stakeholders' workshops, Brussels, July 4th, 2024.

5.7 The path to harmonisation: the limits of current models

The key problem is that these Data Spaces are designed on architectures that have to coexist with existing systems. The main question concerns the ability to enable simple communication between these different systems, even though they are built by separate organization, sometimes with competitive interests.

Data spaces are secure, controlled virtual spaces for sharing data between multiple organisations, large and small. These exchanges are governed by digital contracts governing the rights and limits of sharing. A Data Space has a purpose (marketplace, industrial data exchanges, data sharing within a large ecosystem), a theme that provides the DNA, the primary reason for public and private players to sit around the table to find solutions to issues that require the collaboration of many players to be addressed. The technology underlying Data Spaces incorporates governance, regulation and data transaction management tools right from the design stage. In this way, they guarantee participants complete transparency over the rights granted for the use of the data. It is the data provider who imposes the rules. There will also be a catalogue of available information that can be consulted by all parties. Finally, information will be transmitted electronically in just a few steps. A Data Space has a set of specifications to facilitate interoperability for data sharing, covering data publication, contract negotiation and access to data within the Data Space. However, here again, exchanging data will require it to be described and detailed (here we are talking about data ontology) so that everyone can use it. Without this, the integration of systems will once again be largely specific, even if these pieces of code will be common in a connector, and therefore a source of additional costs in creation and maintenance in operational condition. Interoperability is therefore also a requirement. Of course it can work without it, but you must expect the costs of reprocessing the data to adapt it.

Data spaces are therefore innovative and modern tools for organising and regulating the participation of economic agents around information sharing, with the aim of addressing complex issues such as climate, transport, agriculture, etc. But the interoperability of data in its semantics, so that everyone can understand it with the same reference system, is key to the future of territorial Data Spaces. Furthermore, the effort required to comply will be all the less significant if standardisation is implemented as soon as data is collected on data platforms. The latter will thus expose catalogues of data already correctly formatted to the Data Space.

Given the considerations on the different levels of interoperability required, it is possible to distinguish 2 archetypal options for building an interoperable ecosystem between data platforms:
A fundamentally decentralised approach. In this approach, the technical data exchange services are managed locally by each participant (e.g. by implementing specific decentralised connectors), and support the elements of technical interoperability, a subset of organisational interoperability (identity verification), and legal interoperability (management of the contractual transaction). The advantage of this approach is that it is based on technologies that can be open source and gives participants considerable freedom in the implementation and management of data exchange services. The difficulty lies in the fact that federated services must be developed specifically to ensure syntactic, semantic and political interoperability, as well as some organisational interoperability (development of a federated catalogue). It should be noted that this approach can be long and costly (if not impossible for small companies), that compatibility between locally implemented services is not guaranteed, and that governance management can be extremely complex.
A fundamentally federated approach, based around common technological platforms that ensure all levels of interoperability. Under this approach, all the services described above are offered to participants, which reduces the effort required to enrol them. The other advantage is that operational European data exchange technologies already exist and are available within the SM4RTENANCE consortium (e.g. SQS, Dawex, Sovity, etc), and cover many of the levels of interoperability described above. However, true interoperability cannot be built around a single technology, as this would lead to a 'vendor lock-in' and severely limit the autonomy of territories.

Within this framework, an intermediate path may be considered, based first and foremost on a 'federated' approach (common services platform), but favouring technological diversity so that the territories and participants have sufficient autonomy in implementation.
Under this approach, the challenge would be to identify and select data exchange solutions to create a catalogue from which local authorities could choose. These solutions will have to meet the following conditions

- Be operational
- Implement Gaia-X principles and Trusted Data Transaction standards
- Cover as many levels of interoperability as possible, as described above.

In addition, for these solutions to be interoperable with each other (e.g. if A has chosen solution X and B solution Y), a certain number of conditions will have to be met:

- Shared or compatible taxonomies and metadata structures for describing products and services
- Shared or compatible contractual management metadata structures

Eventually, creation of a service 'meta-platform' (*SM4RTENANCE Portal*) to ensure these compatibilities. This meta-platform would house the federated catalogue of products and services published by the Data Spaces, the repositories for the metadata structure and taxonomies, and potentially the services enabling transformations from one structure to another.

6 Governance principles for Data Space federation and harmonization

The European Union (EU) has produced a confidence-building framework for the development of a data economy by defining a European Data Strategy, based on a series of regulations (Data-Act, IA-ACT, Data Governance Act, etc.). One of the aims of this European strategy is to pool data through interoperable 'Common Data Spaces' (CDS) (Data Governance Act of 30 May 2022). It defines a set of harmonised basic conditions, with the aim of strengthening trust and boosting the availability and re-use of data - the 'FAIR' principles - with a high level of cybersecurity. The philosophy behind this strategy is that when there is a level playing field in the data economy, companies compete on the quality of services, not the quantity of data they control. So the question is: how can we ensure that the data architectures being built, which also have to coexist with existing systems already deployed by organizations, will be compatible with each other? How can we aspire to simple communication between these different systems when they are being developed by separate private players? Is it possible to reach a consensus when the innate competition between private players drives them to create closed solutions designed to protect their economic interests?

6.1 TRIALS Data Space Governance principles requirements

This chapter focuses on gathering the requirements for the governance structure of trials participating in SM4RTENANCE, addressing both the development and operational environments, as well as processes for decision-making and standardization within the Data Spaces. The governance framework will be established in WP6 to support the legal, operational, and technical requirements outlined in previous tasks and ensure effective data sharing and collaboration.
The objective of this deliverable is to gather and define the key requirements for the governance of Data Spaces used by the trials[53]. A Data Space Governance Framework is defined in the Data Space Support Centre (DSSC hereinafter) Glossary as "*the structured set of principles, processes, and practices that guide and regulate the governance, management and operations within a Data Space to ensure effective and responsible leadership, control, and oversight. It defines the functionalities the Data Space provides and the associated Data Space roles, including the Data Space governance authority and participants*". In order to determine the requirements for a governance framework that is fit for purpose in the Sm4rtenance context, not only legal mechanisms, but also technical and organisational mechanisms are taken into account. Specifically, the legal framework governing Data Spaces necessitates the following:

1. **Legal and Organizational Agreements**: This includes both bilateral and multilateral agreements, as well as comprehensive policy documents and procedures.

[53] Data Space governance is distinct from Data governance. In this document we focus on Data Space governance. For more information on this distinction see the DSSC blueprint 1.5.

2. **Technical Infrastructure**: This infrastructure must inherently implement these agreements and policies to the greatest extent possible. A critical component of this requirement is the use of 'automated' contracts.

Specifically, this chapter identifies the governance principles and mechanisms that are considered important by the participants in the trials for managing data at both the individual organization level and within the Data Space.

Methods

The results noted in this chapter are based on desk-research of the relevant legal documents for Data Spaces[54], and thereafter seven semi-structured interviews with key stakeholders from the participating trials. For this study, we interviewed 7 respondents, 6 of which are members of Trials participating in the SM4RTENANCE project and 2 of which are technical Data Space providers (one entity overlaps). Analysis of the interviews reveals the commonalities and variations in the requirements of stakeholders and relates these to the relevant legal document. The questionnaire for these interviews was designed taking into account existing literature and knowledge on digital governance and Data Spaces[55]. These interviews provided a flexible framework for capturing a broad range of insights while allowing for the in-depth exploration of specific governance-related challenges and needs.

Limitations

However, the scope of this study is subject to certain limitations. The limited sample of key stakeholders of the trials means the findings may reflect the specific perspectives of interview participants. Additionally, the evolving nature of Data Spaces and related regulations presents ongoing challenges for governance design. This is, furthermore, the first iteration of this study, limited by the time and resources available.

6.1.1 Review of Data Space Governance

An initial assessment was conducted to determine the type of legal documents and legal, technical, and organizational mechanisms that should be provided for by each Data Space to govern the interactions between an organization and a Data Space. Building on the SITRA rulebook and Catena-X, a set of documents was identified that contribute to the legal framework of Data Spaces, and a review of the literature on data governance was used to identify the necessary mechanisms thereof. This list is intended to be illustrative, not exhaustive, of what legal documents are expected to be implemented by the trials, acknowledging that these may be categorized differently or expanded upon by the Trials. To enable a Data Space to participate on a Data Space federation level, agreements can be made between Data Spaces. This requires one additional document that expands on aspects such as cost balancing, shared services, et cetera.

[54] Based on the Catena-X documentation and SITRA rulebook
[55] Based on DSSC, SITRA rulebook, Catena-X documentation, Sm4rtenance trial handbook

Table 4. List of legal documents that govern the interactions between an organization and a Data Space.

Documents part of the Data Space rulebook	Description	Use
Constitutive Agreement	Document signed before the start of operations that establishes the operating organization	Signed once by founders of Data Space
Accession agreement	A document for Data Space participants that outlines their intention to onboard the Data Space	Apply with
Exit Agreement	A document for Data Space participants that allow offboarding of the Data Space	Exit with
General Terms and Conditions	Legally binding terms that govern the general function of the Data Space. Will hold references to all other documents	Accept explicitly
Code of conduct	The norms and best practises that are agreed to be applied by Data Space participants and operators	Accept explicitly
Governance Model	Data Space-specific description of the rules and **procedures,** applicable decision-making mechanisms, and further governance provisions regarding the administration of the Data Space.	Understand + accept implicitly
Use-case terms of use	Legally binding terms that govern the access to, among others, dataset(s) regarding the use case. A use case is defined by the Data Space Support Centre (DSSC) Glossary as *"a specific setting in which two or more participants use a Data Space to create value (business, societal or environmental) from data sharing."*	Accept explicitly
Data Product Contract	Legally binding terms that govern the access and use of specific dataset(s). Defined by a data provider	Accept explicitly

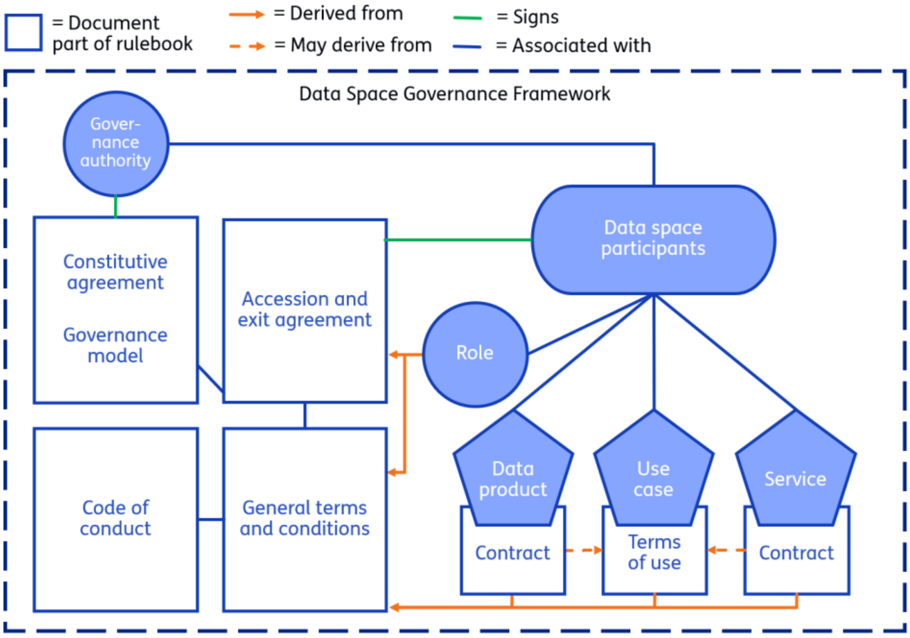

Figure 21. Data Space Governance Framework – Illustrative overview.

In addition to the legal documents that are part of the Data Space rulebook, the kind of content for each document can be specified further. To determine the requirements for the governance of Data Spaces in SM4RTENANCE, we make clear which kinds of choices have to be made in order to shape the governance documents outlined above. We draw from the work of Abraham et al. (2019) on governance mechanisms to structure our findings.[56]

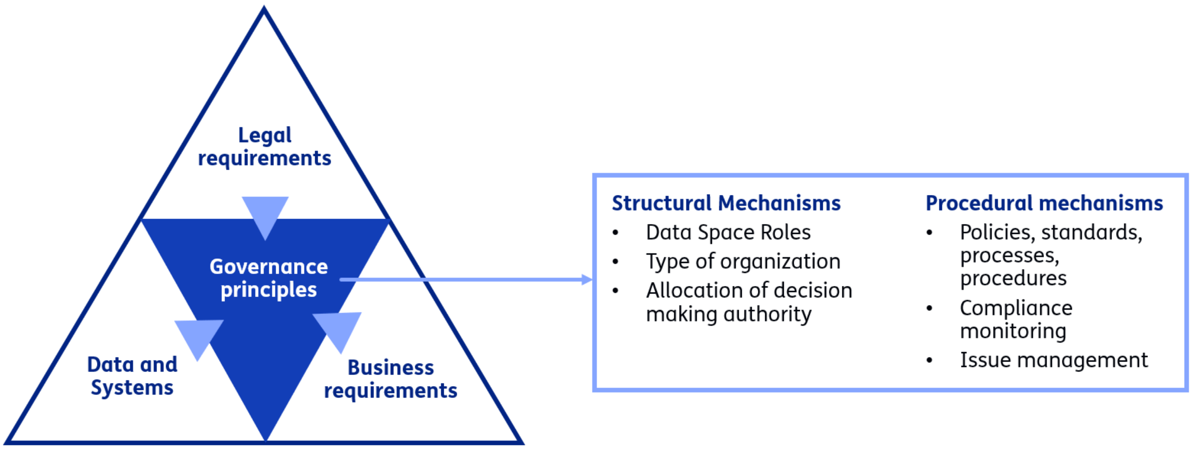

Figure 22. Conceptual Framework for Governance (modified from Abraham et al., 2019, p. 429). .

As seen in Figure 22, governance principles are derived from a combination of Legal requirements (the legal obligations and rules that are expected to be taken into account), Data and Systems (the degree to which data and systems are expected to be of use to facilitate governance), and Business

[56] Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International journal of information management, 49,* 424-438.

requirements (aspects related to governance that are considered key for the organizations subjected to the governance).

The governance principles feed into governance mechanisms, which are split into two categories:

1. Structural mechanisms
2. Procedural mechanisms

Structural mechanisms concern choices such as the inclusion of the kinds of roles and responsibilities of participants in the Data Space. The what, who, and how of decision making in a Data Space depends on factors such as the type of organization (e.g. profit vs. non-profit) and the degree of centralization of the decision making power.

Procedural mechanisms address choices about data policies, standards, processes, procedures, contractual agreements, performance measurement, compliance monitoring, and issue management.
Although none of these mechanisms appear particularly dependent on digital technology, a key objective of the requirements gathering is to elucidate the role of technological components as part of each of the governance mechanisms.

6.1.2 Governance principles and mechanisms

Based on the interviews, we first elaborate on the governance principles that are to be taken into account during the creation of the governance of the Data Space (6.1.2.1). Each of these influences and can be implemented by the structural and procedural mechanisms discussed in the sub-section thereafter (6.1.3).

6.1.2.1 Governance principles – general principles

Continuity: Establish a governance framework that maintains long-term sustainability and reliability of Data Spaces, including persistent policies and oversight mechanisms. This includes a requirement to consider changes in the role of Data Space Authority and/or Data Space Operator.
Transparency: Implement open and clear governance practices where policies and decisions are communicated effectively to all stakeholders.
Neutrality: Ensure the governance framework does not favour any specific data provider, promoting fairness and inclusivity.
Competition and collaboration: Foster a competitive environment where data providers and consumers can innovate and offer value-added services. Competition and collaboration should also be encouraged between Data Spaces themselves, in order to ensure that there is no lock-in. This requires, in part, data portability between Data Spaces so that data can be efficiently exchanged and moved between Data Spaces when necessary.
Flexibility and adaptability: Data Spaces are an evolving technology *and* an evolving ecosystem, intended to be deployed into a variety of contexts and use cases. Even within the narrow set of use cases discussed here, flexibility and adaptability emerged as an important principle to be adopted in

order to allow for Data Spaces to adapt to new types of contracts, roles, and business models based on evolving needs. Governance structures should, therefore, be flexible and agile enough to accommodate such innovations.

Foster community development within the Data Space ecosystem. Encourage the development of a community of stakeholders, including data providers, consumers, and service developers.

Trust: The importance of trust in this interaction was highlighted by many of the respondents. Develop governance practices that foster trust through transparency, security measures, and fairness.

Confidentiality: Establish policies and technical safeguards to protect data from unauthorized access and disclosure during storage, transmission, and processing.

6.1.2.2 Principles Related to data ownership:

Data Ownership and Management: Data ownership should be with asset ownership, Establish clear policies linking data ownership to asset ownership, enabling clear specifications of what *is* to be shared and what is *not* to be shared. **Data Ownership and Management:** Establish clear policies linking data ownership to asset ownership, enabling clear specifications of what *is* to be shared and what is *not* to be shared.

Clearly distinguish between mandatory and non-mandatory data for effective data management. Define and separate mandatory data required for basic operations from non-mandatory data that may enhance functionality, aiding efficient data management.

Data Sovereignty: maintain control over confidential data, prevent unauthorized dissemination, and prohibit unauthorized secondary use. Ensure data providers retain control over their data with access controls and usage policies to prevent unauthorized use.

Protection of Intellectual Property: IP and trade secret protection should be embedded strongly within the system, in its technical and legal frameworks.

Promote the development and support of data models. Encourage the creation and adoption of standardized data models to improve data quality and compatibility.

Robust and enforceable access control policies. Establish access control policies defining who can access data and under what conditions, enforcing compliance through technical means.

Enable data traceability to support certifications and compliance. Incorporate mechanisms to track data usage and lineage, facilitating audits and regulatory compliance.

6.1.2.3 Principles Related to implementation:

Implement modular, plug-and-play systems, not just for the connector but also to check compliance and set up contracts. Design standard interfaces that allow for plug-and-play functionality. For example, integrate contracts into existing processes and systems, such as ERP systems.

Enhance ease of use by automating processes such as data transfer, validation, and identity management, minimizing manual intervention. Implement automation for routine tasks like data transfers, validations, and identity management to reduce errors and increase efficiency.

6.1.2.4 *Principles related to Business Models:*

Enable connectivity to data marketplaces. Support the ability to sell data and connect to data marketplaces, expanding revenue streams and promoting data-driven innovation.

Implement context-specific systems tailored to different Data Space needs. Design Data Spaces that can be customized to meet the specific requirements of different sectors or use cases.

6.1.3 Data Space Governance Framework Requirements

Table 5. Data Space Governance Framework Requirements.

Level	Data Space Governance mechanisms	Description (Terms in bold below are defined in the DSSC Glossary. Direct quotes from the DSSC Glossary are italicised.)	Governance Framework Requirements (Terms in bold below are defined in the DSSC Glossary. Direct quotes from the DSSC Glossary are italicised.)	Relevant Documents
1	Structural mechanisms	Governance mechanisms that outline the roles and responsibilities and the allocation of decision-making power within the Data Space.		
2	Data Space Roles	An elaboration of the Data Space Roles, in relation to the associated rights and duties. One Data Space Participant may take on multiple roles in a Data Space, and different roles in different Data Spaces.		Governance model, Constitutive Agreement, General Terms and Conditions
3	Common intermediary / Operator	A Common Intermediary is defined as 'A party who provides federation services that are common to all participants of the Data Space.', where Federation Services are defined as 'Services which facilitate the interplay of participants in a Data Space, enabling them to engage in (commercial) data-sharing relationships of all sorts and shapes.	All respondents agree with the necessity of the 'Common Intermediary' or 'Operator' role. The term operator is used when a single actor has more or less control. It is defined as a 'service provider that provides most of the federation services that are common to all participants of the Data Space'. Some of the participants note that it is important for the Common Intermediary or Operator to be neutral and trustful, perhaps even requiring a 'Data Space Operator' license. It is important to note that the Common Intermediary or Operator may qualify as a Data Intermediation Service Provider under the DGA, and may have to comply accordingly. This should assist,	

		The Federation services perform an intermediary role in the Data Space.’	inter alia, with ensuring that the Common Intermediary or Operator is neutral and trustful.	
3	Data Product Owner	‘A party that develops, manages and maintains a data product. A data product owner is not necessarily a Data Space participant.’	All respondents agree with the necessity of the Data Product Owner role. However, it is also important to note that a Data Product Owner can be separate and distinct from a Data Rights Holder and Data Product Provider.	
3	Data Space Governance Authority	‘The body of a particular Data Space, consisting of participants that is committed to the governance framework for the Data Space, and is responsible for developing, maintaining, operating and enforcing the governance framework.’	All Respondents agree with the Data Space Governance Authority role, with some emphasising the distinction between a Data Space Governance Authority and the Common Intermediary or Operator as being an important one to maintain and with some emphasising the important of neutrality for this role. The rules for a Data Intermediation Service Provider under the Data Governance Act 2023 may be relevant to this role. Applying the same may address many of the concerns regarding this role, including for instance for continuity and neutrality.	
3	Service Providers	Role in a Data Space that offers services to support finding, sharing, and using data above and beyond federation services. For instance, Data Space intermediaries, participant agent intermediaries, personal data intermediaries, value-creation service providers, participant agent service providers.	A small majority of the respondents agree that there may be additional ‘service providers’ involved in the Data Space in the long run. The other half did not comment on service providers. This may require, for instance, roles such as Data Space Intermediaries, Participant Agent Intermediaries, Personal Data Intermediaries, Value-creation Service Providers, and Participant Agent Service Providers. Given the current state of the responses, it is important to create flexibility in the Data Space Governance Framework for the creation of new types of service providers in the future.	

3	Auditor	A certified party in a Data Space that ensures compliance with legal requirements, or governance policies and standards.	The majority of the participants foresee an auditor or inspector role as part of the Data Space. These may be public inspection bodies, or private bodies that check, for example, the background of prospective participants or adherence to agreements by existing participants. This service may be provided via Trust Anchors, Assurance, Certification, Attestation, Declaration, Validation, or Verification. This may require the provision of a Validation & Verification Service or a Notary.	
3	Data Product Consumer	'A party that commits to a data product contract concerning one or more data products.'	All Trials foresee a Data Product Consumer. A Data Product Consumer may also be a Data Recipient.	
3	Identity issuer authority	Role in a Data Space that issues digital identities to participants for secure access.	Some respondents highlighted the importance of Identity issuers, which may be the Data Space operator or authority, but may also be another trusted third party that issues verifiable credentials. This is an important component of Identity and Attestation Management, which is necessary for Access Control, discussed below.	
2	Allocation of decision-making authority	Refers to the organisational unit that has the power to set forth data governance related decisions.	The insights herein should be taken into account to set up the functioning of the Data Space governance framework and the setup and procedural rules for the Data Space governance authority, which it needs to follow and enforce.	Governance model, Constitutive Agreement, General Terms and Conditions
3	Type of organization	Refers to the classification of entities participating in the Data Space, such	All respondents foresee the need for a legal entity that acts as the authority of the Data Space. Most of the respondents have not yet made a final decision on the type of organisation. A	

		as businesses, government agencies, or non-profits.	small majority of respondents suggest a for-profit entity, which may return its profits to the benefit of the Data Space participants. Some respondents suggested a not for profit, and a minority did not indicate a preference. An association along the lines of a 'stichting' in Dutch corporate law might provide a balance between the two.	
3	Centralized / Decentralized decision making	Refers to the type of decision making in the organisation, ranging from decentralised (decision making distributed among members) to centralised (decision making by a single authority)	Some respondents expressed a preference for centralized decision making, while a small majority expressed a preference for decentralized decision making, and a final set noted that the degree of centralization may be context dependent. Decentralized decision making was understood to include, for example, expert committees, peer groups, and voting by members of the Data Space. Some respondents highlighted the importance of decision making power to be allocated to the parties that pay for the Data Space.	
1	Procedural Mechanisms	Procedural mechanisms address data-related questions ranging from data strategy to issue management.		
2	Policies, standards, processes, procedures			
3	Data quality requirements		Respondents suggested that the following factors can be taken into account to determine appropriate data quality requirements: High frequency, continuous, measurements and sharing of key data. Inspections of data quality, especially for data related to compliance. Version control of data.	Use-case Terms of Use Data Product Contract

			Mappings between different data models to avoid mistakes in translation between different data standards.	
3	Data Contract & Policy Negotiation	Data Policy Negotiation is defined as 'The process of reaching agreements on data policies between a data rights holder, a data provider and a data recipient. The negotiation can be fully machine-processable and immediate or involve human activities as part of the workflow.'	A Data Transaction requires, inter alia, a Data Product Contract between Data Space Participants. All respondents indicated that automated contracts, or Smart Contracts as per the DSSC Glossary, could further be useful in maintaining data sovereignty. Some respondents discussed how standardised Data Access Policies and Data Usage Policies would be very helpful, while some emphasised that the machine-readable contracts used in the Data Spaces should be seamlessly integrated with existing business process, including for instance with ERP systems. A Data Product Contract should therefore align with the Data Policy, Data Access Policy, Data Usage Policy, and the Data Policy Negotiation and Data Policy Enforcement mechanisms, and the Data Space Governance Framework should allow for the usage of an appropriate Policy Definition Language. This Data Product Contract should be integrated into business processes as much as possible, potentially at a use-case level. Some respondents also indicated a need for including templates for standard agreements related to use-case and data usage, such as a maintenance contract, a service contract, or a supply contract, while other respondents noted that they would likely have to conduct negotiation regardless, but that standardised agreements could still be helpful as long as there is room for such flexibility as may be required. A final set of respondents also indicated that templates could be particularly helpful in case of repeat customers, where previous	General Terms and Conditions, Governance model, Use-case Terms of Use, Data Product Contract

			arrangements can be used as templates. Finally, some respondent also indicated that the Data Policy and Data Product Contract negotiation process could also benefit from automated checks, for instance to make sure if a potential supplier has the data available in the right formats.	
3	Data Contract & Policy Enforcement	Data Policy Enforcement is defined as "A set of measures and mechanisms to monitor, control and ensure adherence to established data policies."	Some respondents indicated that it would be important to link the termination of the Data Product Contract with the termination of the Data Access Policy, though a minority also suggested there can be a delay between the two events by agreement between parties. It is therefore suggested that the Data Product Contract be aligned with the Data Policy Enforcement and the Access Control, specifically in for instance providing an automatic termination date for the Data Access Policy in line with the Data Product Contract.	General Terms and Conditions, Governance model, Use-case Terms of use, Data Product Contract
3	Entrance to a Data Space	This is a part of the Operational Processes of a Data Space Governance Framework.	All respondents agreed that there need to be rules for the entrance of new participants, though opinions differ on the types of rules suggested. A small majority suggested that checks before participation are a good idea, with some specifically proposing testing with regards to cybersecurity and data quality. Some mentioned the necessity to agree to the Data Space Governance Framework before participation, with a minority suggesting automated contracts may be helpful.	General Terms and Conditions, Governance model, Accession Agreement

			Some respondents also suggested using external audits to establish reputation-based risk profiles upon a Data Space Participant's first entrance to the Data Space, with increasing automation based on transaction data over time perhaps through a Notary, and also indicated that having appropriate credentials should be a pre-requisite for access. Upon ascertaining compliance, a party may be issued a Membership Credential to enable its participation in the Data Space. Another minority set of respondents indicated that there should be a central system to manage this entrance, perhaps with a community manager, and that this should be automated as much as possible. A small set of participants mentioned that it would be good to have documentation and training for onboardings now, but over time the goal should be that Data Spaces are easy to understand and deploy. A final set stated that that technical support is good to have for new entrants as well.	
3	Moving and/or exiting from Data Spaces	This is a part of the Operational Processes of a Data Space Governance Framework.	A small majority respondents indicated that moving from one Data Space to another should be possible, with some indicating that it is important to ensure that this does not negatively impact ongoing contracts. A minority of participants mentioned that when a Data Product Provider moves between Data Spaces, in case of ongoing contracts, it should be ensured that the data they have	General Terms and Conditions, Governance model, Use-case Terms of Use, Exit Agreement

			promised to make accessible should still be accessible through the Data Space (e.g., via a federation). A few mentioned a sustainable approach to microservices as being a part of ensuring such continuity, and others mentioned that portability between Data Spaces is a challenge. A minority indicated that it would be important to specify in advance the reasons for which an entity can be allowed to leave a Data Space, the circumstances in which this may result in a penalty, and that data that was already shared should (still) be protected after leaving. Finally, some participants mentioned that data access should be terminated after a set period of time upon exit, requiring alignment between Operational Processes and Data Product Contracts, and that an offboarding document should be presented as well.	
2	Compliance monitoring			
3	Automated Contract Monitoring		All respondents agreed to the importance of data and contractual monitoring mechanisms, to varying degrees. The mechanisms suggested by the respondents include but are not limited to automated monitoring of client actions and/or data flow for compliance with some including notifications of access to data, and the ability to separate confidential data and data to be shared in real time. A small set of respondents suggested granular implementations of Data Access Policies and Data Usage Policies as well as homomorphic encryption, or other trusted computing	General Terms and Conditions, Governance model, Use-case terms of use, Data Product Contract

			approaches, in sync with the functioning of the connector and (centralised or decentralised) identity management to address this requirement. Finally, a few respondents also suggested putting the data on the blockchain to ensure traceability.	
3	Access control		All respondents emphasised the important of effective Access Control. Some mentioned the importance of role-based access control, while a minority further went on to specifically recommend highly granular and federated role- and event-based access controls and integrated into business process flow. Finally, some respondents emphasised the importance of access control to protect confidential data.	General Terms and Conditions, Use-case Terms of Use, Data Product Contract
3	Cybersecurity		This is an important issue for the respondents, and a small majority of respondents suggested different mechanisms to ensuring appropriate levels of data security, including but not limited to: cybersecurity and legal agreements to avoid unapproved data dissemination; regular intrusion testing, cybersecurity certifications, and bug bounties; and management protocols in the unfortunate event of data breaches.	General Terms and Conditions, Code of Conduct, Governance model, Data Product Contract
3	Compliance with regulations		Support with general and sectoral compliance is a strong requirement for all respondents. Also drawing on the results of the D2.1, we see a long and varied list of compliances, including but not limited to: the Data Act, Digital Product Passport regulations, Textile sector regulations, Data Protection regulations, AI regulation. Some of the participants also mentioned that they may, potentially, process personal data. There is therefore a need to investigate how Data Spaces can implement these compliances by default, including taking into account insights from norm engineering, and to design appropriate procedures for compliances on a per use-case	General Terms and Conditions, Code of conduct, Governance model, Use-case Terms of Use, Data Product Contract

			basis, such as for instance making provisions for conducting Data Protection Impact Assessments or Fundamental Rights Impact Assessments.	
3	Standards		Standards are, similarly, an important consideration for all of the respondents. There is a long list of standards to be complied with as well, including but not limited to: (internal and external) data sharing standards, cybersecurity standards, automation standards, and ISO regulations. These will also have to be taken into account for the Data Product Contract, but can also be further specified on a per use-case basis.	General Terms and Conditions, Code of Conduct, Governance model, Use-case Terms of Use, Data Product Contract
3	Intellectual property		In addition to the aforementioned agreements, a majority of the respondents require support for NDAs, and agreements regarding intellectual property and licensing, including dataset ownership, are crucial to most of the respondents. Determining ownership of original data and derivates, and enabling the parties to determine the same through direct interaction as and when necessary, is crucial to the respondents. A minority specifically mentioned in this scope agreements regarding usage of data to train AI. These should be further taken into account in the design of the General Terms & Conditions, but also for the Data Product Contract.	General Terms and Conditions, Use-case Terms of Use, Data Product Contract
2	Issue Management			
3	Dispute Resolution		A minority of respondents indicate a preference for having the options to file disputes with the Data Space Governance Authority, and that there should be an option to take further	General Terms and Conditions,

			legal measures as well (including mediation, arbitration, or approaching a court). A second minority of respondents suggest pairing legal options with technical measures, e.g., cutting of data access in case of non-compliance. Some respondents indicated a role for trusted third parties, for instance trade associations, that can also be approached with complaints, while some respondents indicated it would be good to have rules for compensation, and risk assessments in case of data leaks. Finally, in contrast, some respondents also indicated that they do not see the Data Space Governance Authority as an entity that can help in cases of disputes.	Code of conduct, Governance model, Use-case Terms of Use, Data Product Contract

Table 4: Data Space Governance requirements framework

6.2 TRIALS modelling approach

Using a MBSE (Model-Based Systems Engineering) approach can be very beneficial for SM4RTENANCE's Data Space trial projects, including improved communication and alignment between project partners, in-depth analysis of Data Space architectures of the project, comprehensive requirements support, and strong traceability between the constraints and needs expressed at the beginning of the project and the technical achievements.
The project model could be supported by the DSSC framework as described in Section 4.2. We first model the DSSC framework in Capella/Arcadia in order to fill it up with the Trials' information. The purpose of the model is to represent the framework as it is described by going further in explaining the links between the concepts and elements of it.
Capella and Arcadia are closely connected tools and methods used in systems engineering to facilitate the design, analysis, and management of complex systems. They are widely adopted in industries such as aerospace and defence, where MBSE is critical.
We describe in the Figure 23 the main concepts of the DSSC and in Figure 24, the developed view of the "Data product" key concept.

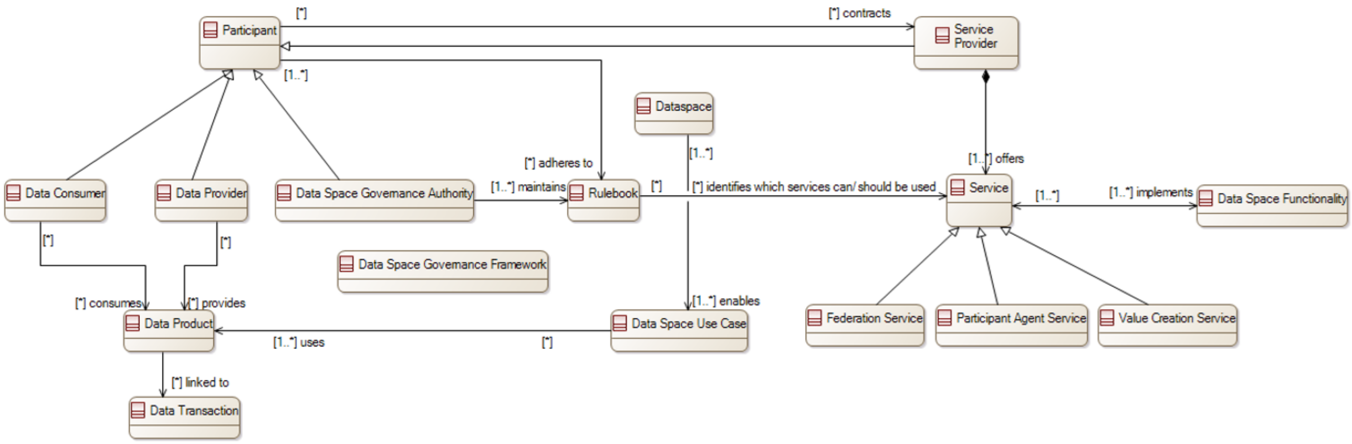

Figure 23. DSSC Key Concepts overview.

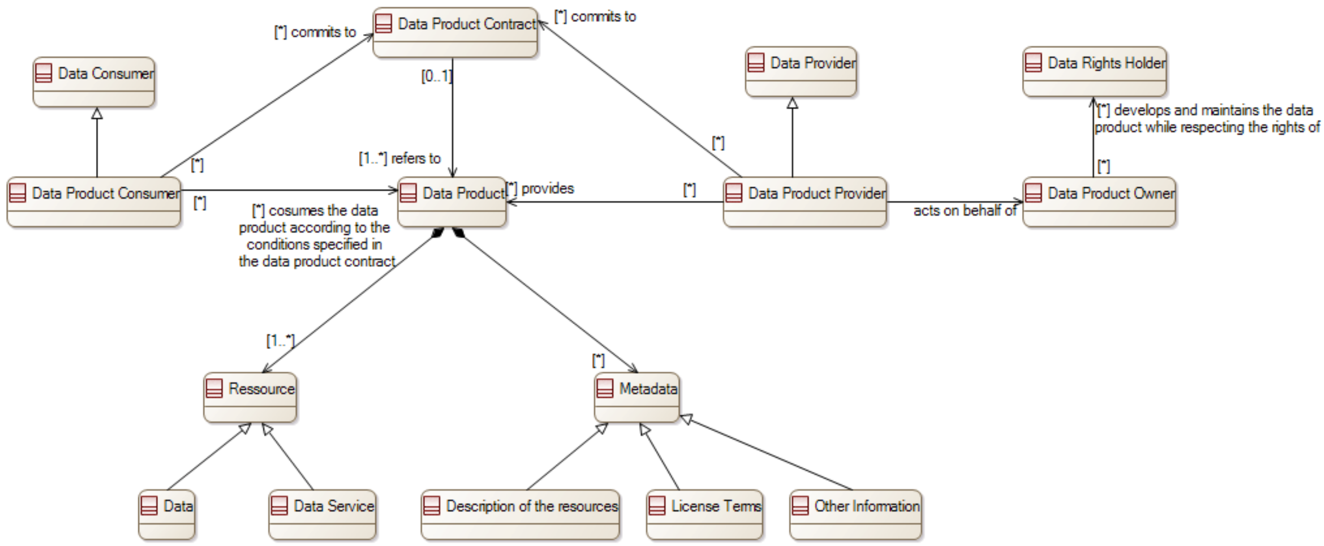

Figure 24. The DSSC Data Product concept and its relative ones.

The DSSC framework proposes a Building Block view as shown in Figure 4, which we modelled and extracted from the blueprint documentation a comprehensive description of the capabilities corresponding to these building blocks. The next three Figures (25-27) represent these Business, Governance and Legal capabilities:

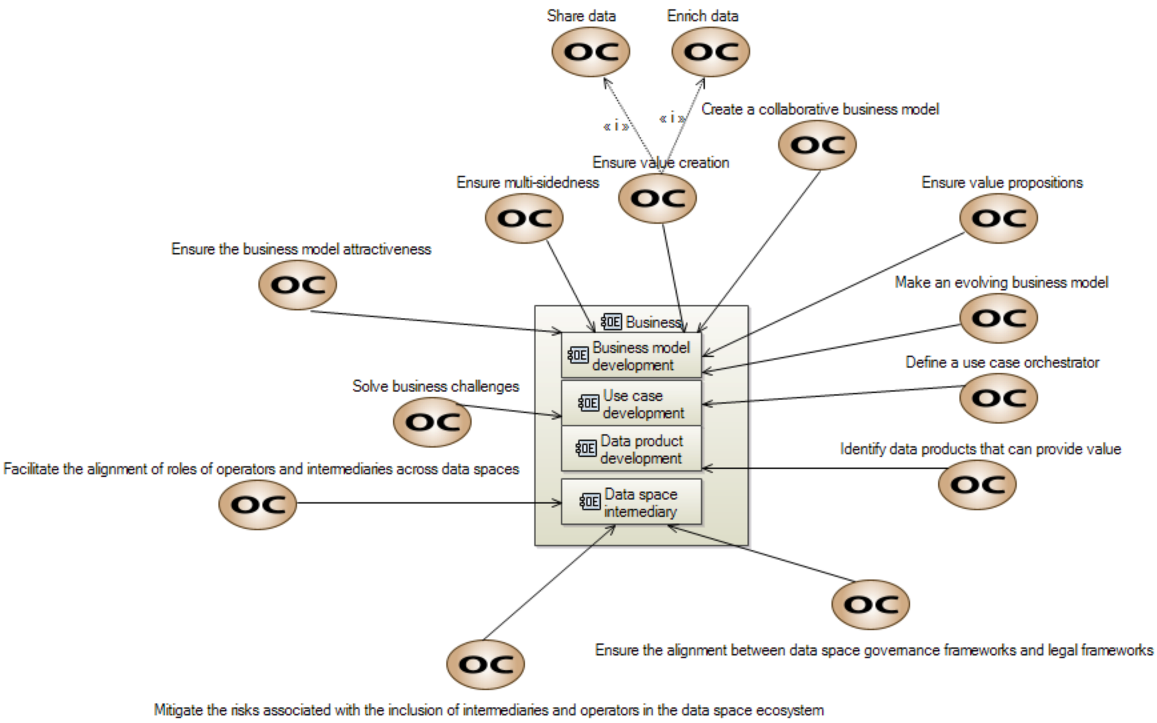

Figure 25. Business Capabilities.

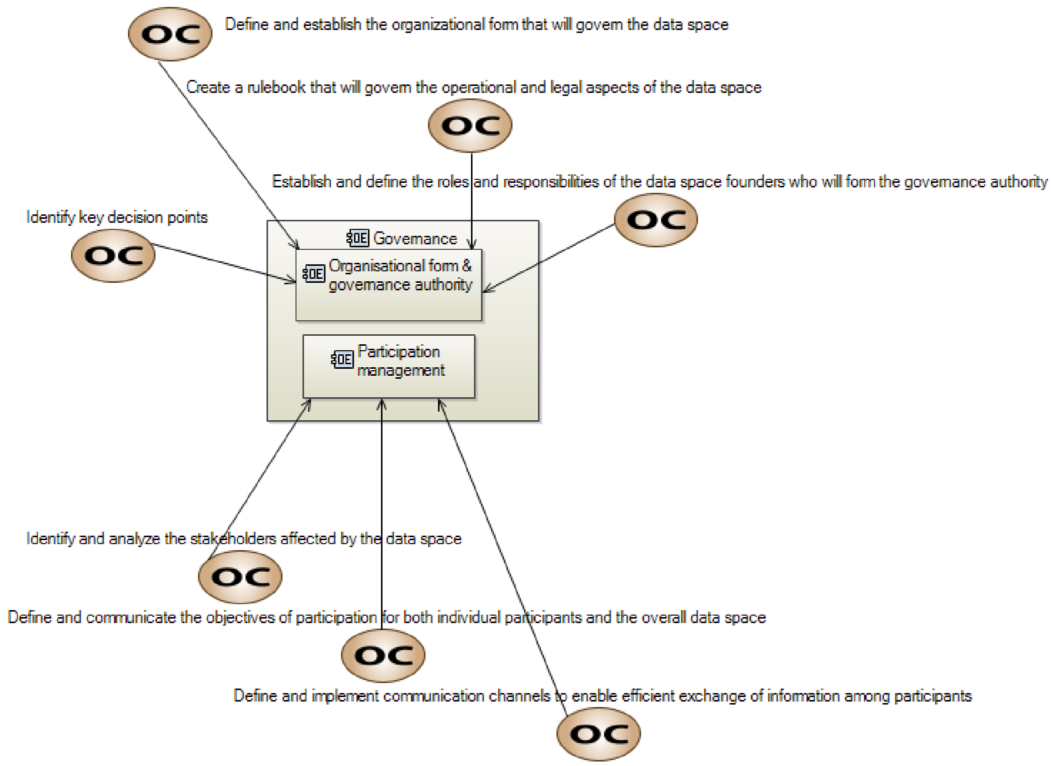

Figure 26. Governance capabilities.

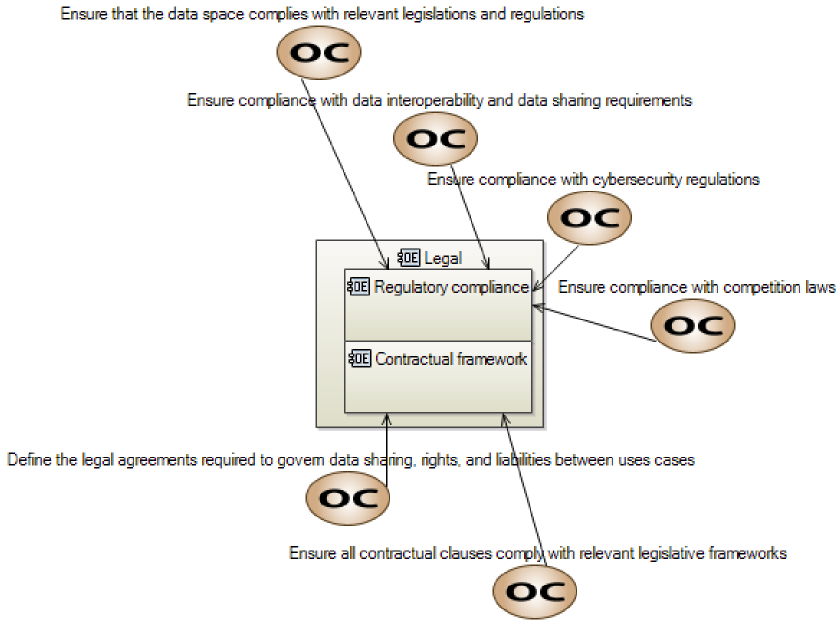

Figure 27. Legal capabilities.

This in-depth analysis of the DSSC framework is at this point only a draft, but it will be enhanced during the project and could afterwards drive the establishment of requirements for the design of the Data Spaces of each Trial of the SM4RTENANCE project. This will be initially tested on one of the pilots, in order to assess whether it is worth extending to the others.

7 The path to Data Space harmonization

The levels of interoperability for data have been defined in the previous sections (5,6)
Fundamental, or Technical. This level concerns IT systems and protocols that enable data to be transferred, prior to it being interpreted. Ex: SFTP, Open API
Structural or Syntactic. This concerns the format of the data, which is a prerequisite for it to be interpretable by a computer system. e.g. JSON, CSV, etc.
Semantic. This level concerns the additional information (metadata), and the way in which the data is organised, to leave no room for interpretation of the meaning of the raw data. For example, business or sector data standards, international accounting standards, etc.
Governance. This level covers several sub-levels which enable several systems and organisations to exchange data beyond the technical, syntactic or semantic framework. This involves sharing a vision, within an ecosystem of well-defined participants, with a business model and common rules.
Organisational. The challenge is to manage organisations and their users, in terms of identities, access rights and roles.
Legal. The aim is to provide a common legal framework of trust at two levels: Between ecosystems, between organisations (e.g. GCU)
All these levels must be covered to ensure interoperability between heterogeneous infrastructures or disjoint ecosystems.

To sum up, real interoperability between Data Spaces will have to be built on a certain number of common principles and 'federated services.

- Use of 'federated' solutions or platforms ensuring communication, at a technical level, between several protocols (API, FTP, databases, etc.).
- Use of 'federated' solutions or platforms providing automatic transformation from one syntax format to another.
- At the same time, promotion or even imposition of a sufficiently restricted framework of syntax standards within territories, covering the various sectors and use cases.
- Promotion of (semantic) data standards with sectoral or even sub-sectoral granularity
- Use of 'federated' solutions or platforms to check that a dataset complies with a standard, or even to transform a dataset to make it compliant with the standard.
- Use of 'federated' solutions or infrastructures supporting all the conditions required for a trusted data transaction, as defined in the future CEN TDT standard, and complying with the Gaia-X principles to ensure genuine interoperability. These services must be capable of managing:
  - Identity verification in a distributed or decentralised environment.
  - Verification of claims (Verifiable Credentials) in a distributed environment.

- The provision of a federated 'data products' catalogue based on common principles and compatible technologies in terms of metadata structure.
- The end-to-end process of contractualisation and licensing of data, potentially including invoicing.

SM4RTENANCE Blueprint will achieve these levels of interoperability through the implementation of the components of the SM4RTENANCE architecture.

The main challenge for Data Space interoperability lies in that there is no single technical or organisational approach that can be standardized and applied for the establishment of a specific Data Space. Every business sector has its own characteristics and must follow very specific requirements. The Data Space infrastructure and components should thus support flexibility, adaptation, and modularity. SM4RTENANCE blueprint & infrastructure will therefore aim to define a set of services and components that can be used both to deploy the SM4RTENANCE Data Space and to helps other Data Spaces to federate around SM4RTENANCE. The architecture is based on:

- DSSC Blueprint v.1.5.
- DSSC Co-Creation method
- Interviews with trials

SM4RTENANCE blueprint will be composed of the following:

- **Building Blocks** define needed functionalities for a Data Space as business, governance, legal and technical dimensions. SM4RTENANCE Blueprint uses the Building Blocks as the high-level structure to define the functionalities.
- **Services** define how different functionalities can be implemented. SM4RTENANCE Blueprint describes the services at a conceptual level but does not go into the specifics of the implementation. SM4RTENANCE Blueprint has been defined in modular fashion to promote openness and interoperability.
- **Tools** are the possible implementations of the services. These can be open or proprietary.

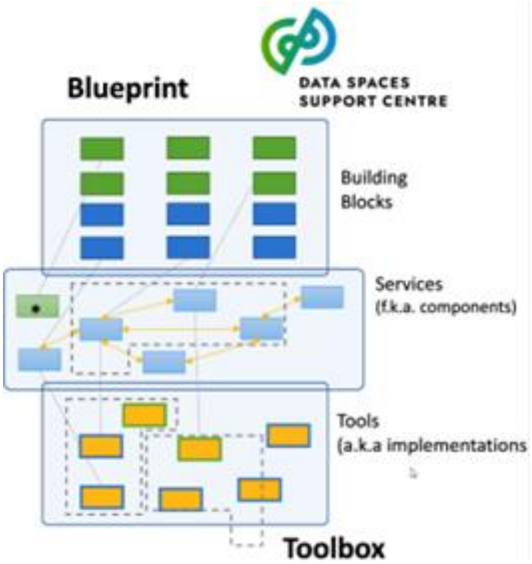

Figure 28. DSSC Building Blocks, services and tools.

Implementation of the SM4RTENANCE Data Space services according to the DSSC Blueprint

Key Concepts

		Building Block	Data Space Participants	- Data Consumer	- Data Provider	- Data Space Governance Authority	- Service Provider	Services	- Federation service	- Participant Agent Service	- Value Creation Service	Data products	Rulebooks	Data transaction	Data space governance frameworks	Data space functionnalities	Associated WP/task	Lead partner
Organisational &Business	Business	Business Model	x			x	x	x							x	x	T2.3	CARSA
		Use Case development	x				x	x				x			x	x	WP5	SQS
		Data Product										x			x		WP5	SQS
		Intermediary and operators	x				x	x							x	x	WP5	SQS
	Gouv.	Organizational Form & Governance Authority	x			x	x						x		x	x	T6.1	TNO
		Participation Management	x			x									x		T6.3	SYXS
	Legal	Regulatory Compliance	x			x	x								x		T6.2	NTT
		Contractual Framework	x		x	x							x	x	x	x	T6.2	NTT
Technical	Interop	Data Models	x	x					x	x		x					T2.4	FF
		Data Exchange							x	x							T4.3	NTT
		Provenance & Traceability	x		x		x		x	x				x	x	x	T3.3	Sovity
	Sover. & Trust	Access & Usage Policies and Enforcement	x	x	x		x			x			x	x	x		T3.2	Atlantis
		Identity & Attestation Management	x							x				x	x	x	T3.5	SQS
		Trust Framework	x			x	x		x	x			x		x	x	T3.2/T3.3	Sovity
	Value Creation	Data, Services & Offerings Descriptions	x	x	x		x		x	x	x	x		x	x	x	T3.3	Sovity
		Publication & Discovery	x	x	x		x	x	x	x	x			x	x	x	T3.3	Sovity
		Value Creation Services	x				x	x	x	x	x					x	T4.5, T3.3	Sovity, NTT

Figure 29.SM4RTENANCE Data Space components with respect to the DSSC Building Blocks.

The services and components of the SM4RTRENANCE Data Space have been organized in the picture above, to illustrate how it fits with the latest DSSC blueprint (v1.5). As highlighted in the next picture, the SM4RTENANCE services and components will be available within the SM4RTENANCE Portal. The SM4RTENANCE portal framework will act as a single management interface for Data Space participants. They will be able, for example, to register their organisations, manage their organisation and user data, and manage their technical integration to the SM4RTENANCE Data Space federation (e.g. IdP or Connector). The portal will integrate other value-creating services, such as the marketplace, the register of digital twins or the sandboxing and IA services. The portal will list certified applications (T3.5), and will also enable Data Space services and solutions to be federated with the DOME portal.

To enable identity interoperability, the main cornerstone for Data Space federation, SM4RTENANCE will be based on the open and decentralised concepts of GAIA-X, in particular self-sovereign identities. Each legal entity associated with a trading partner number should also be able to obtain a DID (decentralised identifier) that complies with W3C standards. The Managed Identity Wallets service will implement Self-Sovereign-Identity (SSI) (T3.2). The connectors (e.g. Eclipse Data Space Connector, SOVITY, TNO, TRUE, etc) will rely on a DAPS instance to acquire and validate dynamic attribute tokens (DATs). In doing so, it implements JWT client authentication (RFC7523) for OAuth2. This protocol allows connectors to authenticate themselves to the DAPS with their X509v3 certificate and in return obtain an access token that they can use to access other connectors. In addition, the portal will make possible to access all the connection points in the Data Space via API connection point.

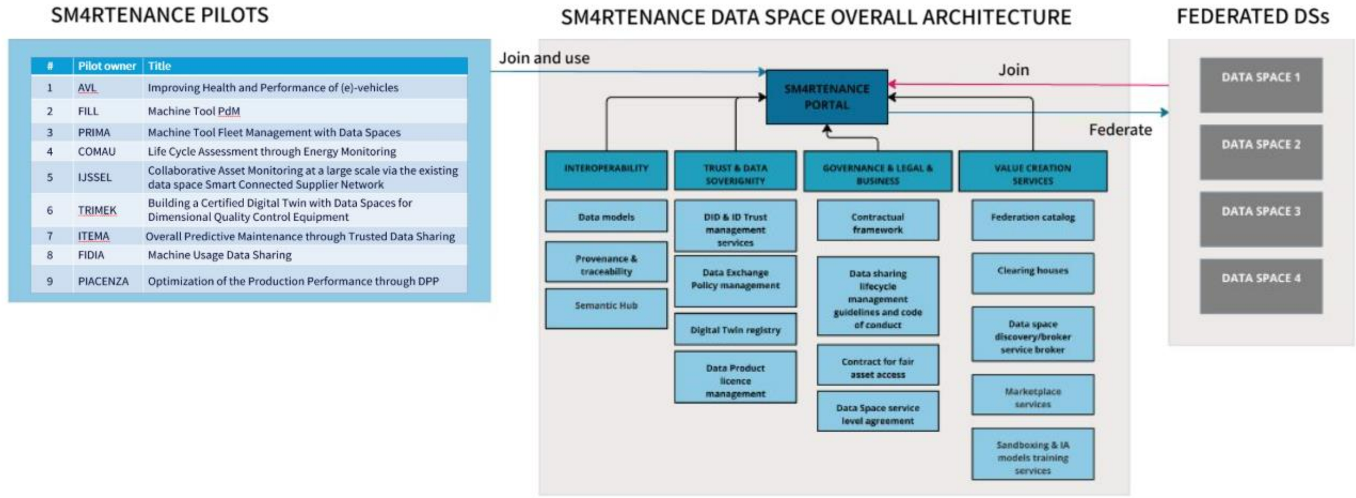

Figure 30. SM4RTENANCE Data Space components categorization.

The SM4RTENANCE Portal will be the main component for achieving interoperability and achieve the federation of Data Spaces. As explained in the picture below, every specific Data Space of the future federation will be managed at local Level. Data Space owner(s) will have to choose technology (e.g. connector), identity management, access (to the Data Space) rules/policies and what information to expose via API to the SM4 portal backend. A trusted user (organisation/person) via Frontend/Backend/API will be able to:

- View basic description of the Data Space A (purpose, members,...).
- View Data Space A catalogue (if shared by Data Space A Owners).
- Request to access Data Space A (if allowed by Data Space A Owners).
- Manage its SM4 credentials.

A trusted user (organisation/person) or a group of them will have the possibility to add/create a new Data Space and connect to SM4 Central Architecture. To create a new Data Space, technology provided by SM4 members can be used to speed up interoperability/federation. At the end, any Data Space should be interoperable with the SM4RTENANCE central architecture.

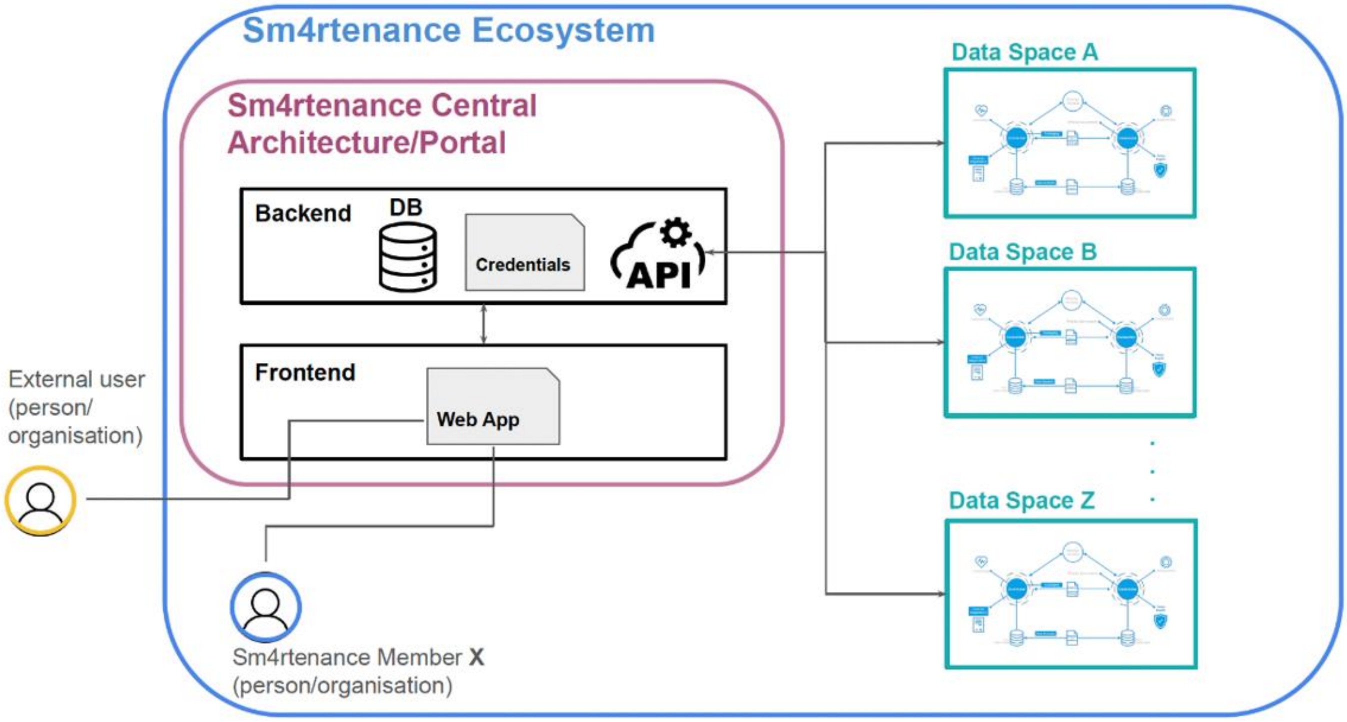

Figure 31. SM4RTENANCE preliminary high-level architecture model.

For the first delivery of SM4RTENANCE services, it has been decided to have a first minimum level of federation support. The objective is to support a minimum level of federation that works with the cornerstones of the Data Spaces federation, while ensuring alignment with standards, protocols and technologies used in existing Data Spaces, and giving SM4RTENANCE the possibility to quickly test what works or not with live Data Spaces (Data4Industry-X, SCSN).

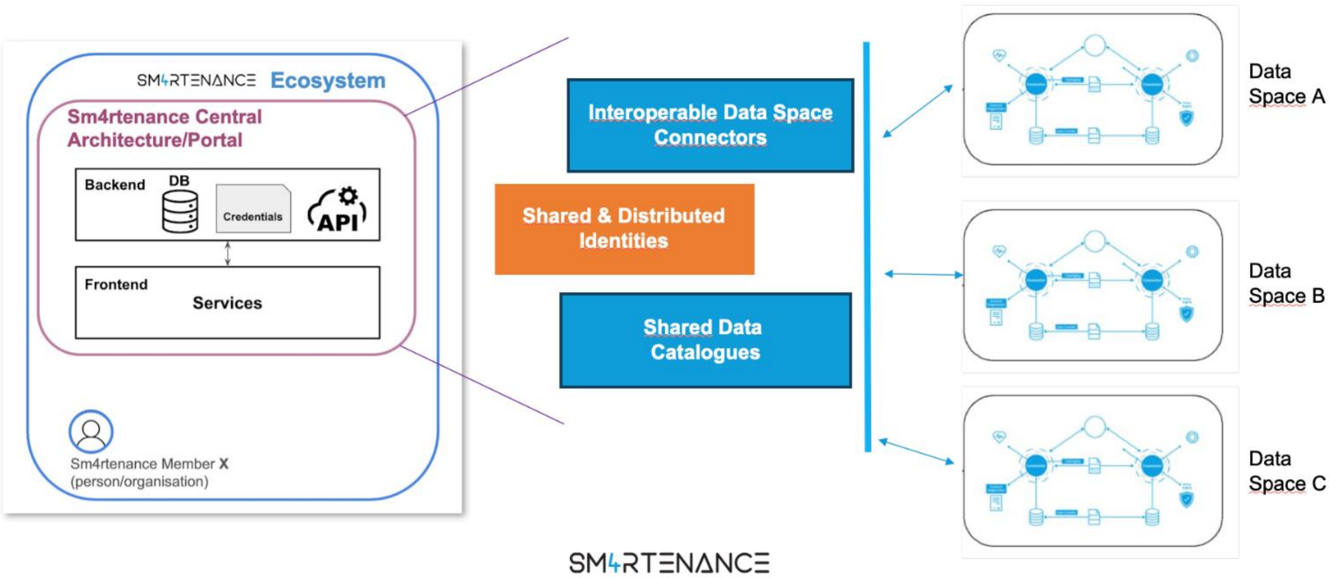

Figure 32. SM4RTENANCE first core services to support federation.

To support the federation of Data Spaces around the SM4RTENANCE portal and the interoperability between and within Data Spaces, SM4RTENANCE architecture will rely on the use of common open standards and protocols.

7.1.1 Common standards and open components to support Data Space harmonization and achieve technical and semantic interoperability

7.1.1.1 OPC UA with Companion Specifications

Open Platform Communication Unified Architecture (OPC UA) is an open interface standard specified in IEC 62541 for Industrie 4.0 Communication and is already established in the mechanical and plant engineering industry. It provides an open, secure and scalable communication architecture for vendor-neutral connection. This standard has two decisive features:

1) It allows data to be exchanged between different devices or systems in industrial environments securely and reliably.
2) It enables data structuring and the semantic description and modelling of information.

OPC UA contains both the basic functions, and the information models required for Industrie 4.0 communication and interoperability in Data Spaces.

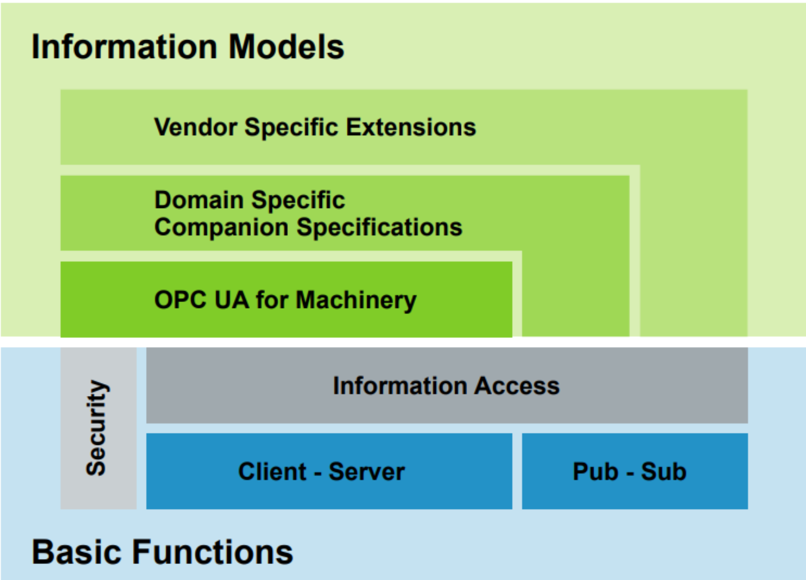

Figure 33. Logical layers of OPC UA[57].

The basic functions cover transport, security and information access:

[57] https://www.vdma.org/documents/34570/80333104/Industrie%204.0%20Communication%20Guideline%20-%202023.pdf/aaa20f84-a6a8-26de-fd63-b699815aeace?filename=Industrie%204.0%20Communication%20Guideline%20-%202023.pdf

- **Transport:** implements information access using various communication mechanisms and protocols based almost exclusively on the Internet Protocol (IP) and therefore requires a network infrastructure that enables IP communication. OPC UA is based on the communication patterns client-server and publish-subscribe. The transport layer enables communication with different protocols such as TCP, HTTPS, UDP or MQTT with client-server and publish-subscribe. These are applicable across all levels from the field to the cloud.
- **Security:** is a key element of OPC UA. Security mechanisms cover the transport layer, the information access and the discovery mechanism and require the administration of certificates and access rights Certificates enable the authentication of OPC UA applications in order to prove their identity. Certificates can be managed either for each OPC UA application, or by means of a company-wide public-key infrastructure (PKI). A PKI can issue, distribute, and test certificates. The Certificate Authority (CA) can be used to issue company-wide certificates. The Federal Office for Information Security (BSI) confirms that OPC UA can be used to implement IT-secure Industrie 4.0 communication.[58]
- **Information access:** includes method calls to read and write variables and to observe events.

When implementing OPC UA in a first step the basic functions are implemented as a uniform communication interface for information access (language analogy: grammar). Variables provided by machines and plants can be found and manually subscribed to.
In a second step it is necessary to provide the structure and definition of the information to be exchanged – the **Companion Specifications**. The use of Companion Specifications increases interoperability, because it provides standardized definition of information (language analogy: vocabulary) through standardized information models. To reach interoperability is crucial that **data/ information is defined only at its source**. Thus, they are defined only once and they can be unambiguously transferred and used for different purposes, such as Data Space Applications. Furthermore, OPC UA Companion Specifications allow an efficient implementation, because the information model already exists and can be adopted. Three categories of information model can be specified:

- **OPC UA for Machinery** (OPC 40001) is the harmonized basic specification for the entire mechanical and plant engineering industry. The information within can be used in various sectors equally, i.e. across multiple domains. The content is based on use cases and is therefore divided into individual elements that can be used as required (e.g. Machine Identification, Machinery State, Process Values, Result Transfer, Counters, Job management, etc.) Standard specifications available here: https://www.vdma.org/catalogs
- Industry or **domain-specific companion specifications** comprise the integration of standard information, data types, objects and methods specified in a certain domain or industry (e.g. Machine Tools, Robotics, Geometric Measurement Systems, etc.), and thus describe the information through a standardised domain-specific information model. Standard specifications available here: https://www.vdma.org/catalogs
- **Vendor-specific extensions** are information models extended in a manufacturer-specific manner on the basis of functions that go beyond the standard and are based on the experience or protected knowledge of individual manufacturers. They solely contain information that a manufacturer expressly wishes to offer and can be protected against unauthorised access.

[58] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/OPCUA/opcua.html

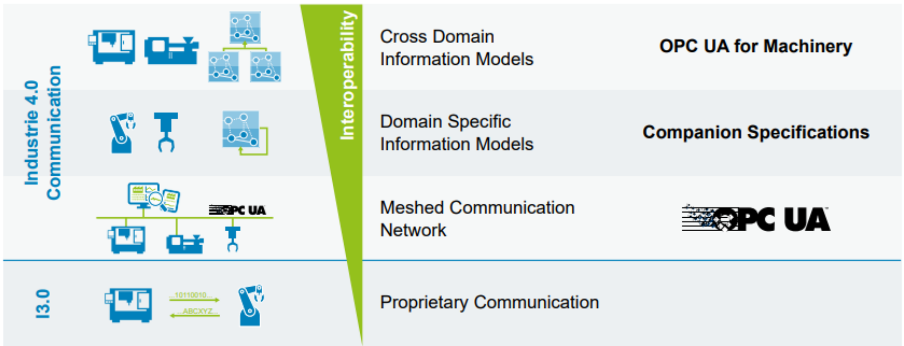

Figure 34. Interoperability through Industrie 4.0 communication 59.

In the field of mechanical and plant engineering, Companion Specifications are created under the umbrella of the VDMA together with the companies relevant to the industry and the OPC Foundation. All Companion Specifications are being administered by the OPC Foundation.

- All standard Companion Specifications for mechanical and plant engineering industry are open available here: https://www.vdma.org/catalogs
- The nodeset files associated with the Companion Specifications are provided by the OPC Foundation and can be downloaded from the following GitHub repository: https://github.com/OPCFoundation/UA-Nodeset

OPC UA and other technologies such as Asset Administration Shell (AAS) complement each other well. Machine Information is defined at its source and is already standardized in OPC UA Companion Specifications (single source of truth). During operation, asset data can be aggregated and transferred via OPC UA an allocated e.g. to the AAS, which can be used for information about an asset along its entire life cycle.

7.1.1.2 Asset Administration Shell

The Asset Administration Shell (AAS) serves as the standardized digital representation of an asset and is fundamental for the interoperability of Industry 4.0 components organized within Industry 4.0 systems. Assets in complex systems are interdependent and must interact with other assets or respond to environmental influences in terms of resilience[60]. Assets are defined in IEC 62443-2-1 as "a physical or logical object owned or controlled by an organisation and having either a perceived or actual value to the organisation". The Industry 4.0 component is defined as the combination of the asset and its digital representation, the AAS. Each Industry 4.0 asset is associated with an Asset Administration Shell that grants access to its properties, services, and event-related information. AAS can exist for both physical and non-physical entities, meaning that devices, workers, products, and even processes can have their own Asset Administration Shells. Industry 4.0 encompasses a holistic

[59] https://www.vdma.org/documents/34570/80333104/Industrie%204.0%20Communication%20Guideline%20-%202023.pdf/aaa20f84-a6a8-26de-fd63-b699815aeace?filename=Industrie%204.0%20Communication%20Guideline%20-%202023.pdf

[60] https://reference.opcfoundation.org/I4AAS/v100/docs/4

understanding of asset, which includes elements such as factories, production systems, equipment, machines, components, products, raw materials, business processes, orders, intangible assets (such as processes, software, documents, plans, intellectual property, and standards), services, human resources, and more.[61] The AAS can represent a simple component, a machine, or a plant at any level of the equipment hierarchy.

The manufacturer provides this standardized digital representation to customers, creating both an AAS for the asset type and for each individual asset instance. Throughout the asset's lifecycle, system designers, asset users, applications, processes, and the asset itself continuously update the information contained within the AAS until the asset is disposed. From the manufacturer's perspective, the asset is considered a product. The manufacturer manages different asset types, each with its own history and different versions. Simultaneously, they produce instances of these diverse types and versions.

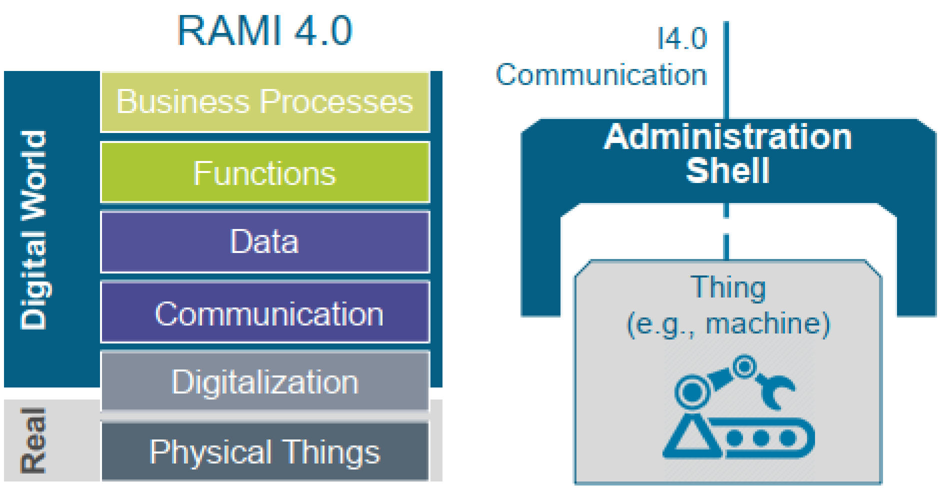

Figure 35. The concept of AAS[62].

7.1.1.3 Digital Product Passport (DPP)[63]

The European Commission (EC) defines a 'product passport' as a product-specific data set, which can be electronically accessed through a data carrier to "electronically register, process and share product-related information amongst supply chain businesses, authorities and consumers". The Digital Product Passport (DPP) would provide information on the origin, composition, and repair and disassembly possibilities of a product, including how the various components can be recycled or disposed of at end of life. By providing a detailed digital

[61] Federal Ministry for Economic Affairs and Climate Action (BMWi) "Details of the Asset Administration Shell – Part 1- The exchange of information between partners in the value chain of Industrie 4.0, (Version 3.0RC02), Platform I4.0, May 2022

[62] Graphics RAMI 4.0 © Plattform Industrie 4.0 and ZVEI, Administration Shell © ZVEI SG Modelled und Standards, Pictograph © Anna Salari, designed by freepik

[63] https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability

record of a product's lifecycle, the DPP will improve supply chain management, ensure regulatory compliance and help companies identify and mitigate risks related to authenticity and environmental impact.[64]

Digital Product Passports address three industry needs: First, they capture all relevant information about a product in a single, machine-readable document. Second, Digital Product Passports respond to increasing regulatory requirements and demand for sustainability information along a product's value chain. And third, Digital Product Passports are an important enabler for a circular economy.

DPPs could be implemented in sectors producing batteries, textiles, furniture, electronics, and construction and building materials in a similar way to Material Passports, Building Information Modelling (BIM) and automobiles (Catena-X).

7.1.1.4 IDSA Dataspace Protocol

The Dataspace Protocol (DSP) is at the core of the technical implementation of any Data Space component, ensuring interoperability between Data Space participants and acting as a strategic catalyst for the Data-Driven Economy.

The Dataspace Protocol is a set of specifications designed to facilitate the interoperable exchange of data between governed entities based on Web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate agreements, and access data as part of a federation of technical systems called a Data Space.[65] In addition, the Dataspace Protocol promotes the adoption of standardised vocabularies and ontologies, thereby enhancing semantic interoperability and enabling common interpretation of data across different environments.

The DSP introduces the separation of the control plane from the data plane. This separation improves both security and efficiency. The control plane focuses on decision-making (managing user access, identifying participants and routing data) while the data plane handles the actual exchange of information.[66]

[64] https://circulareconomy.europa.eu/platform/en/knowledge/digital-product-passport-ticket-achieving-climate-neutral-and-circular-european-economy
[65] https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol

[66] https://internationaldataspaces.org/the-dataspace-protocol-a-game-changer-for-interoperability-and-data-sharing/

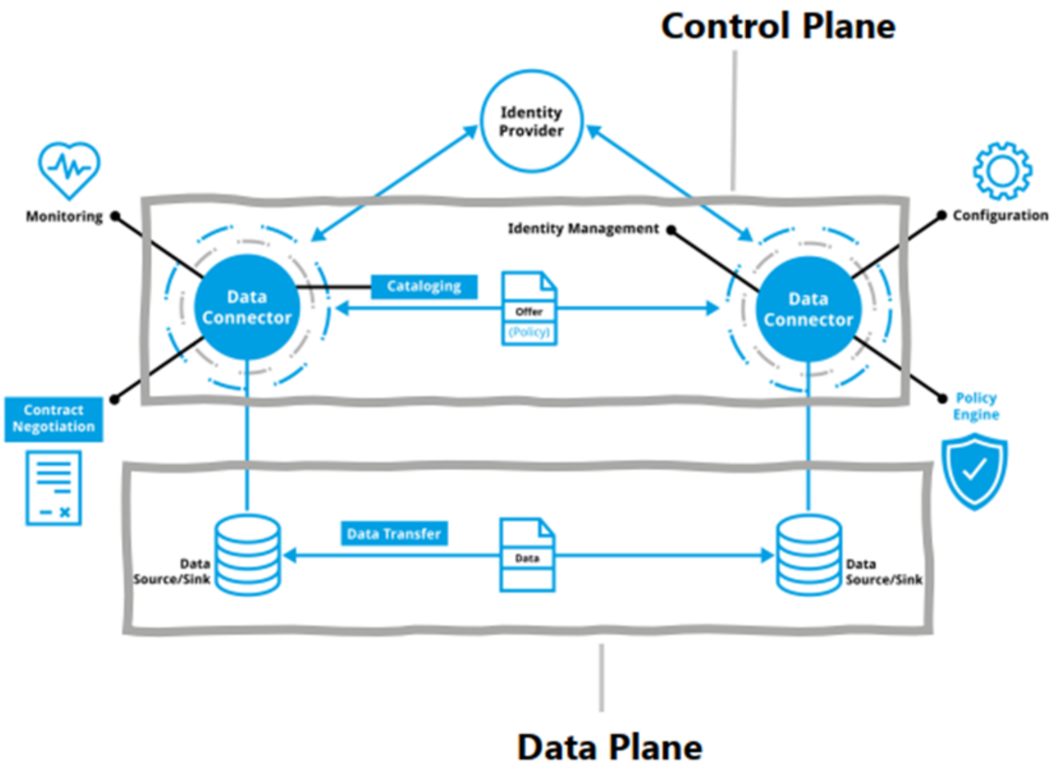

Figure 36. Dataspace Protocol – technical innovation and strategic enabler[67].

A major achievement of the Data Space community was the release of the stable version of the Dataspace Protocol (DSP) in March 2024. The protocol specification follows the functional requirements of the business processes outlined in the IDSA Rulebook, which is based on mutually agreed industry requirements.

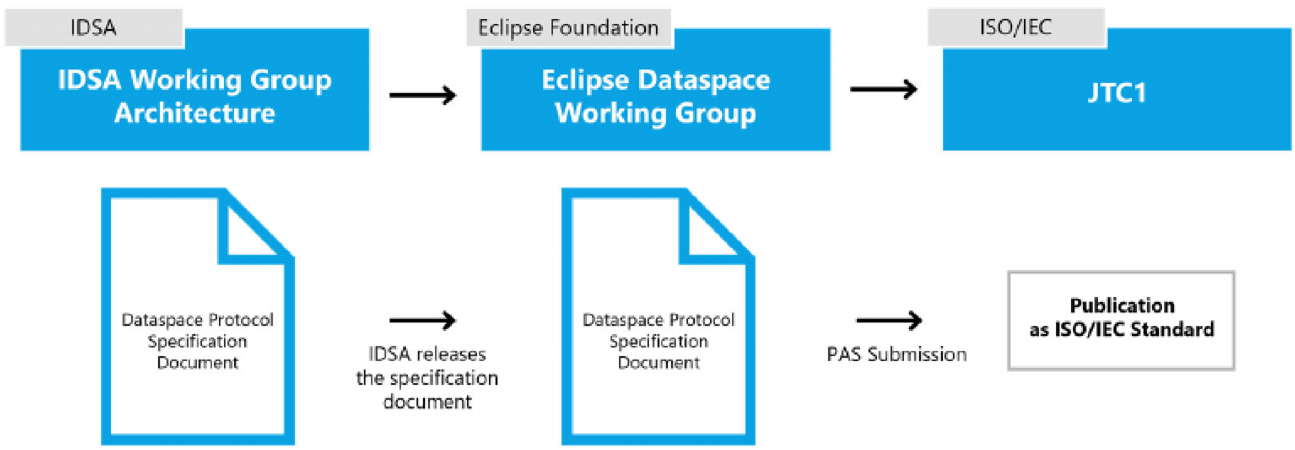

Figure 37. Data Space Protocol pathway to becoming an ISO/IEC Standard.

[67] Turkmayali, A., Gras, N., Making the Dataspace Protocol an international standard, International Data Spaces Association, 2024 https://doi.org/10.5281/zenodo.12663036

The DSP will soon become an international standard (see Figure 37), a remarkable accomplishment for the entire Dataspace ecosystem, as we approach the end of the year. The Technology Compatibility Kit (TCK), currently being developed as part of the Eclipse Dataspace Protocol specification project, called the Eclipse Dataspace TCK, will ensure compliance with the Dataspace Protocol. Test cases created to verify compliance with the specification document are included in the TCK. Connectors that pass the TCK tests will demonstrate compliance with the DSP, providing confidence to users and enabling smooth integration.[68]

7.1.1.5 The Eclipse Dataspace Components (EDC) Connector

The EDC Connector[69] is an open-source framework hosted by the Eclipse Foundation for developing secure, globally scalable data-sharing services. It offers highly customizable components for building control planes, data planes, decentralized identity systems, and federated data catalogues. Supported by leading enterprises and cloud providers, the EDC Connector equips developers with the essential tools needed to create innovative solutions for data-sharing networks. The EDC Connector provides a robust framework for sovereign, inter-organizational data exchange. This framework contains modules for performing data query, data exchange, policy enforcement, monitoring, and auditing. It integrates with existing identity, data cataloguing, and transfer technologies to provide compliance, policy enforcement and governance across organizations. It will implement the International Data Spaces (IDS) standard, along with the relevant protocols associated with GAIA-X. The connector is designed to be extensible to support alternative protocols and integrate with various ecosystems.

Data Spaces can be built by developers utilizing the following services:

- Identity Services for the management and verification of organizational credentials utilizing Decentralized Identifiers (DIDs) and W3C Verifiable Credentials, or alternatively, OAuth2.0 tokens.
- Catalogue services for publishing and securing assets that can be shared with other organisations.
- Control plane services to automate the creation and processing of data use agreements that grant access to data. The Control Plane is responsible for creating contract agreements that grant access to data, managing data transfers, and monitoring usage policy compliance.
- Data plane and monitoring services to initiate and manage data transfers using standard protocols. The data plane describes how the EDC Connector integrates with wire protocols such as HTTP, Kafka, cloud object storage, and other technologies to transfer data between parties.

SM4RTENANCE will support different versions of the EDC connectors:

- The original version,
- The versions deployed and customized by other Data Spaces players (Catena-X, T-Systems, Huawei, Fiware, FDSC, in priority)

[68] International Data Spaces Association, Data Connector Report 84 Version 16 Published September 25,2024 | Version 16.0 available at: https://zenodo.org/records/13838396

[69] https://projects.eclipse.org/projects/technology.edc

7.2 The SM4RTENANCE Data Space Governance model for governance, legal and organizational interoperability

Regarding the DS governance model, its initial inception will follow a centralized scheme (IDSA's DAPS approach). At the time of writing, there are no mature open source decentralized identity mechanisms, while the assessment results reported in Section 6 indicate some preference for a centralized authoritative entity in the form of a Data Space Governance Authority, Intermediary or Operator. The objective will be to progress towards a decentralized Data Space Authority. It does not mean that all the Data Space services will be decentralized; some of them will be, other will be federated, according to best practices and requirements.

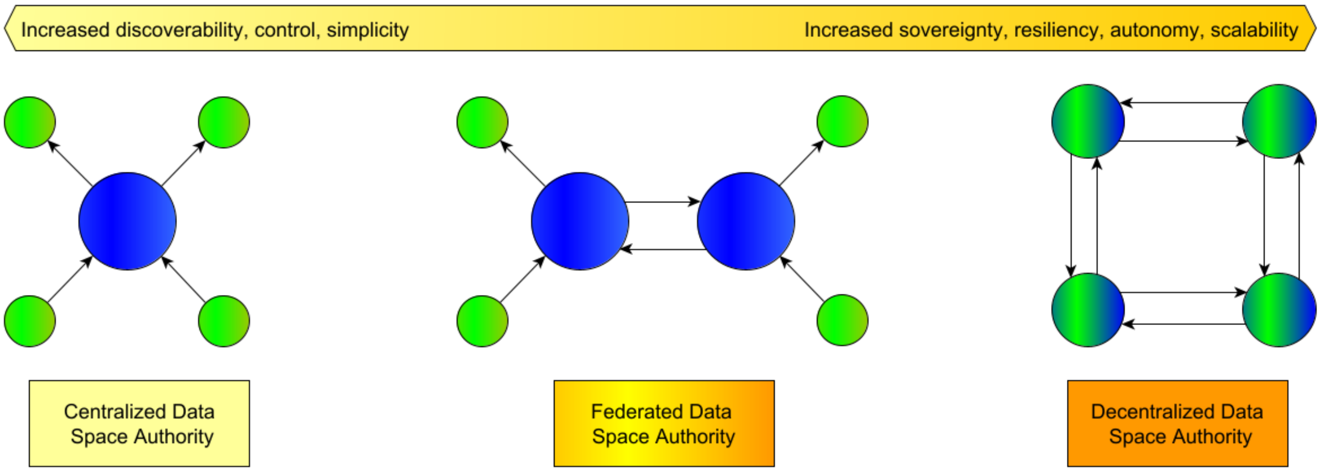

Figure 38. Data Space Governance Authority models with varying degrees of centralisation.

The Data Space Governance Authority will encompass key decision-making points for the effective establishment and operation of a Data Space, including

- the creation of an organisation's form and the establishment of a Data Space,
- the creation of a governance authority
- the creation of a Data Space governance framework
- setting internal rules and policies
- Define the technical specifications for the use of Data Space services
- ensuring compliance with internal and external rules and regulations
- creates mechanisms for continuous improvement of the Data Space, identity management, access controls and risk mitigation to build trust and quality within the Data Space
- maintains and operationalises the Data Space services
- etc

The SM4RTENANCE Data Space Governance Authority will support the federation of Data Spaces around the SM4RTENANCE Portal, which will act like a catalyst for providing the services that will help other Data Spaces to join the federation, by achieving the governance, legal and organizational interoperability of the Data Space (s).

7.2.1 Governance interoperability

In order for Data Spaces, with different legal forms and structures, to work together, it is necessary to define general collective operating rules. These rules concern the business model (between Data Spaces or platforms), the governance, decision-making and escalation processes, and the organisation that will be responsible for steering this governance.

It should be noted in this context that the Data Governance Act, which came into force in September 2023, defines the obligations and responsibilities of organisations that offer data exchange services (known as Data Intermediation Service Providers, or DISPs). Thus, any interoperability strategy within and between Data Spaces will need to devise clear governance processes, at both 'local' and 'federal' levels, and consider the creation of a governance organisation in constructive dialogue with national governance authorities.

More specifically, the interoperability of business models will need to be worked on in depth. For example, if access to a Data Space A is subject to subscription conditions and charges for the use of services, it will be necessary to determine under what conditions other Data Space, and their participants, can access the products and services of platform A.

SM4RTENANCE implementation: Data Space service level agreement contract; Data sharing lifecycle management guidelines and code of conduct

7.2.2 Organisational interoperability

Trust between participants and respect for the confidentiality and security of data are prerequisites for any exchange of data, whether within Data Spaces or between them. To ensure that these conditions are met, a number of factors need to be taken into account:

- Ensuring that the organisations, individuals, or even applications participating (as data provider or acquirer) are who they say they are. This involves :
- Verifying identities. In an ecosystem as heterogeneous as Data Spaces, identities are fundamentally distributed between central national systems and local enterprise systems. The management of distributed identities (or DIDs) is a prerequisite in this context, and must be provided in a 'federated' manner between ecosystems.
- Verification of claims or credentials. An organisation, or an application, may, for example, claim to be ISO 27001 or SOC 2 certified (from a security point of view) when it offers data on a platform. However, the purchaser must be able to check that these claims are well-founded, in order to have confidence in them. This is technically known as 'Verifiable Credentials' (or VCs), which are the subject of a W3C standard supported and implemented as part of Gaia-X.
- Defining and managing data access rights, according to the identities and roles defined for each participant. This requires a 'common' system for managing access rights, which in turn requires federated services between local data platforms.

Furthermore, the fact that the various Data Spaces are interoperable means that catalogues of data products and services exist at two levels:

1. Within a Data Space (locally),

2. In a federated way between all the Data Spaces (globally).

This implies that the various 'local' catalogues can interoperate with a global catalogue. To do this, the following conditions must be met:

- Shared or compatible product and service descriptive metadata structure
- Shared or compatible taxonomies
- Shared or compatible contractual and commercial metadata structure (see Legal Interoperability)

These issues need to be addressed at the level of governance (policy) to define common standards, but also at the level of the underlying technologies (data exchange solutions sharing the same principles for the structure of metadata).

It should be noted that this level is highly dependent on the level of legal interoperability, as access rights will be determined in particular by the contractual conditions defined for access to each dataset or application. For example, 'Open data' will not require access rights to be controlled, whereas private commercial data will only be accessible once a contract has been formally concluded between the supplier and the purchaser of the data.

There are international initiatives aimed at standardising this level. The most advanced, and the only one that takes account of industrial needs and notions of sovereignty, is Gaia-X, which brings together several hundred companies and institutes from all over the world and is in the process of establishing a number of de facto standards for the interoperability of Data Spaces. In particular, Gaia-X is establishing frameworks and specifications for the following topics:

Data exchange, authorisation and consent management

- Identity management: use of DiD (W3C standard), X509 and JOSE for the cryptographic chain
- Verifiable Credentials : use of VCs for services and participants (W3C Verifiable Credential, W3C SHACL and W3C SPARQL), OIDC4VC and OIDC4VP for VC exchanges
- Trust chain (ETSI TS 119 312 and EBSI APIs for Trust Anchors).

In this context, the interoperability strategy between Data Spaces will have to comply with the de facto standards established by Gaia-X, in particular for the 'federated' solutions that will be required to offer and manage data exchange services. Not only will this ensure interoperability between territories, it will also open up Data Spaces to other Data Spaces (e.g. health, mobility, construction, etc.).

SM4RTENANCE implementation : DID & ID Trust management services; federated catalog**ue**; Semantic Hub; common open standards used by SM4RTENANCE services

7.2.3 Legal interoperability

Legal interoperability must be ensured at two levels:

- Firstly, between Data Spaces, and secondly, between organisations. This involves defining the general conditions of use (GCU) that apply to everyone. This is an important element in establishing trust and laying the foundations for the governance interoperability described above.
- For each data exchange or transaction, the supplier of the data (or of services involving the transfer of data) must establish a certain number of essential conditions with each acquirer before the exchange takes place:
    - Start and end of the contract.
    - Licence and conditions for use of the data
    - Monetary compensation

- Responsibilities of the parties involved and associated penalties.
- Other terms and conditions

This interoperability can be ensured by federated services that require participants to agree to terms and conditions, and that manage the data transaction from a contractual point of view. Significant progress has been made recently in this area:

- At Gaia-X level, with the CES (Credential Event Service), which enables the distribution of VCs for services and data products between federated catalogues
- At the standards level, with the Trusted Data Transaction (TDT) initiative, which is in the process of establishing a CEN-CENELEC standard.

The interoperability strategy between Data Spaces will have to ensure that the Gaia-X principles and the processes defined in the Trusted Data Transaction initiative are implemented in and between Data Spaces.

SM4RTENANCE implementation: Data Space service level agreement contract; Contract for fair asset access, Contractual framewor, Data Product licence management; Data Exchange Policy management

7.3 Moving towards the first release

Based on the architecture outlined above and in alignment with the project roadmap, the proposal approved by the WP3 task leaders is to use the Sovity Data Space management portal solution, which is available as an Open Source release (reference link here: https://github.com/sovity/dataspace-portal). This decision aligns with the goal of reusing existing solutions rather than developing new tools from scratch. This approach is also in line with the mission of the Digital Europe Program, as previously described in the architecture. The image below (Figure 39) shows the mapping of the previously defined architecture to the adoption of the Sovity Data Space portal.

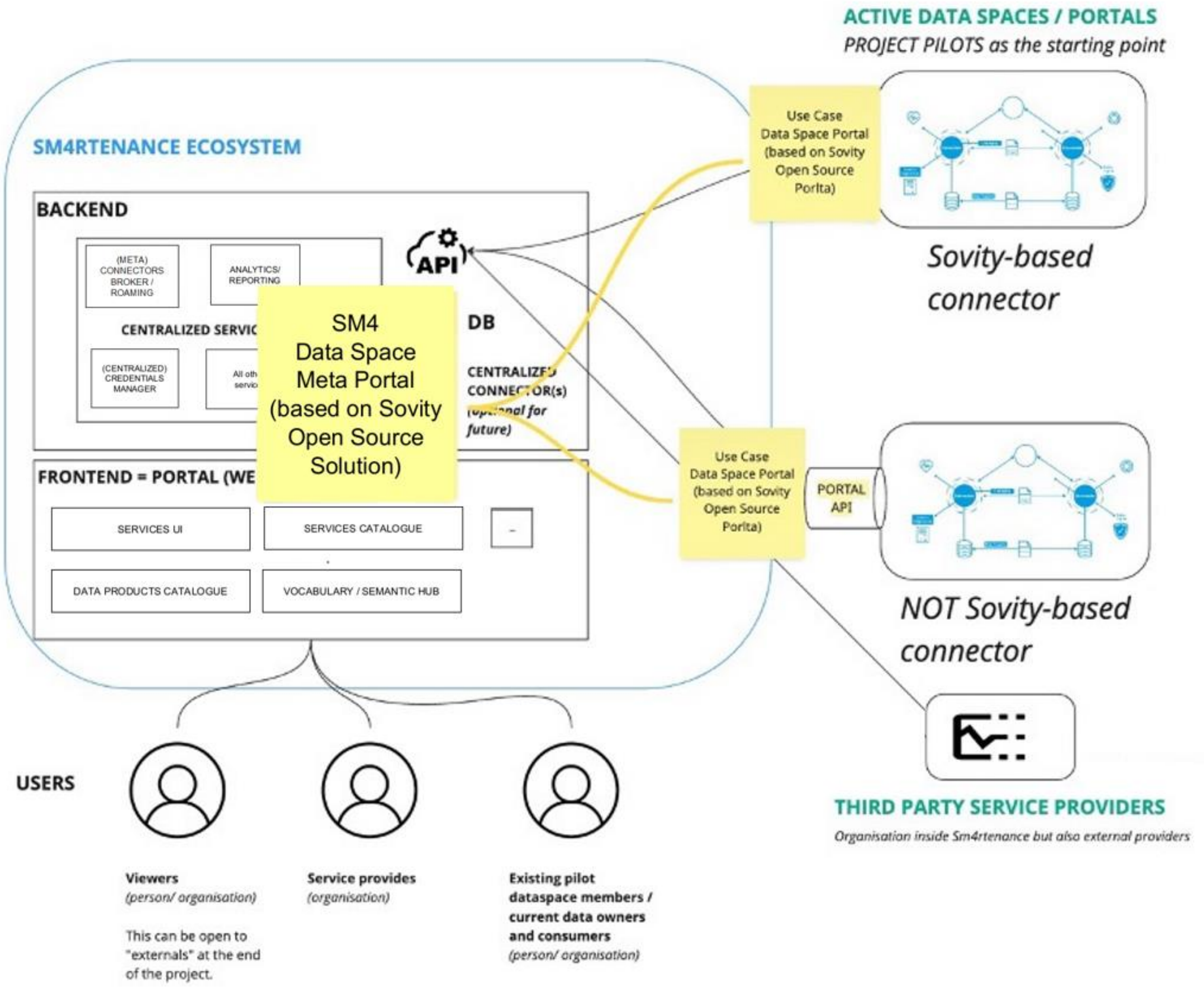

Figure 39. Adoption of the Sovity Data Space portal.

For each individual pilot/use case, the Data Space owners will be able to activate a management portal that tracks data transactions, catalogues, and other key information.
At the central level, a similar meta-portal will be set up, providing access to the information from the individual portals. Appropriate restrictions on shared information will be implemented according to the specific needs of each use case.
For Data Spaces connected to the project that do not use a Sovity-based connector, portal APIs will be provided to ensure the solution remains scalable and versatile, without compromising the integrity and autonomy of local Data Spaces.

8 Conclusion

The SM4RTENANCE initiative represents a significant step towards the harmonization and federation of Data Spaces in the manufacturing sector. Through a structured approach aligned with the DSSC Blueprint and common

EU standards, the project has successfully identified key building blocks and governance principles necessary for achieving interoperability, security, and trust in data sharing.

One of the critical challenges addressed by SM4RTENANCE is the fragmentation of existing Data Space models, which often struggle with interoperability due to varying architectures, governance models, and standards. The initiative seeks to establish a unified and scalable approach that facilitates seamless data exchange across different industrial ecosystems, leveraging on open standards and federated governance frameworks. This ensures that manufacturers, suppliers, and service providers can collaborate efficiently while maintaining control over their data assets.

Furthermore, SM4RTENANCE has placed a strong emphasis on compliance with legal and regulatory frameworks, ensuring that data governance principles align with the European Data Governance Act and the Gaia-X principles. The development of a structured governance model supports transparency, accountability, and equitable data-sharing agreements among stakeholders. The integration of trust and identity management mechanisms, such as Decentralized Identifiers (DIDs) and Verifiable Credentials, further strengthens security and reliability within the ecosystem.

As an enabler of the federation of Data Spaces, SM4RTENANCE will play a crucial role in bridging diverse industrial data ecosystems and aligning them under a common governance and interoperability framework. The initiative will incentivize collaborative efforts between different Data Space participants through the seamless integration of information across industries, reducing data silos and enhancing data-driven decision-making. The initiative provides a reference model that allows various Data Spaces to interoperate while preserving data sovereignty and compliance with industry regulations. This federation is not only set to benefit individual enterprises but also to strengthen the resilience and competitiveness of the broader European manufacturing sector.

The implementation of the SM4RTENANCE Data Space services, as outlined in this deliverable, provides a robust foundation for fostering innovation and efficiency in the manufacturing domain. The creation of a standardized and interoperable framework, will enable businesses to leverage digital transformation opportunities, optimize resource utilization, and enhance operational resilience. Additionally, the emphasis on a federated approach ensures that the benefits of data sharing extend beyond individual enterprises, contributing to the broader vision of a European data economy.

Looking ahead, the next phase of SM4RTENANCE will focus on the practical deployment of the proposed architecture, validating its effectiveness in real-world scenarios. Continuous collaboration with industry partners, regulatory bodies, and technology providers will be essential to refining and scaling the framework. Thus, SM4RTENANCE will accelerate the adoption of data-driven decision-making in manufacturing, paving the way for a more interconnected, efficient, and competitive industrial landscape.

In conclusion, SM4RTENANCE stands as a pioneering initiative that bridges existing gaps in the Data Space ecosystem while cultivating trust, interoperability, and governance. Its contributions lay a strong foundation for future advancements in data sharing, ensuring that European manufacturing remains at the forefront of digital innovation.