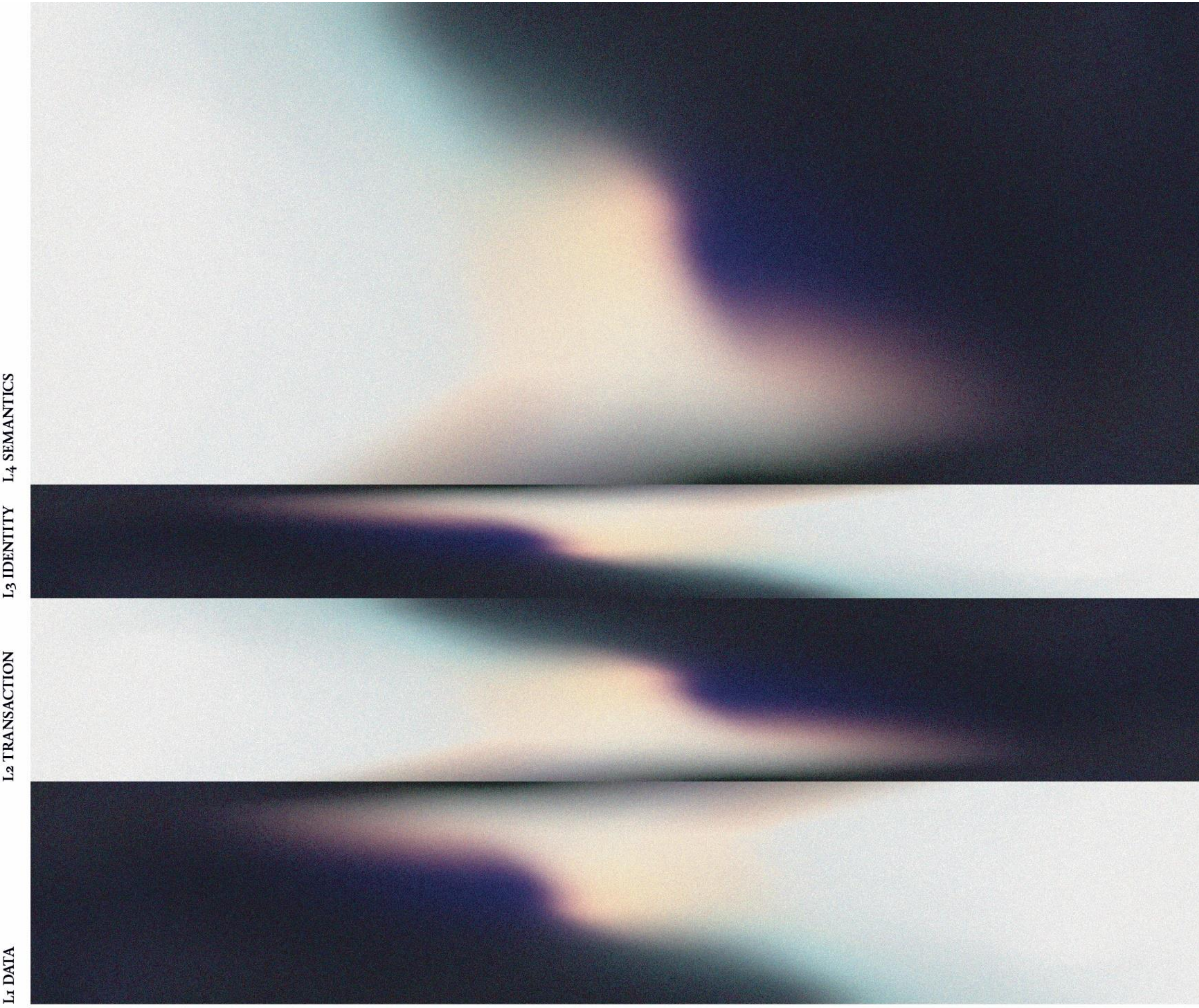


February, 2025

Whitepaper:

Ouranos Ecosystem Dataspaces Reference Architecture Model

Ministry of Economy, Trade and Industry, Japan;
Digital Architecture Design Center, Information-technology Promotion Agency, Japan

METI
Ministry of Economy, Trade and Industry

Digital Architecture
Design Center

Whitepaper:

Ouranos Ecosystem Dataspaces

Reference Architecture Model (ODS-RAM V1)

Annex A. Building-block Portfolio

Annex B. Context Catalog

February 28, 2025

Table of Contents

01 Introduction

1.1 Purpose and significance

This document serves as a *reference*, presenting the technical paradigm, including the hierarchical structure model of dataspaces, and future perspectives for participants in the **Ouranos Ecosystem Dataspaces (hereinafter referred to as "ODS")**—dataspaces promoted by the Ouranos Ecosystem Initiative.

The **Ouranos Ecosystem** is an ecosystem that creates value through new industry collaboration by developing and providing business-digital collaborative domains that connect companies, with digitalization as the enabler. Currently, industry, academia, and government come together to develop collaborative domains related to business-to-business relationships such as commercial distribution (business transactions and contracts), financial distribution (finance and settlement), and logistics (goods), promoting digital transformation across the entire industry and innovation across business and digital layers. This initiative, known as the **Ouranos Ecosystem Initiatives**, aims to realize the Ouranos Ecosystem.

This document aims to provide an open opportunity for constructing service-driven dataspaces to address societal issues and create value within the Ouranos Ecosystem by establishing a technical paradigm for future system implementations, fostering the participation of various entities and ensuring interoperability. The protocol specifications designed and developed based upon this document will ensure **Data Free Flow with Trust (hereinafter referred to as "DFFT"[1])** and therefore to form a common paradigm in enterprise data interoperability.

1.2 Readers and expected actions

This document targets a broad spectrum of domestic and foreign industries that support the Ouranos Ecosystem Initiative, particularly those responsible for designing architectures for data interoperability within the enterprise domain. The primary reader includes individuals responsible for design and development in corporate development and data management departments, as well as

[1] The concept aims to promote the free flow of data while ensuring trust in privacy, security, and intellectual property rights. Digital Agency. DFFT. https://www.digital.go.jp/en/policies/dfft

those in research institutions. Readers should possess knowledge of technical and business development related to data management, which is essential for understanding a *dataspace*.

This document plays a role as a meta-architecture for designing new architectures or evaluating the strengths and weaknesses of existing architectures for data interoperability across companies, industries, and national borders in the industrial domain. Introductory guidance and knowledge stacks for participants in dataspaces, including practitioners and planners in business divisions of companies, as well as government agencies and other industrial sectors, will be developed and released sequentially from FY2025 onward.

1.3 Scope

This document covers dataspaces, a key pillar of the Ouranos Ecosystem Initiative, and focuses on the following three topics:
*Note that the comprehensive overview of activities, strategies, use cases, and community building related to the Ouranos Ecosystem Initiative falls outside the scope of this document; these aspects will be disclosed in the future.

(1) **Ouranos Ecosystem Dataspaces Reference Architecture Model (ODS-RAM)**

Ouranos Ecosystem Dataspaces Reference Architecture Model (hereinafter referred to as "ODS-RAM") is a service-oriented architecture model designed to expedite the societal implementation of dataspaces within the industry. While maintaining a certain level of logical compatibility with the **International Dataspaces Reference Architecture Model (hereinafter referred to as "IDS-RAM")**[2], this document presents a technical paradigm that **allows for more flexible adaptation to the characteristics of industry and market structures, and commercial practices.**

The ODS-RAM encompasses a technology-agnostic specification and other conceptual levels, structured into four loosely coupled *Layers* and four *Perspectives*, each with corresponding roles, protocols, and service models. Chapter 3 and 4 provide detailed coverage of these components. **Note that the ODS-RAM serves as a reference design at this moment and therefore does not impose any binding business/technical requirements upon each dataspace participant's initiatives nor individual use cases.** It is advisable for dataspace participants to conduct a gap analysis using this model to implement functions that align with each dataspace characteristics and maturity.

[2] International Data Spaces Association. International Data Spaces Reference Architecture Model 4.

Note that the ODS-RAM presented in this document is version 1.0 (V1) and is anticipated to undergo agile updates through ongoing discussions and dialogues with industry and academia in the future.

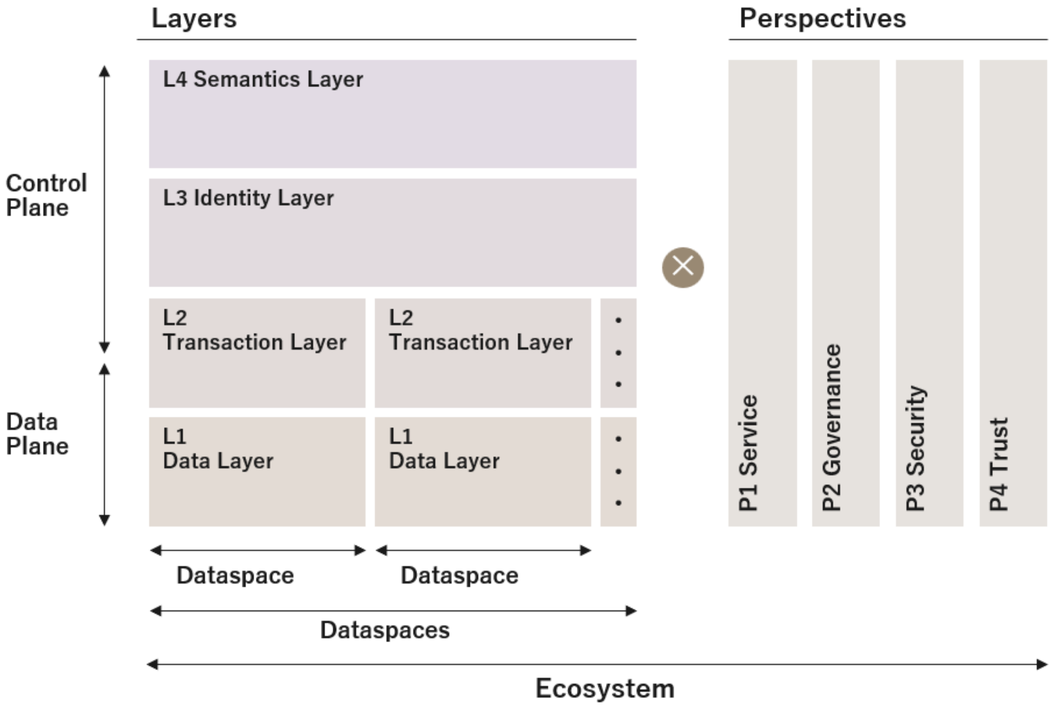


Figure1 Layer-Perspective Relationships in the ODS-RAM (V1)

(2) Building-Block Portfolio

Building-Block Portfolio is an open-source software specification currently available as a reference implementation of the ODS Protocol. Building-Block Portfolio is covered in Annex A.

(3) Context Catalog

Context Catalog is a collection of case studies on the design of the ODS-RAM (V1), where simulations of data interoperability and utilization were conducted in parallel with business development to establish a variety of dataspaces and abstract the necessary functions for each. This document presents the current information and future perspectives on the ODS-RAM (V1) design. Context Catalog is covered in Annex B.

This document is positioned as a *white paper*. **The ODS-RAM per se will be updated as needed based on industry trends from FY2025 onward.** Concurrently, protocol specifications, guidebooks etc., as more concrete documents, will be designed and developed through demonstrations that encompass multiple business requirements. These documents will be released under industry consensus and updated as needed.

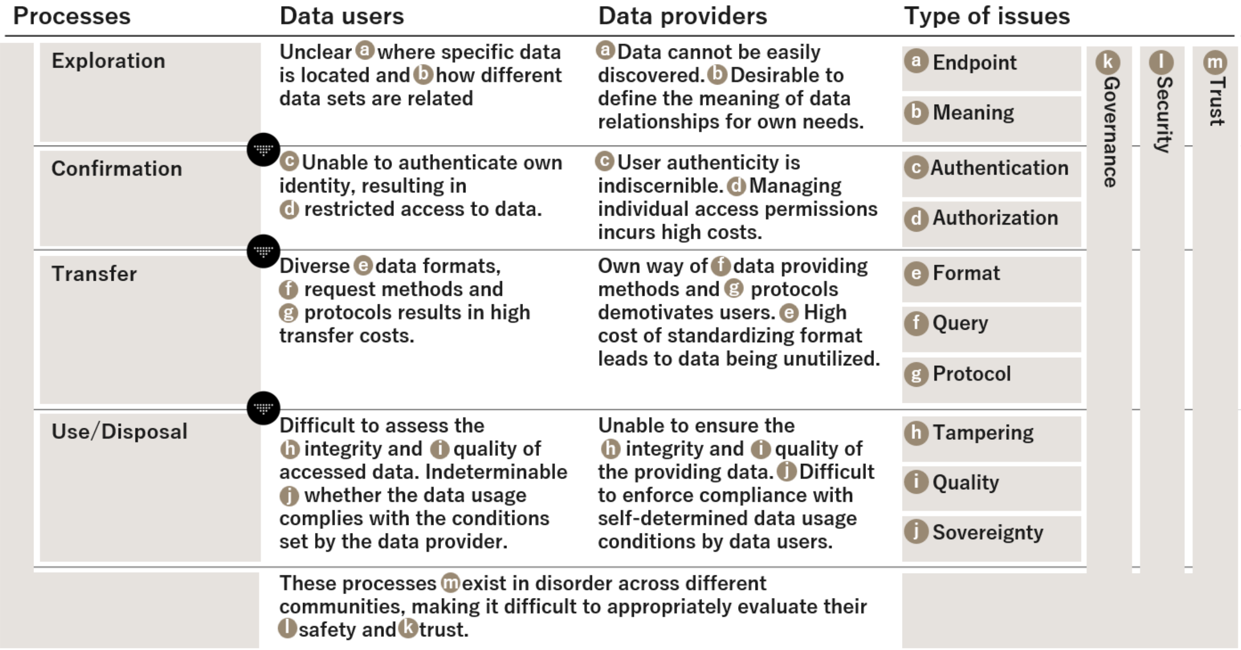
02 Ouranos Ecosystem Dataspaces

2.1 Structural issues

Numerous challenges hinder the DFFT across companies, industries, and nations. These challenges stem from a combination of historical path dependency and pluralistic/multi-layered issues, including the absence of a unified design concept for **data interoperability and utilization,** divergence of business operations from required standards, technical incompatibility with business requirements demanded by the industry and market, and the lack of rules and governance, etc.

The ODS addresses each of these issues, providing solutions for data interoperability and utilization in today's world, where intangibles increasingly become sources of added value and data/software form the foundation of competitiveness. Specifically, focusing on the process of data interoperation and utilization, data users and providers face the following ***13 issues*** across the five processes of data lifecycle: exploration, confirmation, transfer, use, and disposal.

Table1 13 issues in the five processes of data interoperation and utilization



Processes	Data users	Data providers	Type of issues			
Exploration	Unclear ⓐ where specific data is located and ⓑ how different data sets are related	ⓐ Data cannot be easily discovered. ⓑ Desirable to define the meaning of data relationships for own needs.	ⓐ Endpoint ⓑ Meaning	ⓚ Governance	ⓛ Security	ⓜ Trust
Confirmation	ⓒ Unable to authenticate own identity, resulting in ⓓ restricted access to data.	ⓒ User authenticity is indiscernible. ⓓ Managing individual access permissions incurs high costs.	ⓒ Authentication ⓓ Authorization			
Transfer	Diverse ⓔ data formats, ⓕ request methods and ⓖ protocols results in high transfer costs.	Own way of ⓕ data providing methods and ⓖ protocols demotivates users. ⓔ High cost of standardizing format leads to data being unutilized.	ⓔ Format ⓕ Query ⓖ Protocol			
Use/Disposal	Difficult to assess the ⓗ integrity and ⓘ quality of accessed data. Indeterminable ⓙ whether the data usage complies with the conditions set by the data provider.	Unable to ensure the ⓗ integrity and ⓘ quality of the providing data. ⓙ Difficult to enforce compliance with self-determined data usage conditions by data users.	ⓗ Tampering ⓘ Quality ⓙ Sovereignty			
	These processes ⓜ exist in disorder across different communities, making it difficult to appropriately evaluate their ⓛ safety and ⓚ trust.					

The ODS aims to address these 13 issues and promote DFFT based on the following principles.

2.2 Principles

The ODS is constitute of *seven principles*: underlying dataspace principles[3]—***decentralized ecosystem with data sovereignty***, ***common policies and rules defined by governance frameworks*** and ***secure and trustworthy data transactions***—and the extra—***semantic interoperability and machine/AI readability***, ***service diversity and collaborative domains***, ***democratic and open communities***, and ***simple and practical problem solving***.

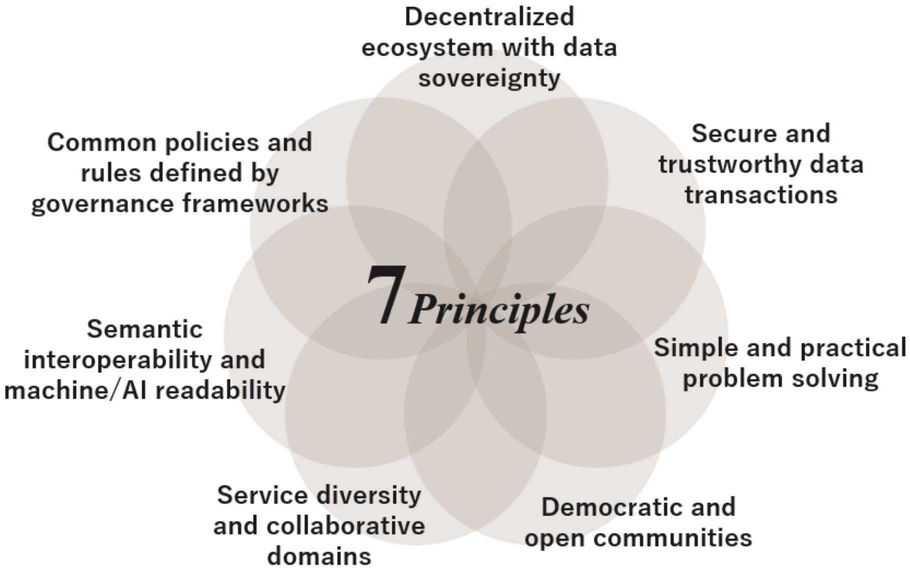

Decentralized ecosystem with data sovereignty
Secure and trustworthy data transactions
Common policies and rules defined by governance frameworks
7 Principles
Semantic interoperability and machine/AI readability
Simple and practical problem solving
Service diversity and collaborative domains
Democratic and open communities

Figure2 Seven Principles of Ouranos Ecosystem Dataspaces

2.2.1 Decentralized Ecosystem with Data Sovereignty

The ODS will create a decentralized ecosystem with data sovereignty. Amidst the global trend shifts in the source of added value from tangible to intangible assets, the role of *software* and *data* is increasing in importance at an accelerating pace. The development of semiconductors and sensors has connected software from the cyberspace to the physical space, and the advancement of micro-electromechanical systems, networks, and communications has extended the influence of information technology into operational technology.

[3] Defined by IOFDS (International Open Forum on Data Society) as follows:
"Data Space" is a decentralized ecosystem with common policy and rules defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty.

With the development of middleware, including computing and AI, software—which until now could only handle **structured data** (data organized in tabular form)—is beginning to engulf **unstructured data** such as documents, images, videos, sounds, and drawings.

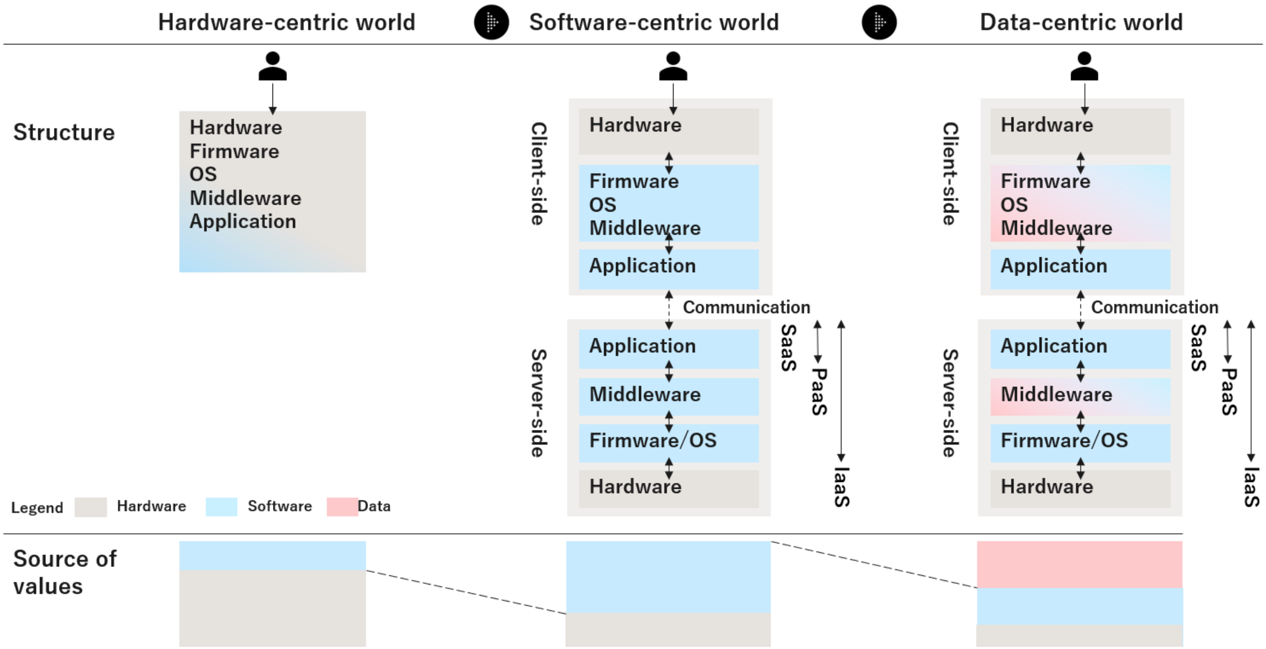


Figure3 Shift in Sources of Value from the Era of Tangible Assets to Intangible Assets

In this software-driven era, where the utilization of both structured and unstructured data leads to competitive advantage, companies can no longer differentiate themselves merely by using data freely available on the Internet. The ability to leverage AI and the computational processing power that drives it to utilize **enterprise data**—which has traditionally been stored within the company—will be a key determinant of competitiveness in the transition from a hardware-centric world to a software-centric world.

On the other hand, since the performance of enterprise data utilization depends on the company's capabilities, companies are not necessarily able to extract maximum added value, inducing activities aimed at expanding the ecosystem based on data through collaboration with partners in various fields. As the need for interoperation and utilization of enterprise data across companies and industries grows, such as when data needs to be aggregated to solve specific issues, potential risks and concerns become increasingly significant—well exemplified by the concentration of enterprise data in a few platform companies or unintended access by competitors. These risks and the associated caution act as barriers to the open use of enterprise data outside the company. The environment for securely providing enterprise data, a source of a company's competitive edge, remains insufficient.

To tackle with these problems, the ODS ensures **Data Sovereignty**[4], which entails self-determination regarding the conditions of storage and use that shall apply when granting permission for data use, maximizing the added value of companies and addressing higher-level societal issues with data at the core. Maintaining sovereignty over the data, even when data storage is managed by intermediaries such as platform companies, enables data providers taking the initiative in transforming business models and, ultimately, industrial structures, by using data. The ODS builds such a decentralized ecosystem characterized by an environment of open and fair coexistence.

2.2.2 Common Policies and Rules Through a Governance Framework

The ODS establishes common policy and rules by a governance framework. Dataspace is an ecosystem that is constructed in a pluralistic/multi-layered manner, spanning across companies, industries, and nations. Although the characteristics and maturity level of each dataspace differ, it is difficult to ensure interoperability unless the basic structure, mechanisms, procedures, and management methods are clearly defined as common policies and rules.

While ensuring interoperability, the ODS **designs and enforces appropriate incentives, policies and rules** for various requirements for data interoperation and utilization: building trust, improving cost efficiency by enhancing data transfer, compliance, and evaluating appropriate data quality, etc. The governance framework should be set and updated at an appropriate level to achieve interoperability.

2.2.3 Secure and Trustworthy Data Transactions

The ODS is oriented toward secure and trustworthy data transactions to achieve DFFT across companies, industries, and nations.

In the context of cybersecurity, the emergence of new forms of supply chains that are dynamically configured across both cyber and physical spaces—due to advancements in semiconductors, sensors, networks, and communications—means that the origins of attacks will be widely dispersed throughout the highly interconnected supply chain. This increases the opportunities for attackers to

[4] Note that no international nor standard agreement on the definition of data sovereignty exists at the moment. For example, IDS-RAM (v4.0) defines data sovereignty as follows: “Data Sovereignty is the ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset.” https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram -4/context-of-the-international-data-spaces/2_1_data-driven-business_ecosystems/2_2_data_sovereignty_as_a_key_capability

identify points of initiation for their attacks, while simultaneously expanding the scope that defenders must protect. As cyber and physical spaces interact, the potential damage from cyberattacks could be substantial. In such a highly networked and dynamically structured supply chain involving various entities, a single company faces limitations in ensuring cybersecurity on its own.

For this reason, the ODS aims to take security measures for data interoperation and utilization across various companies and industries based on **security by design,** a measure to ensure security from the planning and design stages. The ODS contributes to ensuring cyber security throughout the supply chain, including related companies and business partners, taking resilience of business activities into consideration.

2.2.4 Semantic Interoperability and Machine/AI Readability

(A) Semantic interoperability

The ODS ensures semantic interoperability. In data management, the process of standardizing technical specifications, such as interfaces among competing providers, into a single definition corresponds to semantic integration (unification of meaning). This process requires identifying the involved parties, establishing a framework, and examining multiple technical specifications to reach an agreement, which incurs significant costs in terms of time and resources. As the market continues to evolve despite the disarray of technical specifications, a certain level of confusion will persist due to differences in service definitions among providers. Among these disorganized specifications, the most highly regarded model will eventually emerge as the **dominant design** and become the standard. Once established, the standard will facilitate the horizontal division of labor in the market and promote the stabilization and advancement of the industry, leveraging the data effectively.

Currently widely used **database management systems** (hereinafter referred to as “DBMS”) cannot manage data until the schema (data structure) is strictly determined in advance. Furthermore, **data integration systems** that integrate multiple databases likewise do not provide services without semantic integration. This methodology of providing services on the premise of a schema is called **schema-first** (or schema-on-write). The schema-first methodology is a robust approach—once the schema is defined, standard data transfer becomes feasible. **This methodology is particularly effective in scenarios where there is an umbrella organization that is exclusive to a specific industry or where a schema can be quickly agreed upon as a collaborative domain.** In general, however, the process of determining a schema is both costly and time-consuming, and the costs associated with API modifications due to changes in data requirements are also significant. This rigidity of DBMS has been highlighted by Franklin et al. (2005) and Halevy et al. (2006), who first jointly proposed the concept of dataspaces.

To make services available even before semantic integration takes place, the ODS allows the variations in semantics and therefore complementarily adopts a **schema-flexible** (or schema-on-read) methodology, an approach that allows data to coexist while providing and understanding the apparent schema as needed. **Schema-flexible is a dynamic means of tagging metadata to data, depending on the nature of a dataspace, and transforming the data into a desired schema at the time of use.**

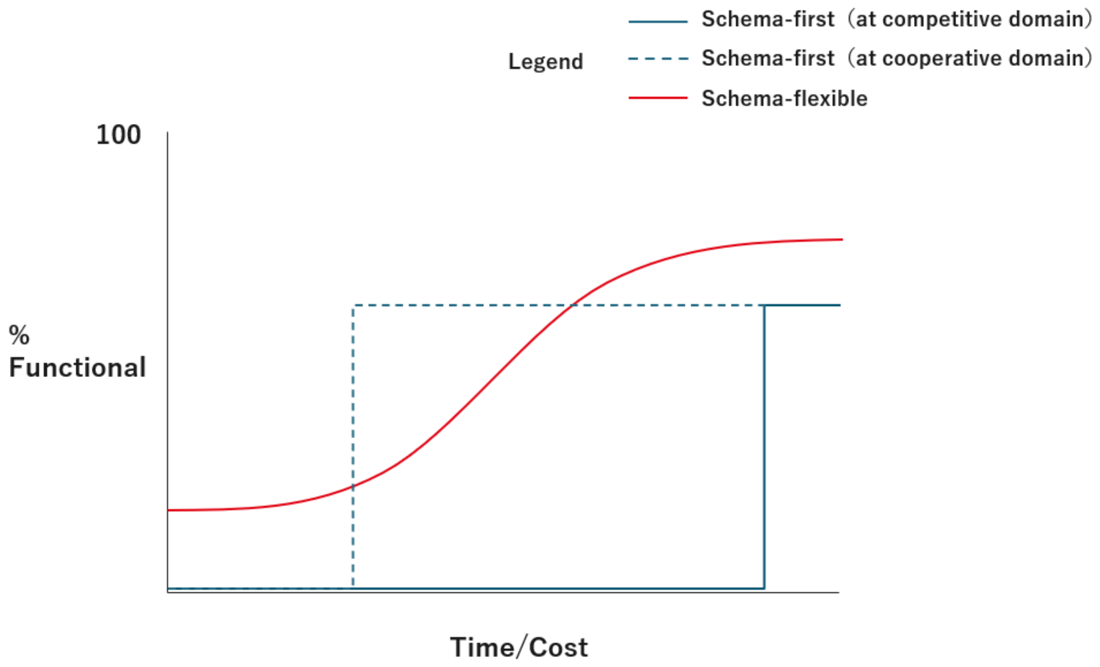


Figure4 Schema-flexible and Schema-first Time/Cost vs. Functional Efficiency

The ODS **facilitates a hybrid approach that combines schema-flexible and schema-first methodologies**, emphasizing the endpoint and meanings of data to achieve semantic interoperability across the ecosystem.

(B) Machine/AI readability

The ODS adopts semantic interoperability and embraces the concept of virtual data integration through a machine-readable network, allowing each data provider to retain their actual data. This ensures machine/AI readability across companies and industries, thereby strongly promoting enterprise data management in the age of artificial intelligence.

Not limited to digital services, in general, a service provider (Company A) understands the points of contact between itself and related businesses (Company B). When a service user requests a service from Company A that partially encompasses the scope of Company B, Company A mediates the connection with Company B for its service users. However, since Company A cannot delve into the specifics of the services provided by Company B, the service user is ultimately required to contact Company B directly. For instance, in the case of a railroad operator and a bus operator, the railroad operator may only indicate the direction of the bus stop without providing details about the bus operations at a station ticket gate. This shallow coordination between service operators diminishes the service experience and convenience for users, negatively impacting consumption behavior and economic activity. This issue mirrors a fundamental challenge in data management, where a single data integration system can aggregate data sets from various sources and unify interfaces but cannot support *all* relevant data in the world.

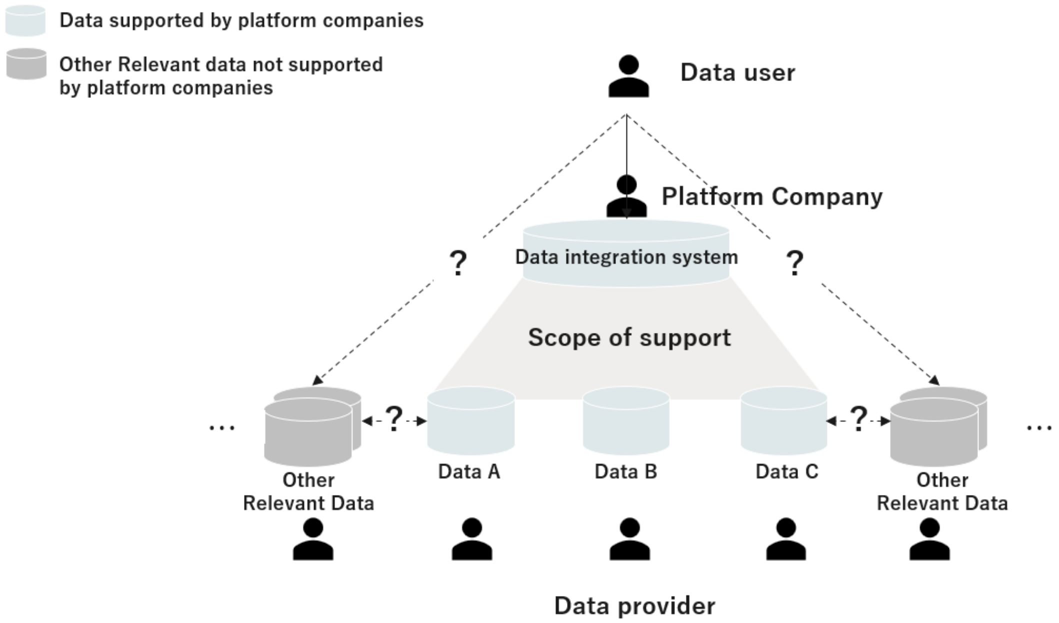


Figure5 "The scope-of-support chasm" of data integration systems

Empowering machines and AI to fully utilize enterprise data that does not exist on the Internet requires overcoming the "scope-of-support chasm" in light of technology and business operations. And no matter how large the scope of a platform company that supports various business domains, the problem will not be solved if there is a trade-off between scalability and operational costs. The situation here suggests the necessity for **distributed services.**

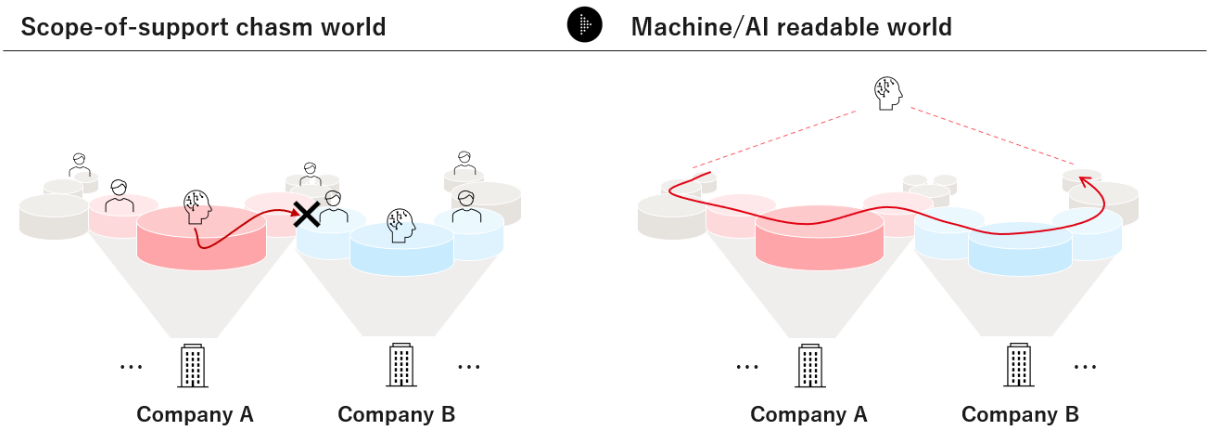


Figure6 Providing seamless service access from the user (machine and AI) perspective

Considering the Internet as a typical example of distributed services, when browsing articles on the web, viewers can navigate various sites by following web links without feeling constrained by the boundaries set by the website administrator—the data provider. In other words, based on the premise of data dispersion, allowing machines and AI to explore the datasets interconnected among businesses and utilize the necessary services and data under the appropriate authority eliminates the need for manual business given an economic rationality. In this context, the ODS will function as a **middleware infrastructure** for machines and AI, serving as the foundational framework that ensures data interoperability by design.

2.2.5 Service Diversity and Cooperative Domains

(A) Service diversity

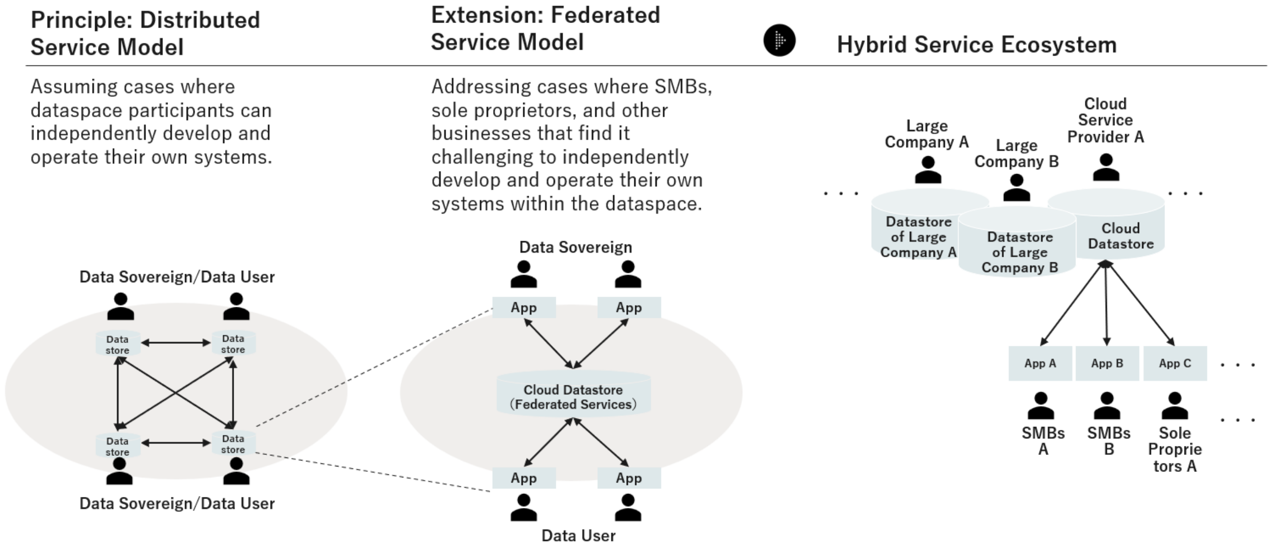
The ODS respects service diversity. Realizing a dataspace that addresses societal issues and creates added value across companies, industries, and nations, necessitates to broadly include data sovereign and users. A key to the broad inclusion is to **avoid architecture models that excessively limit the service interfaces of dataspace participants and to allow for a diversity of services, including existing ones**.

For example, if the service interface is an ERP package implemented by a large company, users can participate in the dataspace without migration insofar as developer modifies it to incorporate the necessary functions. Conversely, however, in markets and industries with a low implementation rate of ERP packages—particularly those involving many SMBs and sole proprietors integrated into the supply chain/value chain, the adoption of more affordable and diverse applications is preferred.

Furthermore, imposing various mandatory technical requirements, given the assumptions that in-house system administrators and outside application service providers can independently design, develop, implement, operate, and maintain all of them, creates barriers to entry to the dataspaces, such as lack of capability.

Given that the *characteristics* and *maturity* of a dataspace depend on actual demand and business practices, mandatory elements in architectural models and protocols that only some service users and administrators can practically handle, may raise the issue of slow or halted penetration in the cross-section of social implementation. It is therefore essential to design the ODS with a consideration for service diversity by default.

The ODS, in addition to the “**distributed service model**” which assumes dataspace participants with independent capability to develop and operate the system, adopts the “**federated service model**” to where multiple dataspace participants are federated with service providers of core technologies, thereby accommodating participants who may struggle to develop and operate their own systems. **The *hybrid service ecosystem* approaches of the ODS allows the architecture model to be more flexible with a variety of service interfaces while ensuring data sovereignty.**


Principle: Distributed Service Model

Assuming cases where dataspace participants can independently develop and operate their own systems.

Extension: Federated Service Model

Addressing cases where SMBs, sole proprietors, and other businesses that find it challenging to independently develop and operate their own systems within the dataspace.

Hybrid Service Ecosystem

Figure7 Hybrid service ecosystem of the ODS

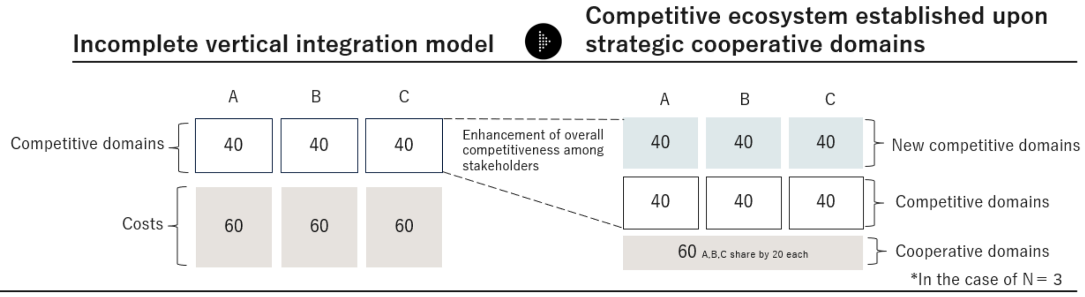
(B) Cooperative domains

The strategic development of cross-industrial/sectorial **cooperative domains** is essential to achieve service diversity. The concept stems from the economic perspectives of both the *demand creation cycle*, where the added value of a service unearths latent demand, and the *supply cost improvement* *cycle*, where an increase in service distribution volume leads to price reductions within the overall ecosystem. Particularly in emerging markets, companies may perceive everything as sources of competitiveness with the intention of differentiation. This mindset can lead them to independently implement initiatives, even in areas where cost reductions could be achieved through collaboration with stakeholders, diminishing the internal resources that should be invested in their own competitive domains. This behavior results in each company offering similar services, leading to the emergence of an **incomplete vertical integration model**, which serves as a barrier to monetization.

Specifically, the waste of investment cash flow (hereinafter referred to as “investment C/F”) due to overlapping investments in the demand creation cycle, along with the pressure on operating cash flow (hereinafter referred to as “operating C/F”) caused by common cost burdens in the supply cost improvement cycle, leads to incomplete vertical integration. Numerous examples exist where incomplete vertical integration erodes the competitiveness of all players who initially aimed for diversity.

In promoting ODS, a waste of investment C/F and an unnecessary pressure on operating C/F should be **strategically separated out as cooperative domains from the perspective of business economics**, whereby sharing costs across the industry and redirecting investment to more competitive and high-value-added domains. The establishment of cooperative domains by industry, government, and academia will lead to the promotion of open innovation through the optimal distribution of common supply costs, as well as the fostering of a healthy competitive climate through the selection of cores and non-cores in the **competitive domain,** driving investment efficiency and the horizontal specialization. Since the boundary between the competitive domain and the cooperative domain is business environment- and time-malleable, a strategic decision of the cooperative domain made in units and periods appropriate for each stakeholder is preferable to that in a uniform and fixed delimitation.

Table2 Incomplete vertical integration models v. Competitive ecosystem established upon strategic cooperative domains


Incomplete vertical integration model
Competitive ecosystem established upon strategic cooperative domains
A
B
C
Competitive domains
40
40
40
Costs
60
60
60
Enhancement of overall competitiveness among stakeholders
A
B
C
40
40
40
New competitive domains
40
40
40
Competitive domains
60 A,B,C share by 20 each
Cooperative domains
*In the case of N = 3

Demand creation cycle	**Overlapping investments:** a waste of investment C/F	**Selection of cores and non-cores in the competitive domain:** a healthy competitive climate, efficient investment
Supply cost improvement cycle	**Common cost burdens:** unnecessary pressure on operating C/F	**Establishment of cooperative domains:** sharing costs across the industry and redirecting investment to more competitive and high-value-added domains

2.2.6 Democratic and open community

The ODS champions a **democratic and open community.** Dataspaces serves as a democratic and open community, where participants are free to participate or secede whenever necessary, while fulfilling various roles under the equal dichotomy of data sovereignty vis-à-vis data user.

The ODS does not simply replicate the existing vertically integrated industrial structure. Instead, the ODS aims to establish a **distributed industrial network** where data sovereigns and users engage in data utilization on equal terms. A distributed industry network enables the open community to swiftly adapt its business practices in the software/data era in response to the evolving needs and environmental changes of society and end consumers.

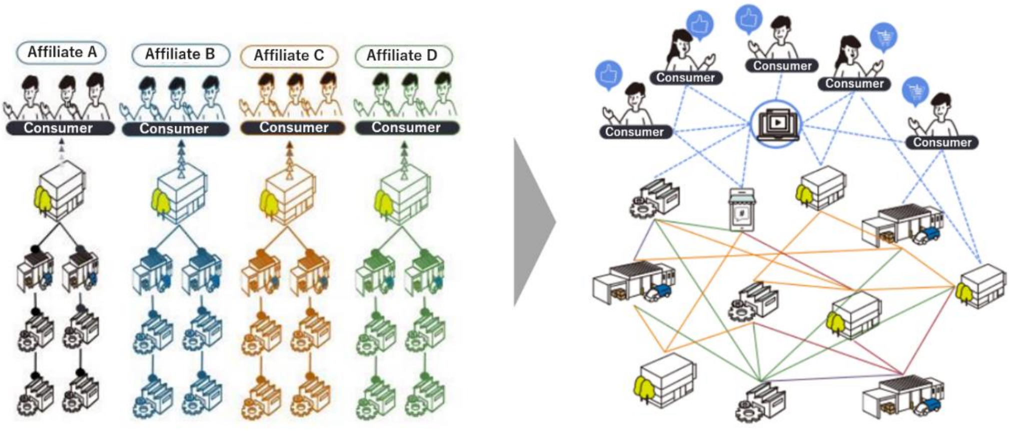


Figure8 Transition to a distributed industrial network [5]

[5] Information-technology Promotion Agency, Japan., Ministry of Economy, Trade and Industry. (2024) p.1

2.2.7 Simple and Practical Problem Solving

The ODS provides **simple and practical problem solving** to facilitate rapid integration into society. Since dataspaces consist of various stakeholders with differing principles of action, pursuing their generalizability without caution may lead to technological, organizational, and business complexities. While the ODS envisions an abstract top-down architecture, it remains focused on addressing societal challenges and creating value, emphasizing strategically scalable simplicity and practical applicability to avoid turning a means into an end in agile business and system development.

Furthermore, to achieve simplicity and practicality, it is crucial that anyone can easily participate in the dataspace, including a positive **User Experience (UX)** for participants by design. The ODS will begin by implementing core components as **opensource software (OSS)** through **reference implementations.** Additionally, the ODS will actively publish development environments such as **Software Development Kits (SDKs)**, along with documentation and knowledge stacks for participants, progressively making resources available starting in FY2025.

03 Architecture

3.1 Structure of the reference architecture model

The ODS-RAM is an **architecture model focused on the service life cycle to expedite the social implementation of dataspaces within the industrial sector**, consisting of **four layers** and **four perspectives** to reflect the seven principles of the ODS.

（1） **Layers**

Layers separate dataspaces into logical hierarchies according to their functional purpose. The ODS consists of four layers: ***Data***, ***Transaction***, ***Identity***, and ***Semantics***. While the Transaction and Data Layers are expected to have defined closed boundaries for each dataspace, Identity and Semantics Layers are designed to function across multiple dataspaces.

Additionally, within each layer of the dataspace, the concept of a ***control plane*** and a ***data plane*** is introduced to abstractly represent the locations where data interoperation processes occur. The control plane governs how data is transferred and the functions required to implement that control, while the data plane is responsible for the actual transfer of data. The control plane corresponds to the Semantics, Identity, and Transaction Layer, whereas the data plane to Data and Transaction Layer. Transaction Layer is expected to function as an intermediary layer between the control plane and the data plane.

（2） **Perspectives**

Perspectives represent logical viewpoints that serve a cross-cutting function in the ecosystem encompassing the entire dataspaces. The ODS consists of four perspectives: ***Service***, ***Governance***, ***Security***, and ***Trust***.

Layers and perspectives of the ODS-RAM target each of the 13 issues of data interoperability and utilization with the relationships shown in Figure 9.

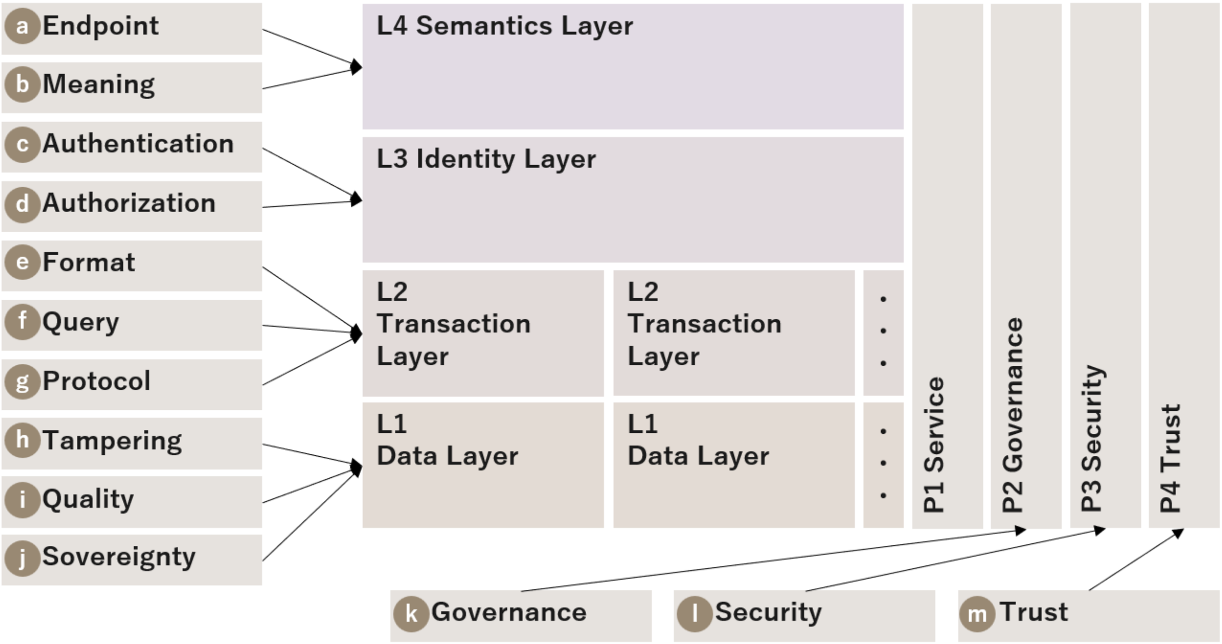
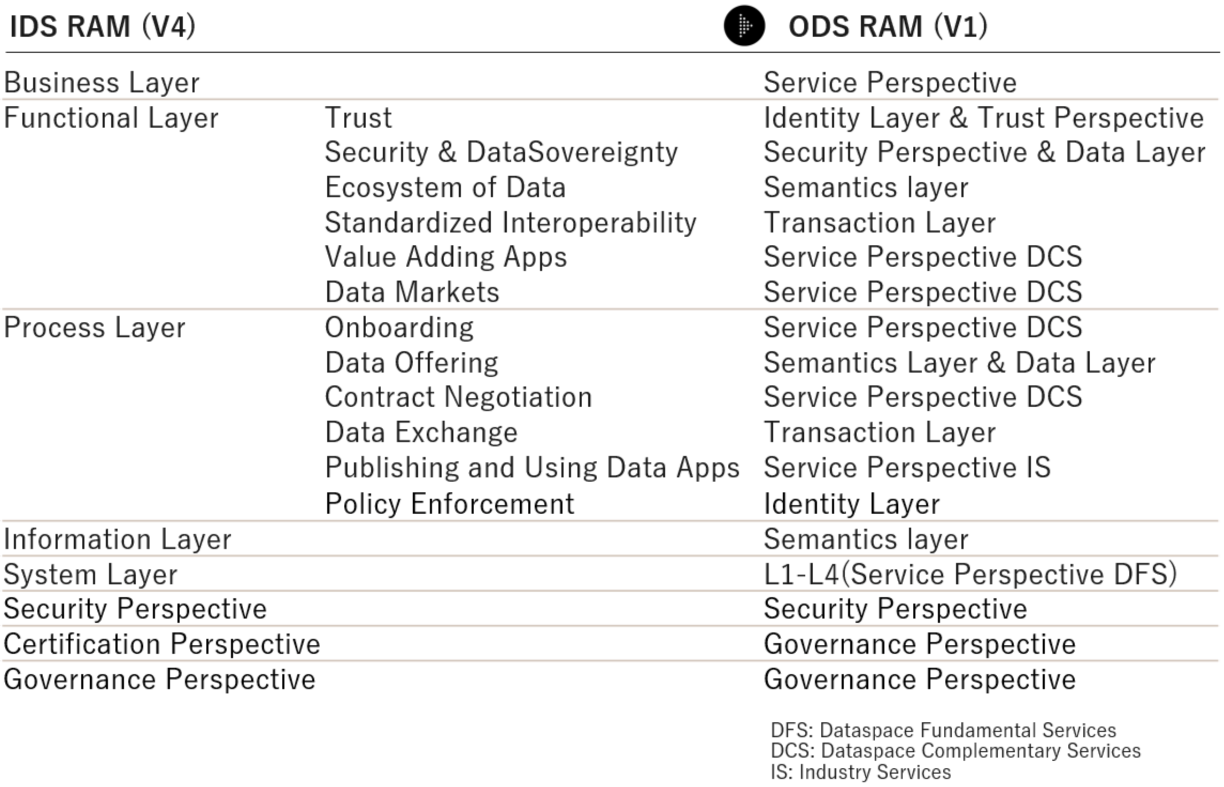


Figure9 Relationships of 13 issues and the ODS-RAM

The relationship between layers and perspectives presented in ODS-RAM and IDS-RAM is organized as follows. The actual interoperability based on logical compatibility will be discussed in future updates of the ODS-RAM.

Table3 Logical compatibility map for IDS RAM and ODS-RAM (assumed as of V1)



IDS RAM (V4)		ODS RAM (V1)
Business Layer		Service Perspective
Functional Layer	Trust	Identity Layer & Trust Perspective
	Security & DataSovereignty	Security Perspective & Data Layer
	Ecosystem of Data	Semantics layer
	Standardized Interoperability	Transaction Layer
	Value Adding Apps	Service Perspective DCS
	Data Markets	Service Perspective DCS
Process Layer	Onboarding	Service Perspective DCS
	Data Offering	Semantics Layer & Data Layer
	Contract Negotiation	Service Perspective DCS
	Data Exchange	Transaction Layer
	Publishing and Using Data Apps	Service Perspective IS
	Policy Enforcement	Identity Layer
Information Layer		Semantics layer
System Layer		L1-L4(Service Perspective DFS)
Security Perspective		Security Perspective
Certification Perspective		Governance Perspective
Governance Perspective		Governance Perspective

DFS: Dataspace Fundamental Services
DCS: Dataspace Complementary Services
IS: Industry Services

The Ouranos Ecosystem Initiative aims to **shift away from a tech-/seller-centric, product-out approach. The Initiative advances social implementation as a facet of business development while adopting a methodology to abstract individual requirements towards a scalable yet market-in strategy.** Moving forward, the ODS-RAM will pursue agile examination by generalizing the business requirements of various use cases with the goal of updating standard models that align with industrial demands.

3.2 Layers

In the ODS-RAM, each layer operates independently and functions in a loosely coupled manner to facilitate a series of data interoperation. In other words, the ODS layer possesses ***detachability***, allowing those who construct a dataspace to selectively determine the necessary number of layers based on the nature and characteristics of that dataspace.

For instance, if meanings and endpoints of datasets in a given dataspace are obvious, the implementation of the Semantics layer is not necessarily required. If a dataspace is established within a relatively limited community where participants' identities can be physically verified, simpler methods can ensure authentication and authorization, making the implementation of the Identity layer not necessarily mandatory. **Flexibility according to each use case is the cornerstone of the**

ODS-RAM where backward compatible options are available to choose post-hoc opt-in as needed in consideration of maturity of the dataspace. The following sections provide details on the functionality of each of the four layers.

3.2.1 Data Layer (L1)

Data Layer (hereinafter referred to as “L1”) resolves the issues of ***sovereignty***, ***tampering***, and ***quality*** related to data. L1 requires functions for data sovereignty exercised by the data sovereign and for data handling that guarantees data integrity and quality.

The data sovereignty exercised by data sovereigns does not necessarily require technical implementation for self-determination regarding the conditions for data storage and usage that should apply when granting permission for data use. Instead, **opportunities for self-determination concerning data sovereignty should be provided within the scope defined by contracts etc., ensuring that such determinations are appropriately reflected in practice**.

Rather than establishing a uniform standard, ensuring integrity and quality by technical or operational means according to the characteristics of the data transfer is preferable since the attributes of data integrity and quality vary across different dataspaces with distinct scopes. In this context, **L1 does not impose requirements on the integrity and quality of the data itself but instead requires the methods for evaluating and calculating these attributes and its results be provided in a manner accessible to participants in the dataspace**.

3.2.2 Transaction Layer (L2)

Transaction Layer (hereafter referred to as “L2”) resolves the issue of ***format***, ***query***, and ***protocol***. L2 requires functions for controlling **the process of transferring data between providers and consumers by a method that is independent of the format of the data (structured, semi-structured, unstructured, etc.) and of the request or method (synchronous, asynchronous, etc.). L2 requires the ability to control the process of transferring data between providers and consumers**.

L2 serves as a node for the control plane and data plane, facilitating the data transfer process control according to the results of endpoint and meaning resolution, at the same time mediating authentication, authorization, data sovereignty, integrity and quality resolutions.

3.2.3 Identity Layer (L3)

Identity Layer (hereafter referred to as "L3") resolves the issue of **authentication** and **authorization**. L3 requires the exchange of **credentials** in a verifiable form to achieve the necessary level of authentication and authorization among dataspace participants.

L3 requires cross-sectional data mobility with the necessary level of confidentiality by implementing access control based on the data storage and usage conditions self-determined by data sovereigns.

L3 ensures the authentication of participants in dataspaces, including level assessments, thereby providing flexible and feasible authentication that aligns with the trustworthiness requirements of data sovereigns and data users within the target dataspace.

3.2.4 Semantics Layer (L4)

Semantics Layer (hereinafter referred to as "L4") is resolves the issue of ***endpoint*** and ***meaning***.

L4 requires the exchange of **metadata** in an accessible form to achieve semantics interoperability among dataspace participants. Metadata is divided into either endpoint-related or meaning-related. Endpoint-related metadata is necessary to access data or services in the first place, while meaning-related to use the data or service in a unique and accessible form with respect to the meaning of the information (input/output data).

L4 **ensures interoperability in L2 data transfer, even if different organizations, industries, or dataspaces hold data with different schemas and attribute information,** by using metadata to semantically and syntactically transform the actual data held by the data sovereign before and by resolving endpoint. L4 serves as a solution for adjusting schemas in an equitable manner during connections between dataspaces, applicable not only in distributed service models but also in federated service models where industry data models are developed on a schema-first basis.

3.3 Perspective

In the ODS-RAM, **each perspective is interconnected and affects all aspects of the data interoperability and utilization.**

3.3.1 Service Perspective (P1)

Principles

The service perspective bridges the business domain and technical domain that encompasses functions and operations. In the ODS-RAM, services are classified into three categories: ***Dataspace Fundamental***, ***Dataspace Complementary***, and ***Industry***.

(1) **Dataspace Fundamental Service**

Dataspace Fundamental Service (hereinafter referred to as “DFS”) provides technical implementations of the functions required for meeting the requirements of the fundamental protocols specified in Chapter 4.

(2) **Dataspace Complementary Service**

Dataspace Complementary Service (hereinafter referred to as “DCS”) provides technical implementations of the functions required for meeting the requirements of the complementary protocols specified in Chapter 4.

(3) **Industry Service**

Industry Service (hereinafter referred to as “IS”) provides business applications, platforms, etc., specific to each industry and use case. Services provided by existing businesses domains may correspond to industry services.

The services in the ODS-RAM are organized as shown in Figure 10 (Service Map). Note that the service map is the **assumptions at this moment and therefore not exhaustive**; those that are particularly typical for DFS and DCS are defined in this section. **The service map is referenced when private sectors primarily provide each service on a competitive or cooperative basis. The technical specifications that need to be complied with to provide the services are presented in the Protocols, and the governance, trust and security concepts are presented in the P2 to P4.**

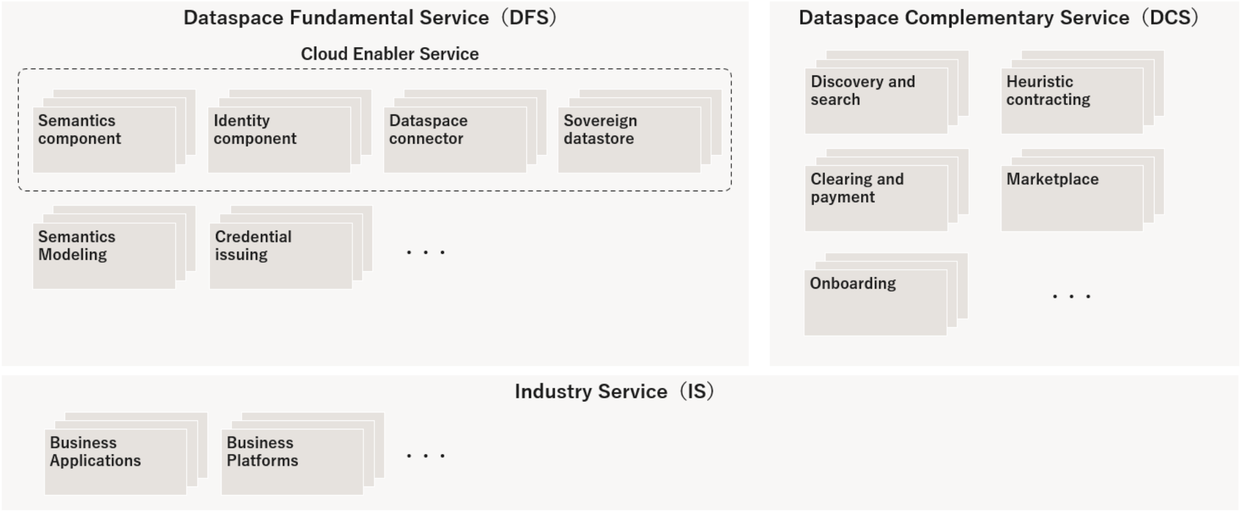


Figure10 Service Map

Dataspace Fundamental Service (DFS)

- **Cloud Enabler Service**

  Cloud enabler service provides core components that play a central role of the DFS in L1-L4, as cloud services (i.e., as-a-service). As to semantics component, identity component, dataspace connector, sovereign datastore, and other core components, the ODS allows third parties to provide these services within the scope of contractual relationships based on terms and conditions agreed to by users. DFS opens the door to participation in the dataspace even for those who cannot implement the technology in-house.

- **Semantics Modeling**

  Semantics Modeling service designs meta models published by semantics providers in L4 and assigns such models to data. The meta model may define the interface of the service, such as the **Semantic Aspect Meta Model (SAMM)**, or one in a tabular form, such as a schema.

- **Credential Issuing**

  Credential Issuing service provides issuance of credential in L3.

Dataspace Complementary Service (DCS)

- **Search**

  Dataspace discovery and search service provides functions for discovering and searching endpoints in L4.

- **Contracting**
  Heuristic contracting service provides the ability for both newly discovered service users and service providers in the dataspace to make new contracts electronically, either on their own or by a third-party service.

- **Clearing and Payment Service**
  Clearing and payment service provides clearing, payment, and billing functions to both service users and service providers in the dataspace, either on their own or by a third-party service

- **Buying and Selling**
  Marketplace service provides functions related to the buying and selling of data where a third party acts as an intermediary between a data sovereign and a data user, or data sovereign or data user on their own.

- **Onboarding**
  Dataspace onboarding service provides necessary support to prospective participants in the dataspace for their participation.

3.3.2 Governance Perspective (P2)

Principles

The governance perspective establishes common rules, policies, etc. to achieve specific objectives, and to manage, supervise, and operate across the ecosystem.

As a leading example of dataspace service governance, the Japanese government has established the "**Certification of Interoperable Data Infrastructure Management Entity**" (CIDIME) to promote the safe and proactive use of data among providers and users, while establishing an environment for consideration of corporate trade secrets, data sovereignty, and ensuring interoperability. The certification covers the entity that operates and manages systems for interoperating data across multiple stakeholders and meets the criteria for safety and reliability, business stability, and interoperability in addition to the certification criteria of the DX Certification[6], thereby externally guaranteeing a certain level of public interest of the entity in accordance with the law.

[6] DX Certification(certification based on Article 31 of the Act on the Facilitation of Information Processing) is a national certification initiative(as of February 2025) that certifies companies that are recognized as ready to promote Digital Transformation and meet the basic requirements specified in the Digital Governance Code, which summarizes what action business managers are required to take to accommodate how society is being transformed by digital technology.

In organizing the functions within the governance perspective, it is necessary to examine common rules and policies required at each layer from L1 to L4, including generally anticipated aspects such as **standardization** and **conformity assessment**. Discussions on the appropriate framework will take place from FY2025 onward, based on practical demonstrations and other considerations.

Unified Meta Identifier（UMI）

To promote efficient data interoperation and utilization, the establishment of a Unified Meta Identifier (hereinafter referred to as “UMI”) is essential as a common identifying rule across dataspaces. The UMI is formulated by abstracting the identifier systems that exist as individually optimized and heterogeneous within companies, industries, and other contexts. It serves as a crucial foundation for resolving issues related to compatibility, searchability, and semantic interoperability in data interoperation and utilization.

Information-technology Promotion Agency, Japan (IPA), for example, has been studying the **4D Spatiotemporal Identifier**[7] to uniquely identify the time-space on the earth as per a reproducible grid system using simple mathematical expressions when handling data related to position coordinates in real space. The 4D Spatiotemporal Identifier is being studied and compiled as a guideline, and its social implementation is in progress nationwide.

3.3.3 Security Perspective (P3)

The security perspective defines the security requirements and measures in the ecosystem as a whole or in parts. The functions in the Security Perspective will be studied and organized from FY2025 onward, while mapping the relationships among architectures by referring to the **Cyber/Physical Security Framework**[8] and other related documents.

3.3.4 Trust Perspective (P4)

The Trust Perspective defines the trust requirements and measures in the ecosystem as a whole or in parts. In terms of organizing functions within the Trust Perspective, studies and discussions from FY2025 onward will include concepts such as **Data Trust**, which pertains to the integrity of data in L1, **Data Trustworthiness**, which relates to the quality of data, and **Trust Anchor**, which serves as the basis for trust in L3.

[7] Information-technology Promotion Agency, et al. (2024).

[8] Ministry of Economy, Trade and Industry. (2019).

3.4 Roles

In the ODS, for the purpose of smooth collaboration that enables effective design and development without the need for experts in each technical field to understand the entire technical system, the core technical components required to participate in the dataspace are divided into three subcomponents from the perspectives of semantics, identity, and transactions, respectively: ***Semantics Component***, ***Identity Component***, and ***Dataspace Connector***. This classification serves as the basis for mapping roles.

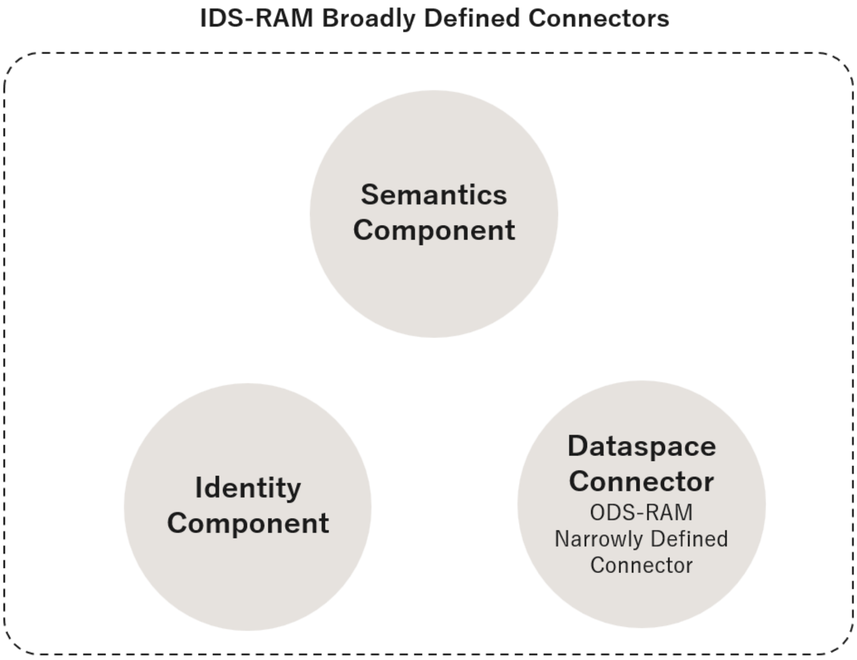

IDS-RAM Broadly Defined Connectors
Semantics Component
Identity Component
Dataspace Connector
ODS-RAM Narrowly Defined Connector

Figure11 Definition of Connector in the ODS-RAM

Based on these premises, Figure 12 shows the roles within the ODS-RAM.

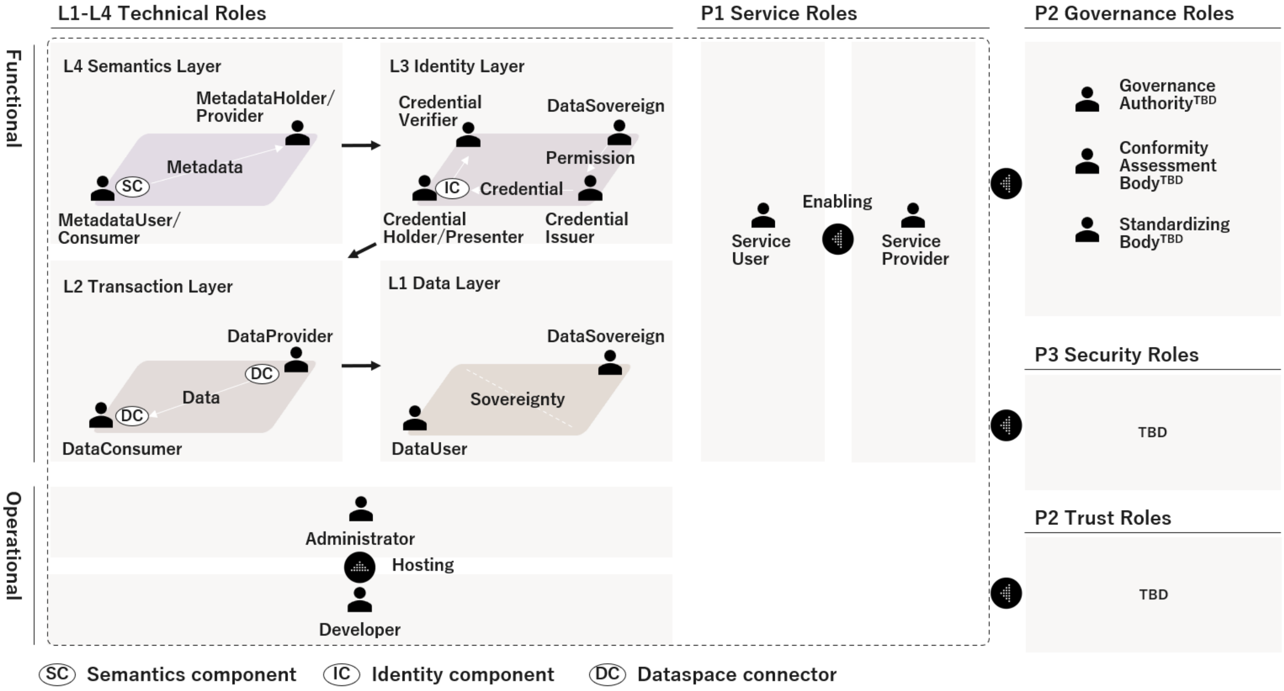


Figure12 Overview of roles in the ODS-RAM

Each role can be broadly classified into the following:

（1） **Service Roles**

Service Roles define the entities that provide and use services in the ODS when focusing on the P1.

（2） **Technical Roles**

Technical Roles define the entities that perform specific functions in the ODS when focusing on the Layers. Technical roles are further subdivided into ***functional*** and ***operational***.

（3） **Governance Roles**

Governance Roles define the entities that manage, supervise, and operate, etc., specific functions of the ecosystem when focused on the P2.

（4） **Security Roles**

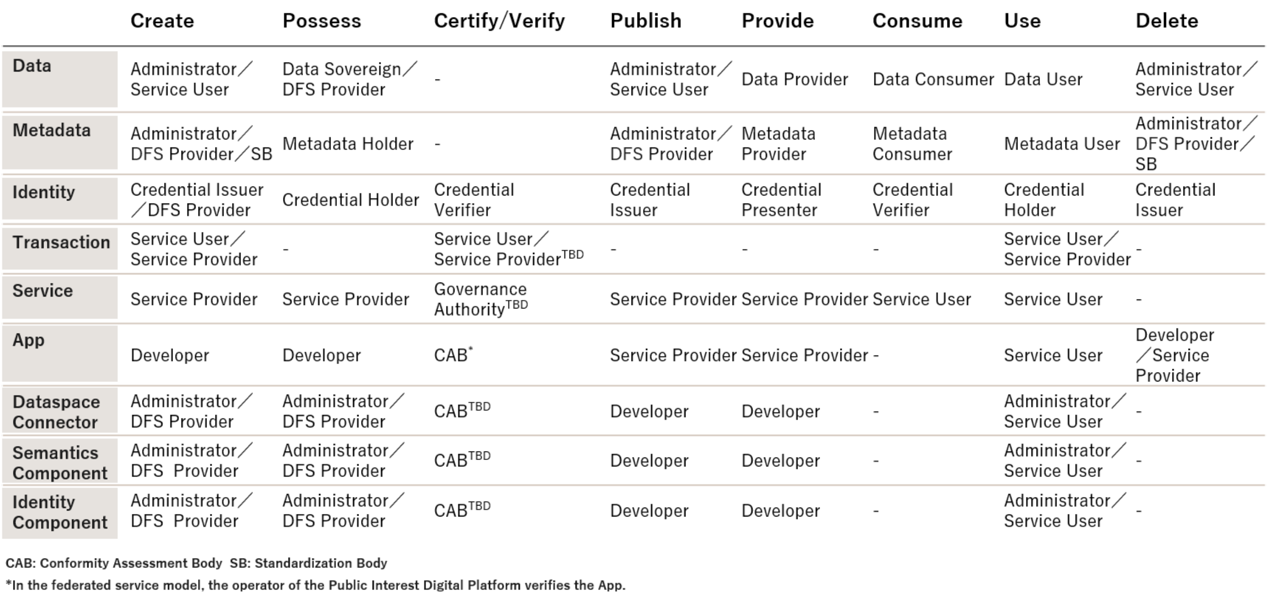
Security Roles define the entities involved in the security for specific functions of the ecosystem when focused on the P3.

(5)　Trust Roles

Trust Roles define the entities involved in trust for specific functions of the ecosystem when focused on the P4.

Each role is organized by object with respect to the layers and perspectives of ODS-RAM, as shown in Table 4 below.

Table 4 Role Mapping by Lifecycle for Key Objects in the ODS-RAM



	Create	Possess	Certify/Verify	Publish	Provide	Consume	Use	Delete
Data	Administrator／Service User	Data Sovereign／DFS Provider	-	Administrator／Service User	Data Provider	Data Consumer	Data User	Administrator／Service User
Metadata	Administrator／DFS Provider／SB	Metadata Holder	-	Administrator／DFS Provider	Metadata Provider	Metadata Consumer	Metadata User	Administrator／DFS Provider／SB
Identity	Credential Issuer／DFS Provider	Credential Holder	Credential Verifier	Credential Issuer	Credential Presenter	Credential Verifier	Credential Holder	Credential Issuer
Transaction	Service User／Service Provider	-	Service User／Service Provider^{TBD}	-	-	-	Service User／Service Provider	-
Service	Service Provider	Service Provider	Governance Authority^{TBD}	Service Provider	Service Provider	Service User	Service User	-
App	Developer	Developer	CAB*	Service Provider	Service Provider	-	Service User	Developer／Service Provider
Dataspace Connector	Administrator／DFS Provider	Administrator／DFS Provider	CAB^{TBD}	Developer	Developer	-	Administrator／Service User	-
Semantics Component	Administrator／DFS Provider	Administrator／DFS Provider	CAB^{TBD}	Developer	Developer	-	Administrator／Service User	-
Identity Component	Administrator／DFS Provider	Administrator／DFS Provider	CAB^{TBD}	Developer	Developer	-	Administrator／Service User	-

CAB: Conformity Assessment Body SB: Standardization Body

***In the federated service model, the operator of the Public Interest Digital Platform verifies the App.**

3.4.1 Service Roles

- **Service User**

  A service user is an entity that uses a service provided by a service provider.

- **Service Provider**

  A service provider is the entity that provides the service to the service user. Services include DFS, DCS, and IS.

3.4.2 Technical Roles

Technical roles do not have a mutually exclusive relationship; some responsibilities may overlap.

Operational Roles

- **Developer**

  A developer is an entity responsible for the system design, development, and implementation necessary to handle the data possessed by the service and the organization to which the developer belongs.

- **Administrator**
  An administrator is the entity that manages the systems and data possessed by the service and the organization to which the administrator belongs. This role involves configuring and operating the service, as well as managing, operating, and maintaining the systems and data possessed by the organization.

Functional Roles

- **Data Sovereign**
  A data sovereign is the entity that possesses data at L1 and exercises sovereignty over the data. Data sovereigns make self-determination regarding the conditions of storage and use that shall apply when granting permission for data use.

- **Data User**
  A data user is the entity that uses data in L1. Data users comply with self-determination made by the data sovereign and acquires, stores, and uses data within the scope of the storage and use conditions set by the data sovereign.

- **Data Provider**
  A data provider is the entity that transmits the data stored in the sovereign data store to the data consumer in L2. The data provider may be the data sovereign itself as the administrator, or a third party DFS service (cloud enabler service) provider acting on behalf of the data sovereign. The data provider uses the dataspace connector in transferring data and cooperates with the data consumer's dataspace connector in transfer process management based on transaction protocols.

- **Data Consumer**
  A data consumer is an entity that receives data from a data provider in L2. The data consumer may be the data user itself as an administrator, or a third-party DFS service provider (cloud enabler service) acting on behalf of the data user. The data consumer uses the dataspace connector to request data transfer to the data provider's dataspace connector, and the two parties cooperate based on transaction protocols to perform transfer process management.

- **Credential Issuer**
  A credential issuer is an entity that issues credentials to credential holders in L3.

- **Credential Holder**

  A credential holder is an entity that holds a credential issued by a credential issuer in L3.

- **Credential Presenter**

  A credential presenter is an entity that discloses credentials in L3 at the request of a credential verifier. The credential presenter may be the credential holder itself as the administrator, or a third party DFS service (cloud enabler service) provider acting on behalf of the credential holder.

- **Credential Verifier**

  A credential verifier is an entity that verifies the credentials held by a credential holder in L3.

- **Metadata Holder**

  A metadata holder is an entity that holds metadata in L4, with the holder differing depending on the endpoint-related and meaning-related metadata. Whereas the data sovereign corresponding to the defined endpoint serves as the metadata holder, an entity who defines the semantic definition itself as the metadata holder.

- **Metadata provider**

  A metadata provider is an entity that provides metadata to consumers of metadata in L4, with the provider differing depending on the endpoint information and meaning definition. Whereas the endpoint-related metadata provider may be the data sovereign itself as the administrator, or a third party DCS service provider (data discovery and search service) acting on behalf of the metadata provider, the meaning-related metadata may be the metadata holder itself as the administrator, or a third-party DFS service provider (semantics modeling service) on behalf of the metadata holder.

- **Metadata User**

  A metadata user is an entity that uses metadata necessary for accessing and interpreting data at L4. A metadata user corresponds to the data user in both endpoint-related and meaning-related metadata.

- **Metadata consumer**

  A metadata consumer is an entity that receives metadata from a metadata provider in L4. The metadata consumer itself may receive metadata as an administrator, or a third-party DFS service provider (cloud enabler service) may receive metadata on behalf of the metadata consumer.

3.4.3 Governance Roles

Generally, governance roles are as to related to manage, supervise, and operate such as **governance authority**, **conformity assessment body**, and **standardization body**, and will be discussed from FY2025 onward.

3.4.4 Security Roles

Security roles will be discussed from FY2025 onward.

3.4.5 Trust Roles

Trust roles will be discussed from FY2025 onward.

04 Protocols

4.1 Principles of the Ouranos Ecosystem Dataspaces Protocol

The **Ouranos Ecosystem Dataspaces Protocols** (hereinafter referred to as "ODP") provide the functionalities necessary to realize various activities of the ODS and ensure interoperability between dataspaces. The ODP consists of a set of ***Fundamental*** and ***Complementary*** protocols.

（1） **Fundamental Protocol**

The Fundamental Protocol is an arrangement for providing fundamental functionalities to operate the ODS. Fundamental Protocol is mandatory arrangement adopted to realize the functions of the corresponding Layers and Perspectives.

（2） **Complementary Protocol**

The Complementary Protocol is an arrangement for providing complementary functionalities to operate the ODS. Complementary Protocol is an optional arrangement adopted as needed to realize the functions of the corresponding Layers and Perspectives.

The ODP is designed to **allow for the flexible adoption of protocols based on the data management** executed within dataspaces. The design aims to eliminate barriers to social implementation, such as the failure to meet business requirements due to overfitting to protocols, thereby facilitating the inclusion of various entities within the dataspaces and embodying the separability of Layers within the protocols. Furthermore, **each protocol is defined in a technology-neutral manner, aiming for vendor-agnostic arrangements that do not depend on specific vendors' technologies or products**.

The requirements for the protocol in the ODS-RAM are outlined below; but the detailed concepts and specifications are planned to be released as the **ODS Protocol Specifications** by FY2025, considering future demonstrations and evaluations.

Table5 Types of Protocols in the ODS-RAM

ODS-RAM	Name of protocols	Type of protocols
Common Functionalities	Versioning	Fundamental
	Logging	Fundamental
	Monitoring	Fundamental
L1	Sovereignty	Fundamental
	Data Trust Assessment	Fundamental
	Data Trustworthiness and Quality Assessment	Fundamental
L2	Transaction	Fundamental
L3	Identity and Trust	Fundamental
L4	Metadata Exchange	Fundamental
P1	Heuristic Contracting	Complementary
	Discovery and Search	Complementary
	Clearing and Payment	Complementary
	Marketplace	Complementary

4.2 Fundamental Protocols

4.2.1 Common Functionalities

Common Functionalities encompass functions commonly used across each Layers and Perspectives and primitive protocols to ensure interoperability among dataspaces. ***Versioning***, ***Logging***, ***Monitoring***, etc. fall under this category.

（1） **Versioning**

Versioning defines the specifications for managing and providing protocol version information in the dataspace.

（2） **Logging**

Logging defines the specifications for observing, collecting, and recording historical information in the dataspace.

（3） **Monitoring**

Monitoring defines the specifications for overseeing, managing, detecting anomaly, and optimizing operations of various activities in the dataspace based on logging information.

4.2.2 Sovereignty

Sovereignty Protocol defines the specifications for self-determination and its guarantee regarding the conditions of storage and use that shall apply when granting permission for data use. The definition and evaluation of the concept of data sovereignty for data interoperation and utilization of data from each service entity's data store each service entity are expected to be compiled from FY2025 onward.

For convenience, the data store that appropriately ensures the data sovereignty exercised by the data sovereign regarding the conditions for data storage is referred to as the **sovereign datastore**. While the sovereign datastore primarily considers data stores provided by third parties, the definition includes data stores managed and operated by the data sovereign themselves.

4.2.3 Data Trust Assessment

Data Trust Assessment Protocol defines the specifications for the evaluation and calculation methods related to data integrity (tamper-proofing) and the referencing and provision of their results.

4.2.4 Data Trustworthiness and Quality Assessment

Data Trustworthiness and Quality Assessment Protocol defines the specifications for the evaluation and calculation methods related to data quality and the referencing and provision of their results.

4.2.5 Transaction

Transaction Protocol defines the specifications for controlling the process of transferring data between data providers and consumers.

4.2.6 Identity and Trust

Identity and Trust Protocol defines the specifications for the identity, authentication and authorization of dataspace participants.

4.2.7 Metadata Exchange

Metadata Exchange Protocol defines the specifications for handling ontologies and vocabularies related to metadata, collection of structural schemas, and shared and reusable metadata schemas. *Note that the term ***catalog*** is not used, as it may evoke associations with specific data catalog software that aggregates fixed schemas using a schema-first approach, such as CKAN, potentially leading to misunderstandings among developers and users.

4.3 Complementary Protocol

4.3.1 Discovery and Search

Discovery and Search Protocol defines the specifications for cross-searching semantic descriptions and other information in the dataspace, including link information. Discovery and Search Protocol complements the Metadata Exchange Protocol and provides the specifications for the discovery and search of endpoints and rapid access to metadata associated with those endpoints.

4.3.2 Heuristic Contracting

Heuristic Contracting Protocol defines the specifications for service contracts that allow newly discovered service users and service providers within the dataspaces to electronically enter into new contracts, either independently or by utilizing third-party contracting services.

To reflect market and industry practices more flexibly, Heuristic Contracting Protocol shall be excluded from mandatory requirements for the implementation of dataspace connectors operated within the ODS and therefore is adopted as an optional. This decision is rooted upon the current situation where many markets and industries do not accept the preparatory actions and responsibilities required for automated, negotiated electronic contracting through dataspace connectors (e.g. the Contract Negotiation Protocol envisioned by IDS[9]) or the Open Digital Rights Language (ODRL) policies for data providers, and hence the absent of sufficient legal arrangements.

By not making protocols that involve challenges requiring long-term transformation mandatory, the ODS aims to avoid hindering the social implementation of dataspaces and positions this functionality as a complementary means. At the same time, future support for automated, negotiated electronic contracting will be discussed and considered regarding the approach to pre-contracting based on Model Agreements for Data Interoperability[10], as well as cases where contracts are not executed.

4.3.3 Clearing and Payments

Clearing and Payment Protocol defines the specifications for clearing, payment, and billing for the use of services in the dataspace.

4.3.4 Marketplace

Marketplace Protocol defines the specifications for buying and selling data in the dataspace.

[9] International Data Spaces Association. (2024). Contract Negotiation Protocol.

[10] (METI 2024a) and (METI 2024b).

05 Operations and Implementations

5.1 Operations and Onboarding

Technical implementation and operations for vendors who develop systems and provide application services, as well as those who in system development and data management departments of companies and government agencies, will be presented in the "**ODS Development and Operation Guidebook** (**tentative**)" to be released during FY2025, based on the ODS protocol specifications to be developed during the same fiscal year. The **"ODS Implementation Guidebook** (**tentative**)**"** for those who are in planning and business divisions of companies and government agencies is also scheduled to be released in FY2025.

Furthermore, the Ouranos Ecosystem Initiative is currently considering strategies to select ongoing efforts aimed at forming cooperative domains for data interoperation within various industries as use cases for the initiative. Details will be made available in future publications.

Annex A. Building-block Portfolio

A.1 Basic Concept

The ODS provides core components that implement the ODP and SDKs as OSS.
These building blocks serve as reference implementations that comply with the ODP and do not hinder participation in dataspaces by leveraging other technology stacks that ensure the feasibility and compatibility of the ODP. Each protocol specification and operational method will adhere to the **ODS Protocol Specifications** scheduled for publication in FY2025.

The core components provided by the ODS will reflect the principles of opt-in/out oriented protocols **by adopting a microservices architecture as a principle and by publishing interfaces, thereby aiming to ensure interoperability and backward compatibility while achieving vendor-agnostic container design and orchestration, being independent from individual products or specific technologies.** Note that the components listed below merely represent the status quo of reference implementations, and that for other protocols will also be published from FY2025 onward.

A.2 Semantics Component

Semantics Component constitutes a core group of components within the Metadata Exchange Protocol. The ODS currently provides the following components as reference implementations as OSS:

- **ODS Semantics Crawler** (hereinafter referred to as “ODS-SCR”) reads semantic descriptions (e.g., RDF) published by metadata providers and sequentially crawl the links contained within them, allowing data users and service users to collect semantic descriptions in scope of interest. The scope of interest is described using a predefined definition method (e.g., SPARQL), and the collection runs according to this description.

- **ODS Semantics Viewer** (hereinafter referred to as “ODS-SV”) allows metadata users to view metadata collected by the ODS-SCR, categorizing it into instance and class information, by presenting in a structure similar to an ER (Entity-Relation) diagram or in tabular format. Through the ODS-SV, even when the metadata provider independently extends the data or services, the metadata user still can understand the meanings of these extensions including the specific tabular data involved.

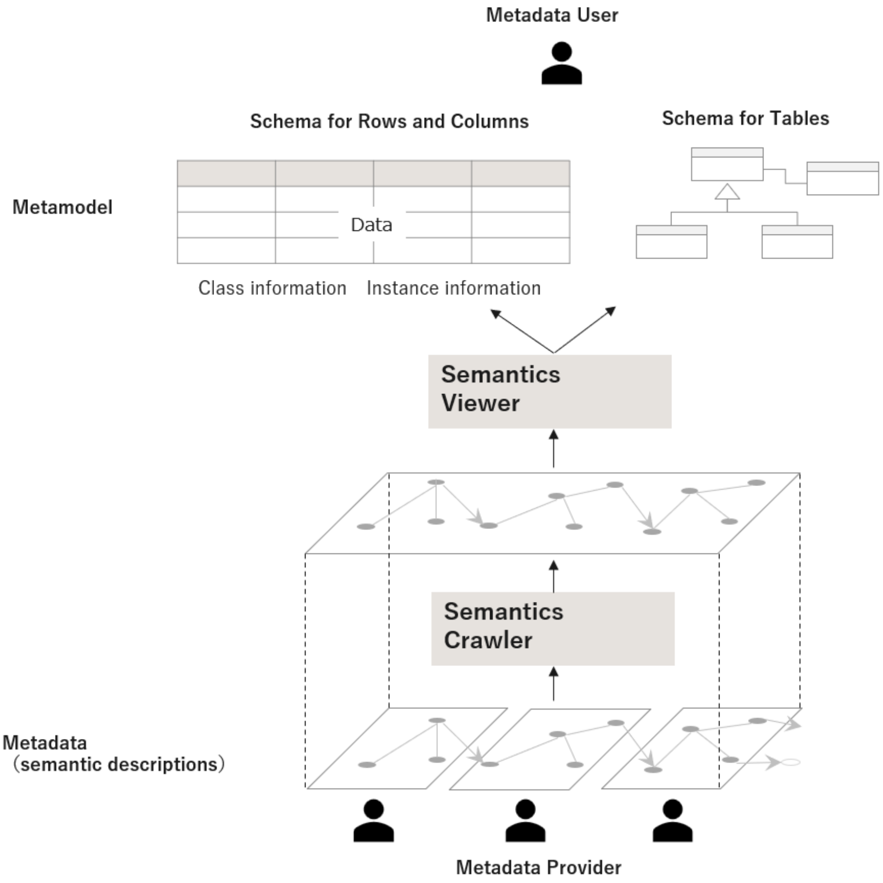


Figure13 How semantics component works

- **ODS Semantics Compiler** (hereinafter referred to as "ODS-SCP") is a developer tool that generates source code necessary for inter-service connections based on models where the semantics description pertains to the external specifications of services (e.g., the Semantic Aspect Meta Model (SAMM)). The external specifications describe not only the information that the service discloses externally but also the services/data per se provided through synchronous or asynchronous calls. Since specialized models focused on semantics are independent of the execution environment, by executing a semantics model compiler (e.g., SAMM CLI) and synchronous API specifications (e.g., OpenAPI Generator), connection modules dependent on the execution environment (e.g., REST) are generated. System developers on the service user side therefore can quickly adapt to the new version by using ODS-SV to understand the data and services and ODS-SCP to facilitate the transition when the service provider implements a version update.

  Note that while the data published as semantic descriptions can be understood in tabular formats without prior knowledge of the schema, conventional synchronous/asynchronous calls are generally more suitable in the case with transaction management and real-time requirements. Recognizing that the responsibility for creating these semantic descriptions may impose developing burden on metadata providers, efforts shall be made to promote the use of GUI-based editors (e.g., Aspect Model Editor) and to develop SDKs in the future, aiming to simplify the onboarding process for L4.

The ODS also provides OSS for the following components as reference implementations of the Discovery and Search Protocol:

- **ODS Discoverer** (hereinafter referred to as “ODS-DI”) enables the initial endpoint and different metadata searches for each type of service, necessary when the ODS-SCR sequentially crawls semantic descriptions containing link information published by metadata providers.

- **ODS Discovery Finder** (hereinafter referred to as “ODS-DF”) allows users to search for which ODS-DI is being utilized for the discovery and search services in each dataspace (or service).

A.3 Identity Component

Identity Component constitutes a core group of components within the Identity and Trust Protocol. The ODS is currently reviewing the specifications, and the reference implementation is scheduled to be published as the **ODS Identity Component** (hereinafter referred to as “ODS-IC”) as OSS within FY2025.

A.4 Dataspace Connector

Dataspace Connector constitutes a core group of components within the Transaction Protocol. The Dataspace Connector serves as a node for the protocols of both the data plane and control plane, as well as DES and DCS services, facilitating communication with the Semantics Component, Identity Component, and other services. The ODS provides the **ODS Flex Dataspace Connector** (hereinafter referred to as “ODS-FDC”) as OSS reference implementation. The ODS-FDC is currently undergoing a version update, and any source code for functions missing in the architecture shown below will be developed and released during FY2025.

The ODS-FDC consists of two logical function groups, **Control Plane Orchestrator** and **Data Plane Modules**, to reflect the nature of L2 as the node of the control plane and data plane.

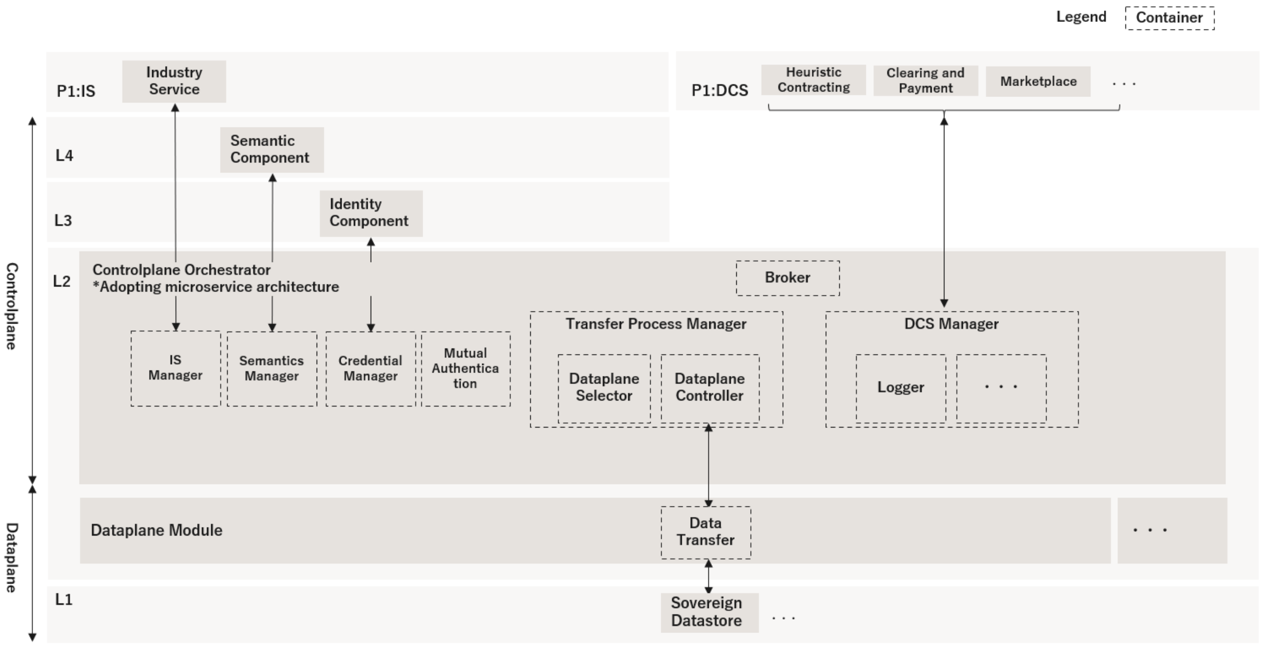


Figure14 System Architecture of the ODS-FDC

Controlplane Orchestrator

The ODS-FDC provides mutual authentication with the counterpart dataspace connector. In addition, the following functions are provided as part of the transfer process management to switch multiple dataplane modules and ensure reliable transfers, callable via API. Note that the functions listed below merely represent the status quo of reference implementations and will be continuously added and updated onward.

- **Mutual Authentication**

  The function that sends the credentials granted by the authentication and authorization resolution (L3) to the counterpart connector, allowing for mutual authentication of identity and attributes as participants in the dataspace between the connectors.

- **Dataplane Selector**

  The function that selects the appropriate dataplane module from multiple available options based on the metadata provided by the endpoint and meaning resolution (L4).

- **Dataplane Controller**

  The function that instructs the dataplane module set by the dataplane selector to start, suspend, or terminate data transfers. It receives execution status, such as completion of data transfer, from the dataplane module, if necessary.

- **Data Transfer**
  The function that transfers data from the endpoint of sovereign data store (L1) to the data consumer upon its request.

The ODS-FDC also includes the following functions to support other functionalities of Layer and Perspectives:

- **IS Manager**
  The function that interfaces with the IS (P1) to use the dataspace connector.

- **Semantics Manager**
  The function that interfaces with the endpoint and meaning resolution functions of the Semantics Component (L4).

- **Credential Manager**
  The function that interfaces with the authentication and authorization resolution functions of the Identity Component (L3).

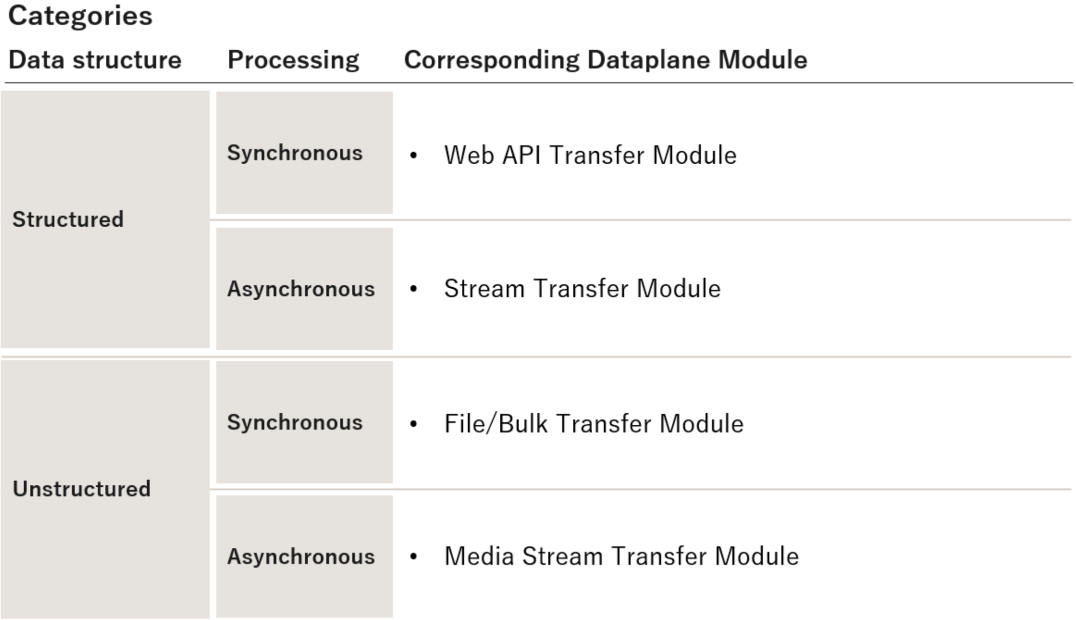
- **DCS Manager**
  The function interfaces with the functions of DCS (P1). The use of DCS is optional, and this function is further divided into sub-functions based on the type of DCS being utilized, allowing for a composable structure where necessary components can be combined.

Dataplane Module

Dataplane modules of ODS-FDC are equipped with the following functions to execute data transfers in accordance with the instructions from the data plane controller of the controlplane orchestrator. Additionally, the ODS allows for direct utilization of the dataplane module without going through the controlplane orchestrator.

- **Data Transfer**
  The data plane module organizes its functions based on a two-tier classification of data structure (structured/unstructured data) and processing method (synchronous/asynchronous) to assist users in selecting the optimal module. In the first tier, classification is based on the characteristics of the data structure whereas the second tier is on the processing method, enabling intuitive selection. Note that reference implementations for each module are currently under development, with plans for gradual release starting from FY2025 onward.

Table6 Classification of Dataplane Modules



Categories		
Data structure	Processing	Corresponding Dataplane Module
Structured	Synchronous	• Web API Transfer Module
	Asynchronous	• Stream Transfer Module
Unstructured	Synchronous	• File/Bulk Transfer Module
	Asynchronous	• Media Stream Transfer Module

(1) Web API Transfer Module

The Web API Transfer module is specialized for low-payload Web API transfers, providing a data exchange interface using general-purpose Web APIs such as Open API. Depending on the use case and service model, versions with the following extended functionalities are offered:

- Validation and Conversion: A version that can easily add type validation and conversion functions based on Open API definitions.
- Additional logic: A version that provide logic beyond validation and conversion. Logic is use-case specific and currently exists for battery carbon footprint data that allows lightweight data exchange via Put/Get method.

(2) Stream Transfer Module

The Stream Transfer Module is specialized for intermittent transfer of small-scale data, such as IoT data.

(3) File/Bulk Transfer Module

The File/Bulk Transfer Module is specialized for large-scale data transfers. An example of the transfer method involves using cloud storage services to perform asynchronous copies between storage areas managed by both data providers and data consumers.

(4) Media Stream Transfer Module

The Media Stream Transfer Module is specialized for real-time streaming data such as video and audio.

- **Logging**

  The function that stores the history of data transfer and access logs. As of March 2025, this function is implemented in the generator module. Upon receiving API requests, the transmission and reception information is recorded as standard output. These standard output logs are aggregated and managed by various cloud and middleware log aggregation services.

- **Authentication Federation**

  The function that verifies whether data users have obtained appropriate authentication by using the interface with the authentication and authorization resolution function of the identity component (L3). This functionality enables the direct use of the dataplane module.

Examples of L3 sequences and deployments in the distributed service model currently envisioned are shown in Figures 15 and 16:

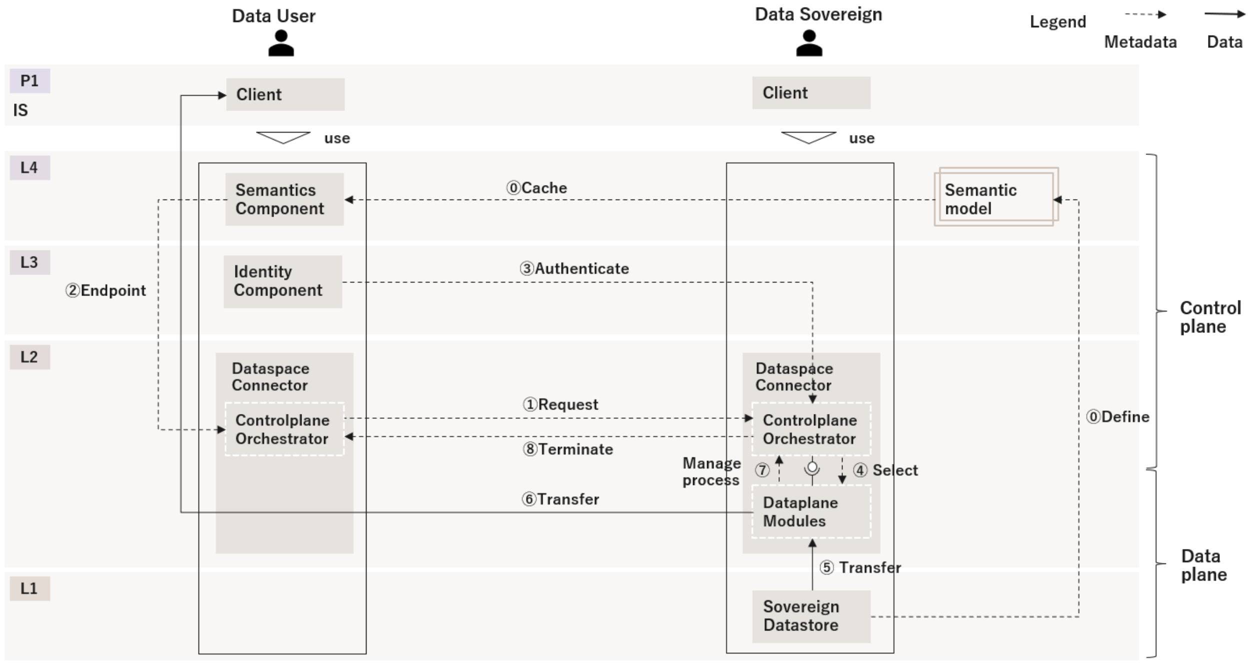


Figure15 L3 Sequence in a distributed service model

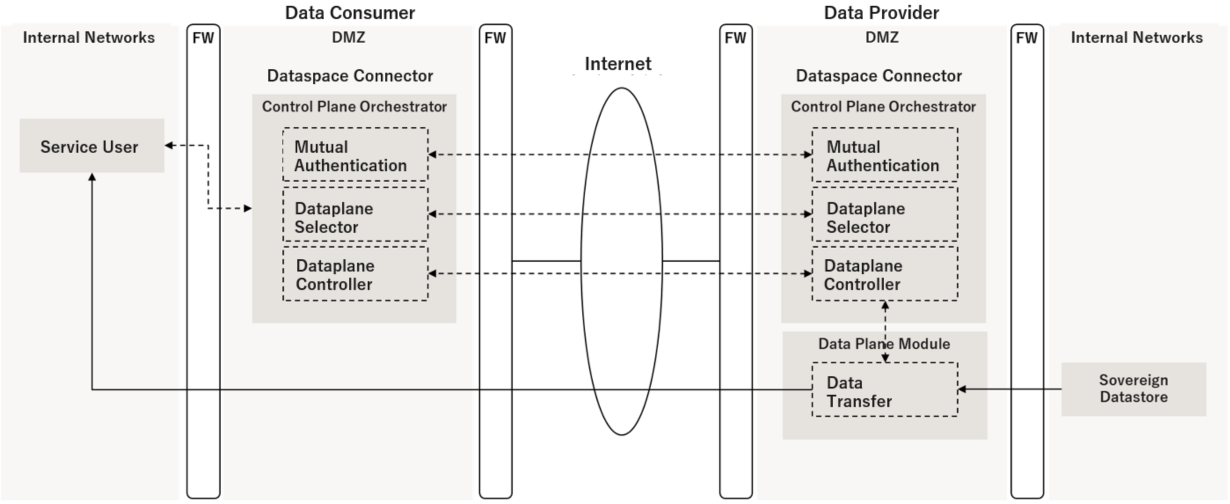


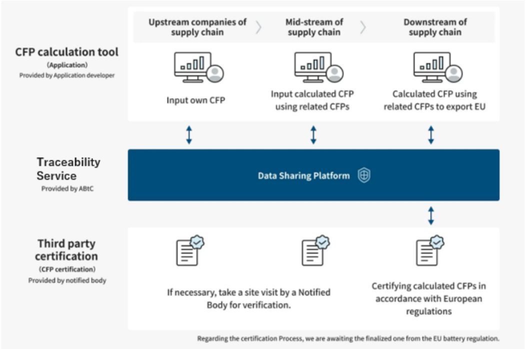
Figure16 Deployment example in a distributed service model

Annex B. Context Catalog

The Context Catalog presents the current information and prospects regarding the cases where ODS-RAM (V1) has conducted compatibility simulations for data interoperations and utilization alongside business development, aiming to establish a diverse range of dataspaces.

Note that these are merely examples of initiatives undertaken at this moment, and this document does not impose any restrictions on the specifications or operations of individual cases. The specific specifications and operational methods for each individual case will be agreed upon and implemented among the stakeholders that form the community advancing the respective service implementations.

B.1 Green Traceability: battery carbon footprint data

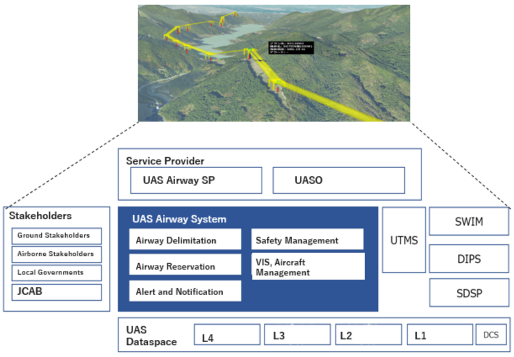

Upstream companies of supply chain
Mid-stream of supply chain
Downstream of supply chain
CFP calculation tool
(Application)
Provided by Application developer
Input own CFP
Input calculated CFP using related CFPs
Calculated CFP using related CFPs to export EU
Traceability Service
Provided by ABtC
Data Sharing Platform
Third party certification
(CFP certification)
Provided by notified body
If necessary, take a site visit by a Notified Body for verification.
Certifying calculated CFPs in accordance with European regulations

Regarding the certification Process, we are awaiting the finalized one from the EU battery regulation.

Roles		
	Service User	Automotive OEMs and Tier 1 to Tier N Suppliers
	Service Provider	• Carbon footprint SaaS Provider • Battery Traceability PaaS Provider

Implementation Timeline	April 2024
Summary	Companies have been required to achieve carbon neutrality and manage entailing risks. Particularly, EU Battery Regulation, which came into effect in FY2024, necessitates compliance regarding battery products. To address these domestic and international regulations, Japan needs to promote data interoperability and utilization among companies while safeguarding enterprise data sovereignty, thereby mitigating business risks. It is, therefore, essential to establish IDI across the entire supply chain for traceability management of carbon footprint data in batteries. Specifically, this involves clarifying the relationship between battery products and their sourced components using trace identifiers, as well as recording transaction relationships between businesses to ensure the traceability of batteries. The initiative will enable the visualization of environmental impact and early detection of risks, contributing to sustainable economic growth and enhancing corporate competitiveness.
Typical data	Carbon footprint data in components and manufacturing process
Necessity of dataspace	Achieving traceability management of carbon footprint data in batteries and promoting data interoperation among companies is essential for complying with domestic and international regulations and mitigating business risks, thereby facilitating the visualization of environmental impact and supports sustainable growth.
Applications Scenarios of dataspace	Compliance with due diligence regulations, Management of sustainable supply chains, and Automation of environmental impact assessments

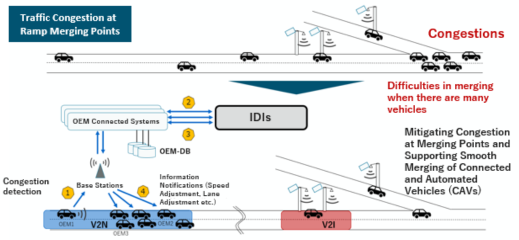
B.2 Airmobility: Unmanned Aircraft Systems (UAS) Airway reservation, access control event data, etc.



Roles		
	Service User	UASO
	Service Provider	UAS Airway Service Provider

Implementation Timeline	March 2025
Summary	Traditionally, UAS flight operators（UASO）have coordinated and communicated route development, securing takeoff and landing sites, and various applications individually, conducting separate risk assessments for each entity. With the integration of the UAS Airway system and the Unmanned Traffic Management System (UTMS), these tasks will be simplified and automated, enabling safer and more convenient flights. This advancement supports the social implementation of missions that address societal challenges, such as alleviating labor shortages in logistics and inspection tasks, as well as disaster response.
Typical data	UAS Airway reservation data and access management event data
Necessity of dataspace	Sharing the reservation information of the UAS airways and takeoff/landing sites managed by the destination UAS airway service providers in the UAS airway system for UASO to operate by connecting multiple UAS airways. Confirming safety during the reservation process, using access management event data for the takeoff and landing sites.
Applications Scenarios of dataspace	Access Charge (Inter-UAS Airway SP Settlement Linked to Direct Flight Reservations), Modal Interoperability for Reservations, and Transmission of Video Data from UAS

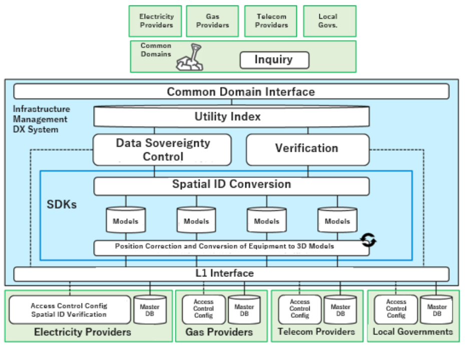
B.3 Mobility: collected automotive, weather, and traffic data in cooperative automated driving support


Traffic Congestion at Ramp Merging Points
Congestions
Difficulties in merging when there are many vehicles
2
OEM Connected Systems
IDIs
3
OEM-DB
Mitigating Congestion at Merging Points and Supporting Smooth Merging of Connected and Automated Vehicles (CAVs)
Congestion detection
1
Base Stations
4
Information Notifications (Speed Adjustment, Lane Adjustment etc.)
OEM1
V2N
OEM2
OEM3
V2I

Roles	Service User	Automotive OEMs
	Service Provider	Automotive OEMs, Weather Information Providers, Traffic Information Providers, etc.

Implementation Timeline	Within FY2027
Summary	Collect traffic information from each automotive OEM and provide vehicle information that spans across different automotive OEMs to the vehicles. Aims to enhance safety and security further through cooperative driving assistance that prevents traffic congestion, especially at the merging points of highway ramps.
Typical data	Collected automotive data, weather data, traffic data, etc.
Necessity of dataspace	Offering safe driving in cooperative automated driving requires the integration of information with different retention characteristics (such as links and coordinates) and information with varying temporal characteristics, to provide users with accessibility to information and ease of connection to individual systems.
Applications Scenarios of dataspace	Utilization of Predictive Information and Application in Route Exploration, etc.

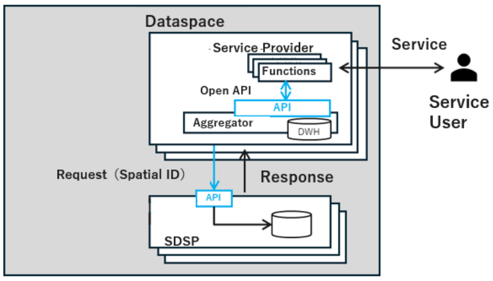
B.4 Infrastructure: underground utility data in infrastructure management



Roles	Service User	Infrastructure Management Companies
	Service Provider	Underground Utility Providers for Electricity, Gas, Telecommunications, and Water Supply and Sewage Systems

Implementation Timeline	After FY2026
Summary	Until now, excavation operators have individually inquired about the presence of underground utilities with various infrastructure management companies. By utilizing the web to make bulk inquiries to multiple infrastructure management companies, this approach aims to reduce the labor involved in inquiries by 50%. This improvement contributes to increased productivity in inspections and construction, addressing the challenges posed by the intensification of disasters and the aging of infrastructure amid a labor shortage.
Typical data	Equipment data for underground utilities such as electricity, gas, telecommunications, and water supply and sewage systems
Necessity of dataspace	Standardizing and unifying the location criteria of the equipment data for critical infrastructure held by each infrastructure management company, and creating 3D models, requires to ensure that the locations where the equipment is buried can be shared among companies under appropriate access control while maintaining data sovereignty.
Applications Scenarios of dataspace	Machine Guidance for Construction Equipment and Aggregation of Damage Status from Various Infrastructure Management Companies During Disasters

B.5 Geospace: geospatial and spatio-temporal data

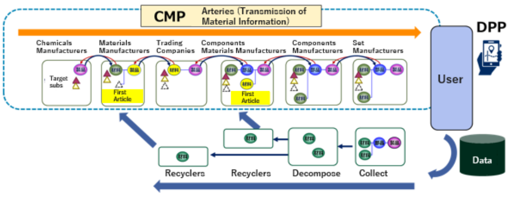


Roles		
Roles	Service User	Service Providers in Each Industry Service
	Service Provider	SDSPs

Implementation Timeline	March 2025
Summary	In various fields such as unmanned aircraft systems, underground utilities, and connected autonomous vehicles, Spatial ID Project promotes interoperability and utilization of four-dimensional spatio-temporal data related to general-purpose geospatial information through reproducible and standardized meshes and a UMI known as Spatial ID. This approach encourages service providers who have been hoarding enterprise data to interoperate with sovereignty, while also creating a safer environment for SDSPs （Supplementary Data Service Providers） that provide geospatial information as a business.
Typical data	Terrain data, building data, restriction zones data, weather data, signal strength data, etc.
Necessity of dataspace	Regarding geospatial data, which serves as foundational data across various fields, achieving data interoperability that includes appropriate secondary use and charging, while maintaining the data sovereignty of SDSP operators who provide data for free or for a fee, is essential for enabling cross-sector utilization by businesses and across different domains.
Applications Scenarios of dataspace	Clearing and Payment for Spatial Information in Dataspaces, Ensuring Data Sovereignty Related to Secondary Use, etc.

B.6 Circularity: chemical substance and resource circulation data in the supply chain

Overview of Circular Economy Data Interoperable Platform

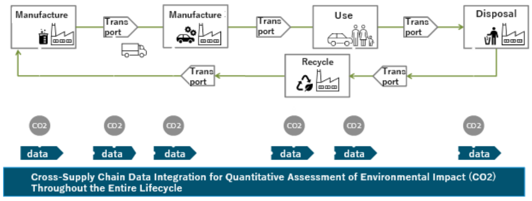


Provide transmission of contained chemical substance information that contributes to the venous system as the first phase.

Roles		
Roles	Service User	Chemicals, Materials, Components, Downstream Manufacturers (Initially: Automotive and Electronics)
	Service Provider	CMP SaaS Provider CMP PaaS Provider

Implementation Timeline	Within FY2026
Summary	In recent years, the transition to a circular economy has become an urgent issue due to environmental constraints such as waste management and climate change, as well as resource constraints stemming from increasing global resource demand and geopolitical risks. This transition aims to maximize the efficient and circular use of resources and their added value. To advance this circular economy, it is essential to visualize the information and actual conditions of products and materials necessary for resource circulation. The goal of this project is to establish a “Circular Economy Data Interoperable Platform” that promotes interoperability of enterprise data. As a use case for this platform, a system for the transmission of chemical substance information （CMP: Chemical and Circular Management Platform） is planned to be provided within the FY2026.
Typical data	Chemical substance and resource circulation data in the supply chain
Necessity of dataspace	Complying with regulations and laws related to chemical substances requires to consistently transmit information about contained chemical substances across the entire supply chain, from upstream to downstream, while ensuring data sovereignty among companies.
Applications Scenarios of dataspace	Information Disclosure （Registration） to DPP, Transmission of Environmental Information Other than Chemical Substances, Expansion of Transmission for Resource Circulation （Recycling, etc.）, and Supply Chain Traceability for BCP （Business Continuity Planning）

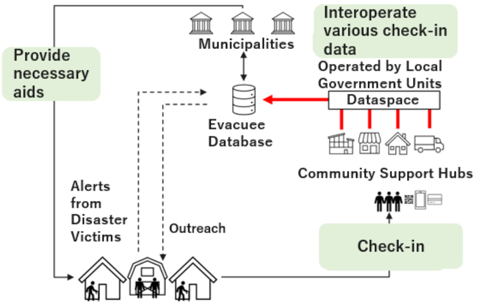
B.7 Lifecycle Assessment: carbon footprint data throughout the entire lifecycle of automobiles


Manufacture
Trans port
Manufacture
Trans port
Use
Trans port
Disposal
Recycle
Trans port
Trans port
CO2
data
Cross-Supply Chain Data Integration for Quantitative Assessment of Environmental Impact (CO2) Throughout the Entire Lifecycle

Roles	Service User	Automotive OEMs and Tier 1 to Tier N Suppliers
	Service Provider	LCA Calculation Application Provider Automotive LCA PaaS Provider

Implementation Timeline	April 2027
Summary	As interest in climate change has increased, various stakeholders are demanding that companies disclose their carbon footprints (CFP). Japan has declared its commitment to "carbon neutrality by 2050" and is promoting a Green Growth Strategy that encourages a virtuous cycle between the economy and the environment. The strategy promotes to create a market for low-carbon products and enhance corporate competitiveness, requiring to calculate CO2 emissions across the company's supply chain using Life Cycle Assessment (LCA) and identify factors for emission reductions that extend beyond individual companies. In the automotive industry, efforts are being made to appropriately evaluate environmental impact reduction activities, build fair LCA methodologies, and reflect opinions in international standardization.
Typical data	CFP data throughout the entire lifecycle of automobiles
Necessity of dataspace	Promoting data interoperation among companies while ensuring data sovereignty and establishing a system that enables CO2 emission reductions across the entire supply chain, thereby allowing for fair evaluation of environmental impact reduction efforts and supporting sustainable economic growth.
Applications Scenarios of dataspace	Management of Sustainable Supply Chains, Automation of Environmental Impact Assessments, and Streamlining of Regulatory Compliance and Reporting

B.8 Disaster Management: evacuee and facility data, etc.



Roles	Service User	Municipalities, Local Government Units Serving Wide Areas
	Service Provider	Community Support Hubs (Support Facilities, Commercial Facilities, Mobile Sales Vehicles, etc.)

Implementation Timeline	After FY2026
Summary	The project contributes to supporting disaster victims and building a more resilient society by establishing a system to connect community support hubs for evacuees outside of shelters with a database of disaster victims. By utilizing this system in a phase-free manner, the project aims to improve the administrative costs, frequency, volume, and speed of collecting evacuee information during disasters.
Typical data	Evacuee Data (Basic Four Information), Facility Data, Location Data, Timestamp, etc.
Necessity of dataspace	Sharing evacuee data collected from various facilities, including different formats and metadata, with a wide-area disaster victim database.
Applications Scenarios of dataspace	Integration of Disaster Response Systems for Municipalities and Utilization in Normal Times

Glossary

- **asynchronous processing**

  A communication method that continues processing without waiting for the results of external calls, such as batch processing, file transfers, and streaming, and receives results through callbacks or similar mechanisms. The receiving side continues to accept data until the calling side stops processing.

- **backward compatibility**

  A state in which a new method of the same series encompasses (is compatible with) the specifications and functions of an older method.

- **cloud enabler services**

  DFS that provides core components that play a central role of the DFS in L1-L4, as cloud services (i.e., as-a-service).

- **Common Functionalities**

  Functionalities that encompass functions commonly used across each Layers and Perspectives and primitive protocols to ensure interoperability among dataspaces. Versioning, Logging, Monitoring, etc. fall under this category.

- **Complementary Protocol**

  An arrangement for providing complementary functionalities to operate the ODS and is an optional arrangement adopted as needed to realize the functions of the corresponding Layers and Perspectives.

- **Control plane**

  An abstract concept that represent the locations where data interoperation processes occur and governs how data is transferred and the functions required to implement that control.

- **Data Free Flow with Trust**

  The concept aims to promote the free flow of data while ensuring trust in privacy, security, and intellectual property rights.

- **Data Layer (L1)**

  A layer that resolves the issue of sovereignty, tampering, quality related to data.

- **Data plane**
  An abstract concept that represent the locations where data interoperation processes occur and is responsible for the actual transfer of data.

- **Data sovereign**
  The entity that possesses data at L1 and exercises sovereignty over the data. Data sovereigns make self-determination regarding the conditions of storage and use that shall apply when granting permission for data use.

- **data sovereignty**
  Self-determination regarding the conditions of storage and use that shall apply when granting permission for data use. Note that there is no international standard agreement on the definition of data sovereignty.

- **Dataspace Complementary Services (DCS)**
  A service that provides technical implementations of the functions required for meeting the requirements of the complementary protocols

- **Dataspace Fundamental Services (DFS)**
  DFS is a service that provides technical implementations of the functions required for meeting the requirements of the fundamental protocols

- **Data user**
  The entity that uses the data in L1 and complies with self-determination made by the data sovereign and acquires, stores, and uses data within the scope of the storage and use conditions set by the data sovereign.

- **distributed service model**
  A service model that assumes dataspace participants with independent capability to develop and operate the system.

- **dominant design**
  A concept proposed as the central idea of an evolutionary model for products or industries, referring to the standard and dominant specifications.

- **enterprise data**
  A generic term for all data (whether structured or unstructured) that companies generate, acquire, process, use, transfer, provide, store, and destroy for economic activities.

- **federated service model**
  A service model that assumes a federation of multiple data participants with core technology service providers thereby accommodating participants who may struggle to develop and operate their own systems.

- **Fundamental Protocol**
  An arrangement for providing complementary functionalities to operate the ODS and is an optional arrangement adopted as needed to realize the functions of the corresponding Layers and Perspectives.

- **Governance Perspective** (**P2**)
  A perspective that establishes common rules, policies, etc. to achieve specific objectives, and to manage, supervise, and operate across the ecosystem.

- **Identity Layer** (**L3**)
  A layer that resolves the issue of authentication and authorization.

- **Industry Service** (**IS**)
  Provides business applications, platforms, etc., specific to each industry and use case.

- **Layers**
  The separation of dataspaces into logical hierarchies according to their functional purpose.

- **Logging**
  The specifications for observing, collecting, and recording historical information in the dataspace.

- **Monitoring**
  The specifications for overseeing, managing, detecting anomaly, and optimizing operations of various activities in the dataspace based on logging information.

- **Ouranos Ecosystem**
  An ecosystem that creates value through new industry collaboration by developing and providing business-digital collaborative domains that connect companies, with digitalization as the enabler.

- **Ouranos Ecosystem Dataspaces (ODS)**
  Dataspaces promoted by the Ouranos Ecosystem Initiative.

- **Ouranos Ecosystem Dataspaces Protocols (ODP)**
  A set of arrangements for providing the functionality to enable ODS activities and ensure interoperability among dataspaces.

- **Ouranos Ecosystem Initiatives**
  Initiatives for the realization of the Ouranos Ecosystem, where industry, academia, and government come together to develop collaborative domains related to business-to-business relationships such as commercial distribution (business transactions and contracts), financial distribution (finance and settlement), and logistics (goods), promoting digital transformation across the entire industry—innovation across business and digital layers

- **Perspectives**
  Logical viewpoints that serve a cross-cutting function in the ecosystem encompassing the entire dataspaces

- **reference implementation**
  A hardware or software designed to achieve a specific function, created with the purpose of assisting others in independently implementing it by using it as a reference.

- **schema-first**
  A methodology in which the schema is predefined, and data is input in accordance with that definition. Syn: schema-on-write

- **schema-flexible**
  A methodology in which data is read without a predefined schema or based on multiple different predefined schemas. In this case, parsing is executed based on metadata or similar information only when the data is read, and it is adapted to fit the schema as needed. Syn: schema-on-read

- **security by design**
  Measures to ensure security from the planning and design stages

- **Security Perspective (P3)**
  A perspective that defines the security requirements and measures in the ecosystem as a

whole or in parts

- **Semantics Layer (L4)**
  A layer that resolves the issue of endpoint and meaning.

- **Service Perspective (P1)**
  A perspective that bridges the business domain and technical domain that encompasses functions and operations.

- **structured data**
  Formatted data such as Web API request/response data, database transfers, and message queues. It is based on clear type definitions using standards such as Open API, Async API, etc., with priority given to the structure of the schema, assuming that the data is readable by the system.

- **synchronous processing**
  A communication method that waits for the result of an external call, such as an API request/response. The process concludes once the specified data transmission and reception are complete.

- **Transaction Layer (L2)**
  A layer that resolves issue of format, query, and protocol.

- **Trust Perspective (P4)**
  A perspective that defines the trust requirements and measures in the ecosystem as a whole or in parts

- **Unified meta identifier（UMI）**
  A meta identifier that is formulated by abstracting the identifier systems that exist as individually optimized and heterogeneous within companies, industries, and other contexts.

- **unstructured data**
  Data with diverse formats such as images, videos, audio, drawings, and log data. This type of data possesses a flexible structure that is not constrained by a fixed schema.

- **Versioning**
  The specifications for managing and providing protocol version information in the dataspace.

Bibliography

- Franklin, M., Halevy, A., Maier, D. (2005). From Databases to Dataspaces: a new abstraction for information management. SIGMOD Record34(4), pp.27-33.
- Halevy, A., Franklin, M., Maier, D. (2006). Dataspaces: A New Abstraction for Information Management. Database Systems for Advanced Applications. Lecture Notes in Computer Science, vol 3882.
- Information-technology Promotion Agency, Japan., Ministry of Economy, Trade and Industry. (2024). Final Report of the Study Group on Vision for Business-to-Business Transactions. https://www.ipa.go.jp/digital/architecture/Individual-link/nq6ept000000e2x8-att/b2btransaction_futurevision_final_report.pdf
- Information-technology Promotion Agency., Ministry of Economy, Trade and Industry. Ministry of Land, Infrastructure, Transport and Tourism., Geospatial Information Authority of Japan., New Energy and Industrial Technology Development Organization. (2024). Ouranos 4D Spatio-temporal ID Definition of Spatial ID and Spatial Voxel https://www.ipa.go.jp/digital/architecture/Individual-link/h5f8pg0000003qbp-att/definition-of-spatial-id-and-spatial-voxel.pdf
- International Data Spaces Association. International Data Spaces Reference Architecture Model 4. https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4
- International Data Spaces Association. International Dataspace Protocol 2024-1 https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol ISO/IEC CD 20151, Information technology - Cloud computing and distributed platforms - Dataspace concepts and characteristics Dataspace concepts and characteristics
- Ministry of Economy, Trade and Industry. (2019). The Cyber/Physical Security Framework. Version 1.0. https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf
- Ministry of Economy, Trade and Industry. (2024a). Interoperable Data Infrastructure Rules Ver. 1.0. https://www.meti.go.jp/policy/mono_info_service/digital_architecture/model_kiyaku.pdf
- Ministry of Economy, Trade and Industry. (2024b). Model Rules for Data Interoperability Explanation and Discussion Points. 1st edition (June 2024). https://www.meti.go.jp/policy/mono_info_service/digital_architecture/moderukiyakukaisetu.pdf

Change Log

February 28, 2025 First edition published

March 31, 2025 English version published

Authors & Contributors

Chief Architect
Michitaka TSUDA Digital Architecture Development Office/Dataspace Strategy Team, Digital Economy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan

Kimitaka TAMURA Architecture Strategy Department, DADC, Information-technology Promotion Agency, Japan
Daisuke MUSASHI Architecture Strategy Department, DADC, Information-technology Promotion Agency, Japan
Keisuke OKA Architecture Strategy Department, DADC, Information-technology Promotion Agency, Japan
Masato ITO Architecture Strategy Department, DADC, Information-technology Promotion Agency, Japan
Nobuaki MORI Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Hiroaki AMINAKA Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Satoshi TAJIMA Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Takuya SUMIDA Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Atsushi UEGOCHI Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Ryota TAKEUCHI Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Takuya NOMURA Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Rei YANO Architecture Implementation Department, DADC, Information-technology Promotion Agency, Japan
Iori MURAKAMI DADC, Information-technology Promotion Agency, Japan/Automotive and Battery Traceability Center
Kiyoto FURUTA DADC, Information-technology Promotion Agency, Japan/CMP Task Force
Chiseki SAGAWA DADC, Information-technology Promotion Agency, Japan
Hideki HANAMI DADC, Information-technology Promotion Agency, Japan
Kohei ISOBE Digital Strategy Office/Data Space Strategy Team, Digital Economy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
Jun OGATA Digital Architecture Development Office, Digital Economy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
Teruyoshi FUJIWARA Automotive and Battery Traceability Center

Contributing Projects

DIGITAL LIFELINE

Digital Lifeline Development Plan

NEDO New Energy and Industrial Technology
Development Organization

New Energy and Industrial Technology Development Organization, Japan
Digital Infrastructure Development Project for Digital Transformation of Industries

Digital Architecture
Design Center

Digital Architecture Design Center, Information-technology Promotion Agency, Japan
Digital Lifeline Realization Project (CAV corridors, UAS Airways, infrastructure management DX, Okunoto digital lifeline)
Battery and Automotive Project
CMP Project
Automotive LCA Project
Spatial Information Project

Publisher & Editor

Digital Economy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan
Digital Architecture Design Center (DADC), Information-technology Promotion Agency, Japan

Reviewers

Group of Service for Citizens, Digital Agency, Japan
Digital Infrastructure Center, Information-technology Promotion Agency, Japan
Data Society Alliance
Japan Institute for Promotion of Digital Economy and Community
OpenID Foundation Japan

Noboru KOSHIZUKA, PhD, Professor, Interfaculty Initiative in Information Studies, The University of Tokyo
Hideaki TAKEDA, PhD, Professor, National Institute of Informatics, Research Organization of Information and Systems
Satoru TEZUKA, PhD, Project Professor, Global Research Institute, Keio University / President, Japan Digital Trust Forum
Hiroshi ESAKI, PhD, Professor, Graduate School of Information Science and Technology, The University of Tokyo