WHITE PAPER “DATA EXCHANGE”

Version 1.0 March 2026

Manufacturing-X
Guidance Board

Manufacturing-X Topic Group „Data Transfer”

1 Table of Contents

2 Table of figures

3 Motivation

The project Factory-X has been tasked to define a common base for exchanging data (see green rectangle in the lower part of figure 1) as the foundation for all projects under the Manufacturing-X umbrella and potentially beyond.

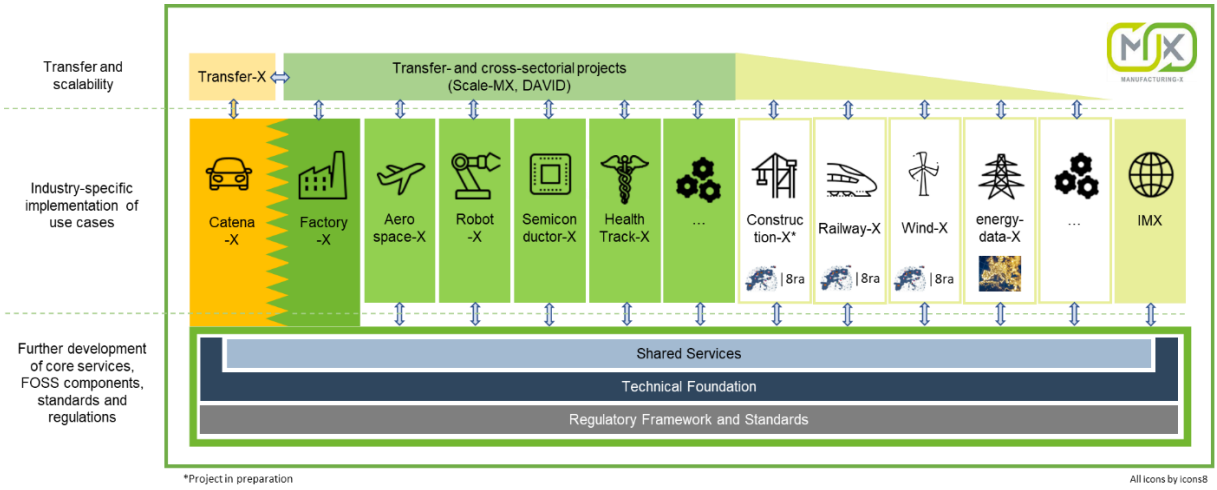


Figure 1: Systemic approach to Manufacturing-X (Source BMWK)

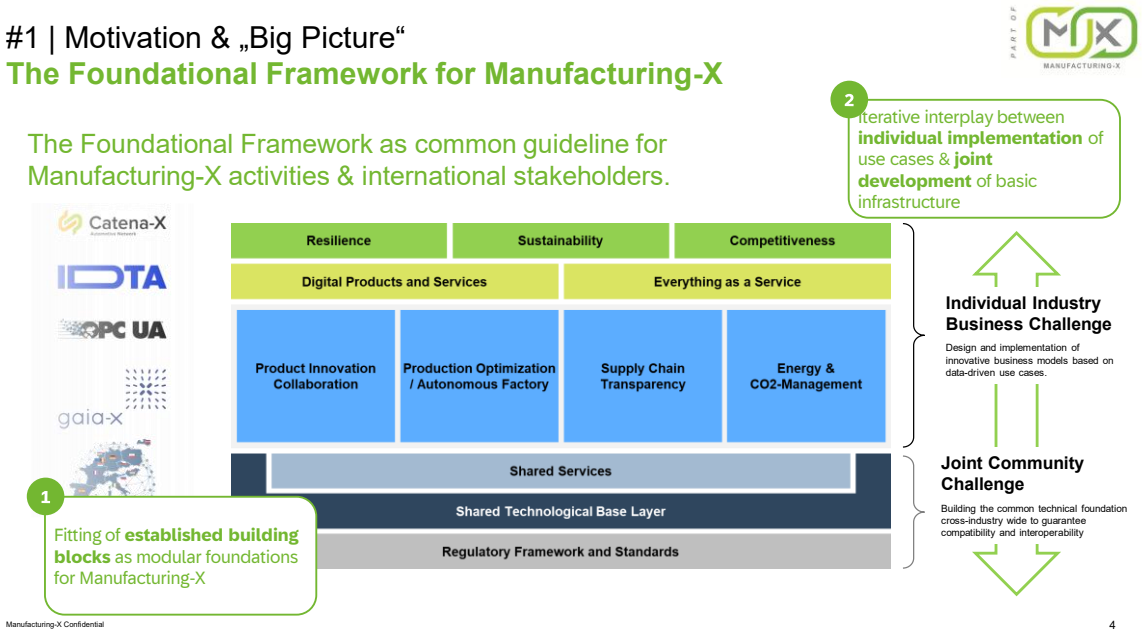


Figure 2 Manufacturing-X Framework for joint community scope

To deliver on this task, Factory-X has defined the MX-Port as a configurable and open concept. The purpose of this document is to detail this concept further in alignment with all relevant Manufacturing-X projects.

3.1 The Goal: Interoperability across industries

Today and even more in the future companies - SMEs as well as large corporations - will exchange and share data with partners from different industries to improve their own business, generate value out of the data or meet regulatory requirements. To illustrate the requirements for the MX-Port, we use the fictitious company “Small Motor Inc.”. It develops, manufactures and supplies electric motors to customers in different industries. For this purpose, the company sources raw materials and parts from suppliers in various industries. “Small Motor Inc.” is involved in various lifecycle processes (e.g., Product Lifecycle Management, Production System Lifecycle Management) and value chains (e.g., product supply chain), see figure 2.

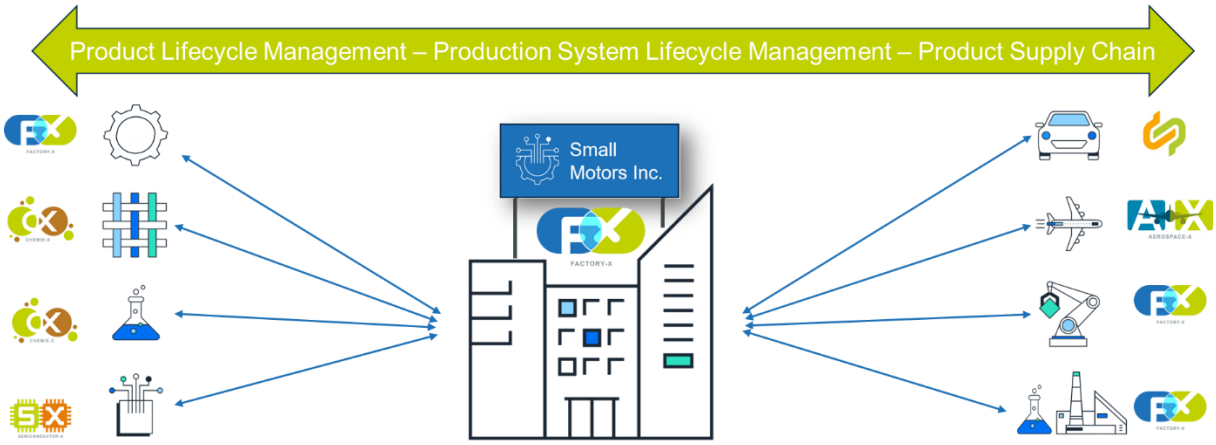


Figure 3: Value chains of “Small Motors Inc.” (source Factory-X)

The MX-Port concept offers an approach for a decentralized, trusted and secure data exchange as well as interoperability and economic scaling. Particularly interoperability is a strategic goal for Manufacturing-X and a core technical element of the MX-Port concept.

In practical terms, interoperability would mean for “Small Motor Inc.” that they will have

- to register, identify and authenticate themselves only once to be able to collaborate with companies from different industries,
- to model its data only once for a given use case,
- to use only one technology stack (MX-port configuration, see below) to realize the “Shared-Service-Box” that allows the use of the required protocols, connectors etc.,
- the free choice in selecting a business application for a use case from several providers.

However, in the real world we will not be able to achieve all goals at the same time. Our objective is to realize a cost-efficient solution approach to increase the benefit for all ecosystem participants.

3.2 Common wording and definitions from the Data Space Support Center are used.

Across the dataspace initiatives it was agreed to follow the building blocks and terminology from the Dataspace Support Center DSSC especially the definition of interoperability (Source: https://dssc.eu/space/SK/812286015/3+-+Interoperability+and+Data+Quality).

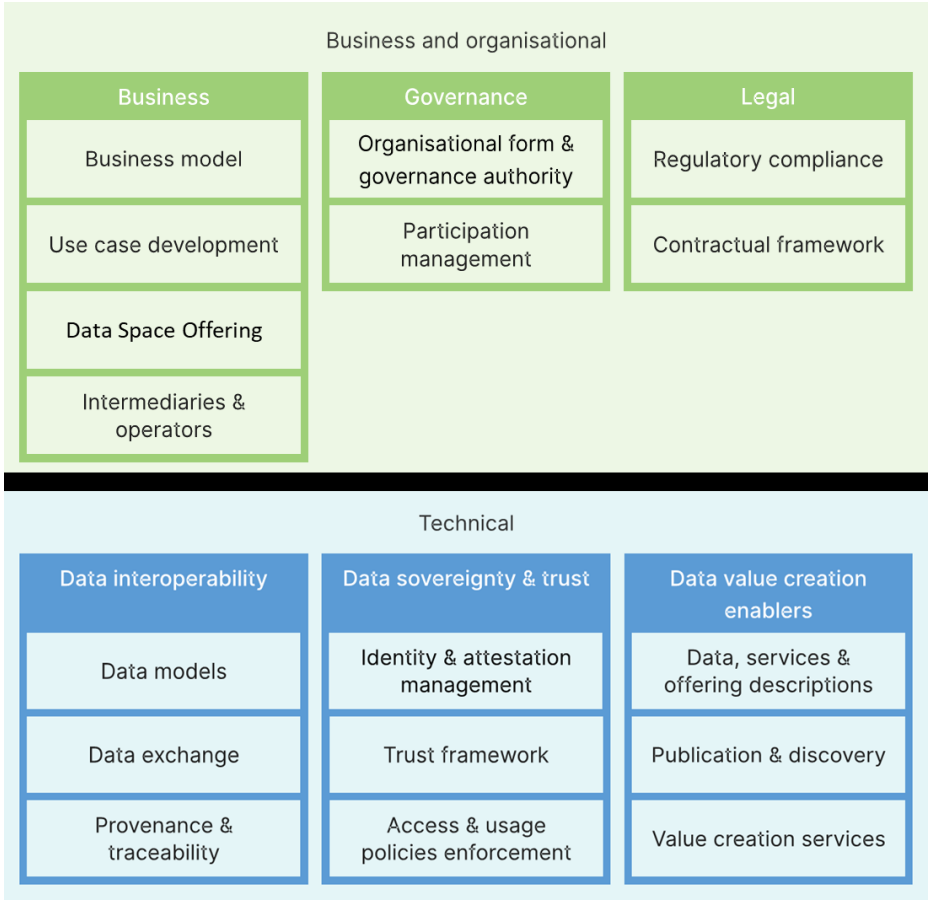


Figure 4: Building Block Overview - Blueprint v2.0 - Data Spaces Support Centre

4 Introduction to Data Spaces

4.1 Guiding Principles of Data Sharing Ecosystems

Aim of Manufacturing-X is to provide a data ecosystem consisting of multiple data spaces based on the principles of interoperability, decentralization, standardization, data sovereignty and a clearly defined business value proposition.

4.2 Interoperability

Interoperability is essential for seamless data exchange within and between dataspaces, covering four key aspects: legal, organizational, semantic, and technical.

4.2.1 Legal interoperability

Ensures data sharing complies with laws, defining ownership, intellectual property rights, privacy regulations, and contractual agreements. Standardized frameworks, such as Eclipse Dataspace Working Group, help align cross-border data exchange while maintaining compliance and trust among participants.

4.2.2 Organizational interoperability

Ensures effective collaboration by aligning processes, policies, and governance models across ecosystem participants. Key aspects include standardizing data-sharing procedures, establishing clear governance structures, and fostering a culture of collaboration.

4.2.3 Semantic interoperability

Ensures data is uniformly understood across all participants by establishing common standards, taxonomies, and ontologies to harmonize data from different sources. Technical interoperability focuses on IT infrastructure, including APIs, protocols, and security measures, to enable seamless data exchange between systems. Both aspects are crucial for effective data sharing, working alongside legal and organizational interoperability to ensure compliance, trust, and usability within the ecosystem.

Focusing on each of these dimensions is essential to developing a sustainable, cohesive data-sharing ecosystem.

4.2.4 Cross-dataspace Interoperability

Interoperability enhances the industry’s digital ecosystem by enabling seamless data exchange across industries and existing systems. Ensuring compatibility with industry standards simplifies SME adoption, lowers entry barriers, and maintains high security standards. This approach supports the evolution of a network-of-networks, aligning with the Manufacturing-X initiative and ensuring scalability by design.

4.3 Decentralization

Decentralization in data-sharing ecosystems distributes control over data storage, access, and distribution across multiple entities rather than a central authority, enhancing data ownership, privacy, and security. It reduces single points of failure, improves scalability, and increases system resilience. However, in regulated industries, centralized control is necessary for dataspace registration to meet strict security standards.

4.4 Standardization

Standardization in data-sharing ecosystems establishes common protocols, formats, and guidelines to ensure compatibility and interoperability across diverse systems. Key elements include data models and formats for structured organization, communication protocols for secure and efficient data transfer, semantics and ontologies for shared interpretation, and compliance and security standards to ensure legal and ethical data use.

4.5 Data Sovereignty

Data sovereignty in the ecosystem ensures clear guidelines on data ownership, compliance, and security, fostering trust and encouraging data sharing. Organizations retain control over their data, including access management and revocation. Cross-border data transfer poses challenges due to differing sovereignty laws, requiring a regulatory framework to ensure compliance. In highly regulated / confidentially sensitive industries, multiple levels of data sovereignty will be necessary, restricting highly sensitive data based on jurisdiction and security standards.

5 Cross Dataspace Data Exchange

The cross-dataspace data exchange requires a common approach to achieve interoperability when it comes to a “cross company, cross dataspace” use cases like for example the Digital Product Passport. Therefore, there needs to be some common ground and “resolvable” artifacts in between the Manufacturing-X dataspaces. As Factory-X is the only X-Project, that uses the MX-Port Variant Leo, the Cross Dataspace exchange applies currently to DCP/DSP only (Hercules or Orion).

The following levels need to be defined:

1. Multiple trusted anchors (Gaia-X, eIDas, Government Organizations, etc.)
    a. Participants of the different dataspaces could share or choose to accept different “certified” Manufacturing-X trusted issuers.
    b. A trusted list needed to keep a record and state who is allowed to operate the Manufacturing-X cross-dataspace
2. Resolvable Identities:
    a. Example: If my company participates in Catena-X and Aerospace-X, I should be able to resolve and understand the identities of the other members.
3. MX-Port Models
    a. It is important to achieve at least at service access level that both parties use the same MX-Port Model configuration.
    b. As a “data provider”:
        i. To set up using the dataspace protocol (DSP) the different services which can be accessed by consumers.
        ii. To configure under which access & usage conditions (which dataspace, agreements, contract references) shall be agreed by consumers to get access to the services in other MX-Ports (e.g. AAS, Business Applications, etc.) using the decentralized claims protocol (DCP) to do the authorization.

c. As a “data consumer”:
   i. Using the dataspace protocol (DSP) we will be able to discover services which are visible for you and filtered relying on the access control management from the decentralized claims protocol (DSP). The visualization of specific offers will depend on the different memberships you have. If you are not member from a specific dataspace, you will not have access to service offers configured at runtime in the MX-Port. It is up to the data provider to configure the access policies with regards on which dataspaces the membership is required.
   ii. Be able to agree with the conditions and receive a “secured” contract agreement which can be used to request access tokens and retrieve data from other MX-Ports (e.g. AAS, Business Applications, etc.) which are behind this “Gateway MX-Port” (e.g. Tractus-X Eclipse Dataspace Connector/Components).

4. Resolvable Semantics

Semantic standards should be re-used defined by use case and or industry / dataspace The minimal requirement is that the different dataspaces align on a common resolvable schema for cross dataspace exchange. For example, using ontologies, which can be defined in an instance level using the well-known JSON-LD technology, which delivers a flexible data structure in JSON which travels with references to the definitions and specifications for each attribute defined in standards/data models in every Manufacturing-X Dataspace.

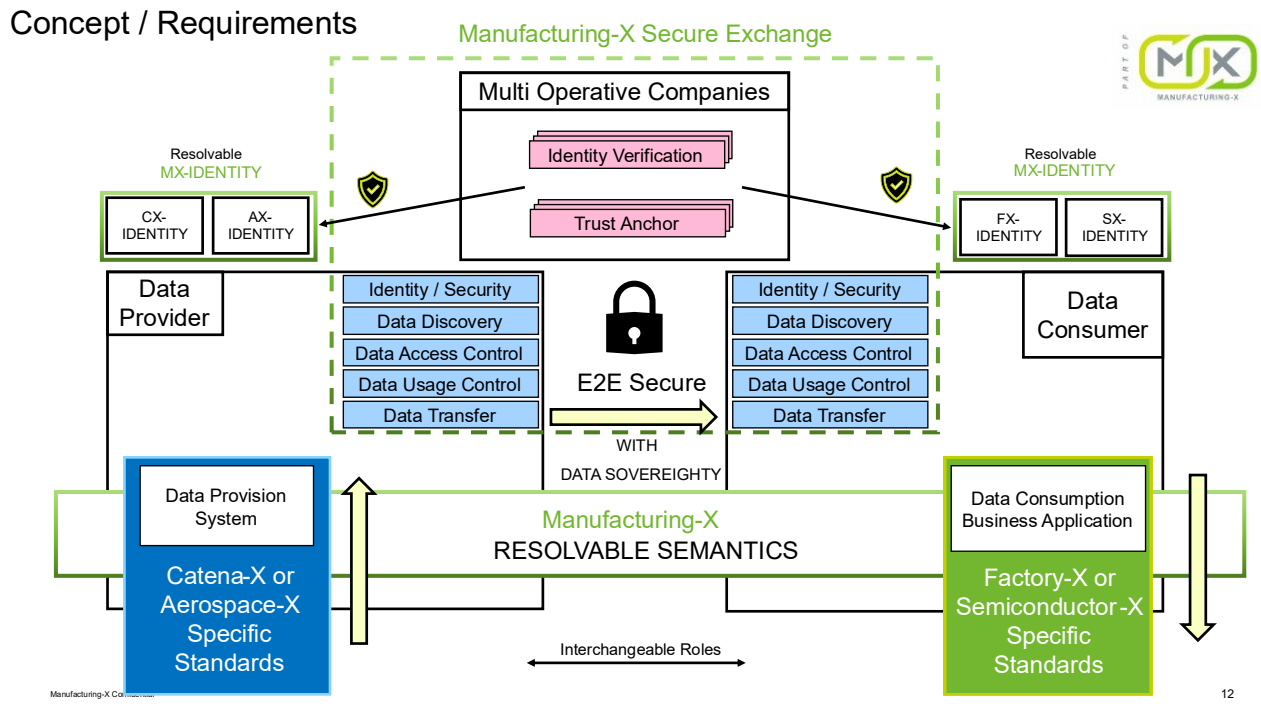


Figure 4 Cross Dataspace Alignment

The vertical integration of the use cases after the data exchange (horizontal integration), will be up to the dataspace to define, since there may be different systems which required different data formats and protocols.

5.1 Details from Cross Dataspace Alignment Diagram:

Here is the description from different MX Data Exchange sections represented in the Figure 4 included above:

5.1.1 Identity Interoperability (Resolvable Identity)

- Data provider and data consumer can discover and identify each other, their identity is “resolvable” in any dataspace and data ecosystem.
- The goal is an E2E data exchange which takes place using an interoperable connector”, (EDC, IDS, other implementations) can be understood from both sides.
- On a technical level, the Identity Credential schemas must have a common semantic.
- Identity interoperability is being worked by the Manufacturing-X Topic Group Identity and will be aligned with this concept.
- The issuance of verifiable credentials must follow the W3C data models.

  Example:

  - Using the DID:WEB defined by the W3C as common identity standard.
  - Using the business partner number legal entity BPNL (technical identification via did:web can change and company identification as business partner required but decoupled from protocol) to create interoperability in an easy company identification and contract exchange. (BPN Credential).
  - Note: current business partner concept from Catena-X represents legal, sites, etc. Requirements to identify the asset e.g. machine directly or the end user using an app in the other company might occur in Semiconductor-X, Factory-X, RoX.
  - I can get specific “membership” credentials for each dataspace, but my BPN credential is supported in any MX Dataspace.
  - I can use my specific membership for specific data access, but my MX dataspace credential for general access purposes (company credentials, cross industry DPP access, etc..).
  - Example from Leo: Human users identified by an email address, non human users identified by an application name and legal entities identified by the company domain.

  - The base identities for Manufacturing-X should be reusable for the data exchange multiple data spaces, so that companies which are part of multiple industries (especially Tier-1’s) can deliver the data under one Identity, saving costs on implementation and when expanding their products to other industries.

5.1.2 Data Exchange Security & Data Sovereignty Interoperability:

- The secure exchange infrastructure, that the “building” blocks for the secure exchange in the middle of the diagram, must be interoperable.
- Make sure that data offers and partners can be discovered in between dataspaces (see Data Transfer & Discoverability) .
- A minimum requirement is to utilize the dataspace protocol DSP and decentral claims protocol DCP, different implementations beside EDC and extensions to the protocol are possible. Note: DSP and DCP are in standardization ISO/IEC JTC-1 etc.
- Currently as described in this ADR[1] which was published from Factory-X, Construct-X, Semiconductor-X and Catena-X, the Eclipse Tractus-X Connector will support multi-dataspace configurations which can be defined by each Manufacturing-X dataspace on a structured way.
- For access & usage control the data sovereignty contract language is resolvable (ODRL specs). Frame contracts, at least a reference to standard policies is required. The Manufacturing-X governance topic group / potential association per industry e.g. Catena-X e.V., will define the policy frameworks (rules of the game) for the data exchange.

5.1.3 Resolvable Semantics:

- Once I can exchange “bytes” with data sovereignty in between companies, I must start thinking “as a data provider” how my “data consumer” can understand the data that is being consumed.
- Therefore, I need at least in a “high level” not a translator, but a “resolver”. I should be able to resolve the data semantics so I can understand it and maybe then translate it.
- Using JSON-LD for the end data (no manner how it was modelled, AAS Templates, SAMM, OPC-UA Companion Spec), could enable the interoperability between dataspaces, since this technology can be used to give context to any data attributes in a JSON payload (which can have embedded PDFs).
- Using the Eclipse Tractus-X KITs[2] to define the semantics for the use cases is a good practice, since the project is open source, and has in its scope creating base technologies, defining use cases that can be used in different industries Cross-

[1] https://github.com/eclipse-tractusx/tractusx-edc/blob/main/docs/development/decision-records/2026-01-07_multi-dataspace-support/README.md

[2] https://eclipse-tractusx.github.io/documentation/kit-framework

Manufacturing-X dataspaces.

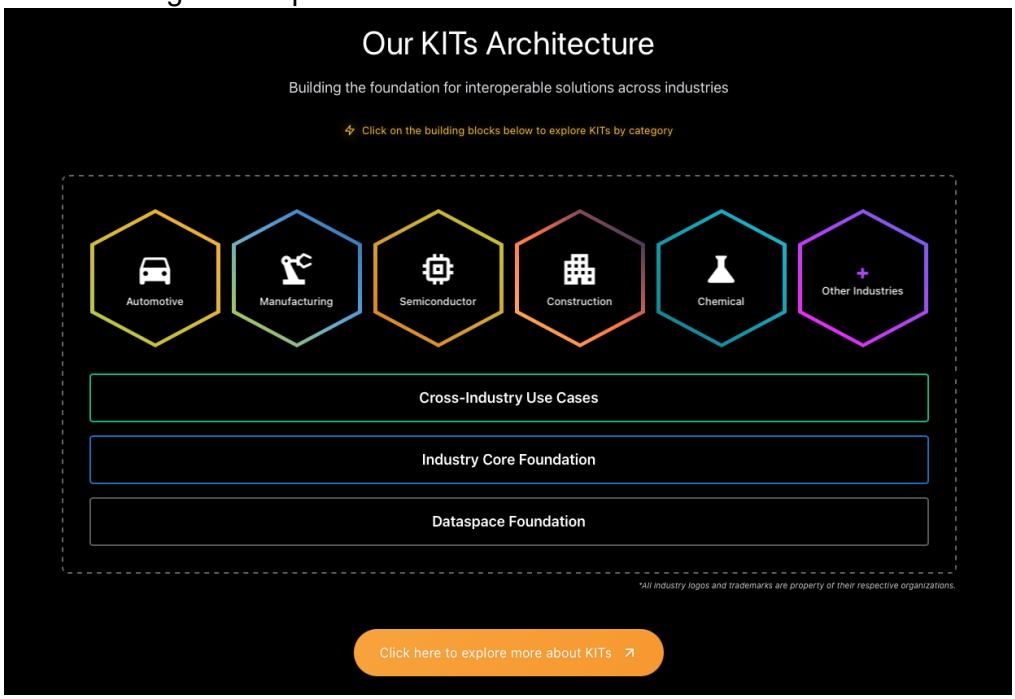


Figure 5: Eclipse Tractus-X KITs Architecture

For example:

- Using Verifiable Credentials (in JSON-LD) for the Inter-Dataspace Data Exchange enables data to travel with its semantic context and is able to be resolved for processing in the consumer side.
- In Tractus-X in the Digital Product Passport Verification example (a good cross dataspace use case): https://eclipse-tractusx.github.io/docs-kits/next/kits/data-trust-and-security-kit/adoption-view/

PCF is also one of the semantic models which would be used by multiple industries.

5.2 Cross Dataspace Data Transfer & Discoverability

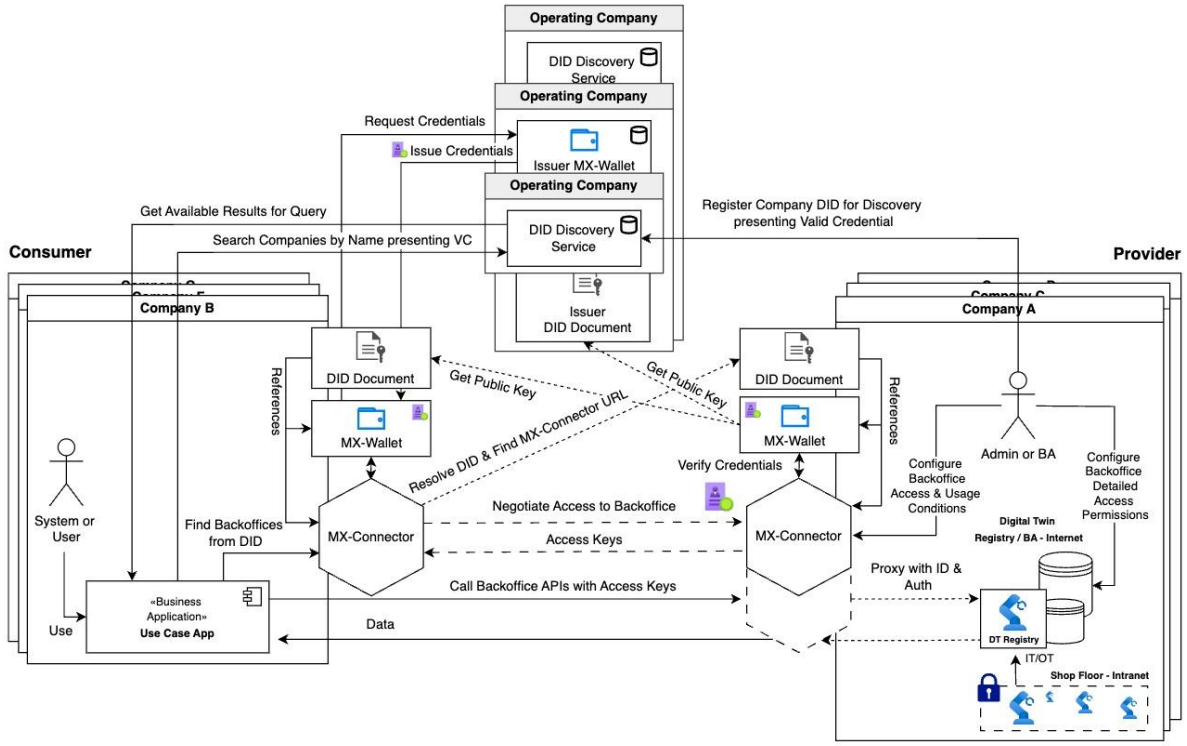


Figure 6 Data Transfer & Discoverability Context

Assuming two companies want to utilize DSP & DCP for the authorization to their systems on a cross-dataspace scenario, they will require a DID Document which allows the external world to verify content generated by you and ensure that the data exchange is “legally” bonded to your company.

5.2.1 Data Provider Clarifications

1. At the provider site,” ONLY” the Digital Twin applications (AAS or OPC-UA) & Business Apps will be made accessible to the public internet, this application can be called “dataplane”.
2. Because of security reasons, the Shop Floor is at a private intranet, it is insecure to do the IT/OT integration allowing another company to access your information directly at the shop floor. There will always be a backend or registry.
3. The access & usage conditions for the Digital Twin applications are provided by an admin or Business Application at the MX-Connector
4. Specific “Asset” access permissions can be configured directly at the Digital Twin applications (since it requires domain knowledge).

5.2.2 Data Consumer Clarifications

1. At the consumer side, only a business application is needed to start the consumption.

2. What happens when the data is retrieved is a company internal decision (if it goes to a system or is simply displayed).

5.3 Assumptions

1. An “dataspace” verifiable credential identity was obtained and exists at the MX-Wallet. If it was obtained at an operator (onboarding) or is fulfilling criteria like “having an EUID credential” is not defined in scope.
2. The internal company systems (Digital Twins) were previously configured with the correct access & usage permissions at the MX-Connector.
3. There is a way to synchronize the DID Discovery Services at the operators, and it is also not specified how and for how much time (since it can cost to keep your company in this “yellow” pages)
4. Only the DID as identifier will be stored at the discovery service. The DID Document resolution needs to be done by each use case application
5. The registration and reading at the DID discovery service is limited by participants who have proof of membership at Factory-X /MX.
6. Not every company can register themselves for a specific category, a “verifiable” proof needs to be presented that this company fulfills his role, example “MAAS” service provider. And how this credential is obtained is also not specified.
7. The Business Applications / Discovery Services / Systems are deployed in Kubernetes environments, which are accessible via URL using the Internet (HTTPS).
8. The DID method used for resolving the DID Documents is “did:web”.
9. The IT/OT integration is abstracted, and remains use case specific, securing the shop floor from direct internet access. The shop floor is excluded from the outside world, secured in an intranet.

5.4 Step 1: Registration for Discover

- Presenting Valid Verifiable Credentials for Authorization. That can be obtained on an onboarding (probably done at an operating company you know) or requested using the wallet an authorized operating company (not in scope how you get it).
- The operating companies will not share the “members” of the dataspace by default; they will only make available for discovery if the participating company requests their DID “ID” to be discovered under an “category/role” or via “company name”.
- The discovery services will be synchronized to avoid duplications.

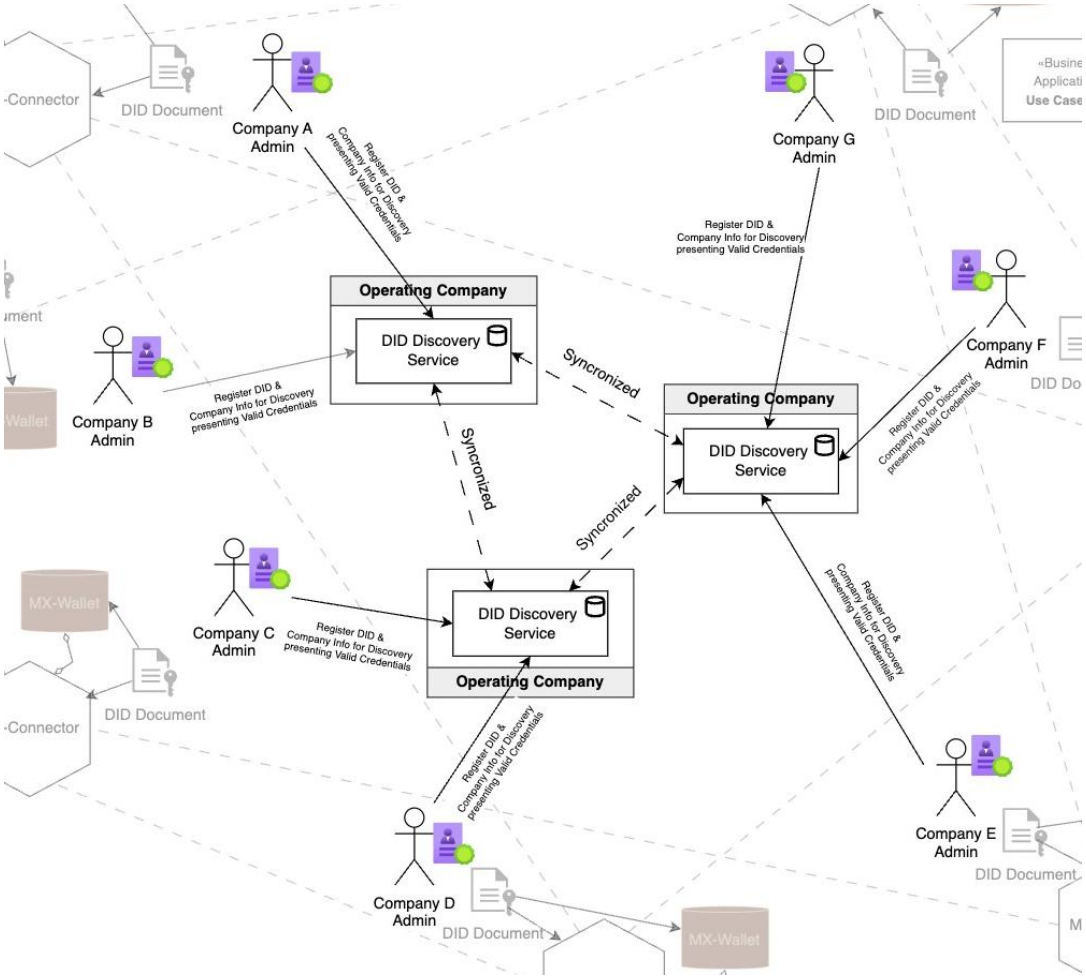


Figure 7 DID Registration at DID Discovery Service by multiple companies

5.5 Step 2: Partner Discovery

1. Search for the “Company A” or by a specific category like “DPP Service Provider”.
    - This would be checked by the Operating Company if the companies available fulfill this role at the Registration, requesting a claim for Security Reasons
    - This company will also use a Valid Verifiable Credential to proof they are members of the dataspace.
2. The Business Application which wants to consume data from “Company A” will need to use the “Universal DID:WEB Resolver” to find the DID Document from the DID found at the discovery service which includes the MX-Connector “Root” Catalog URL.

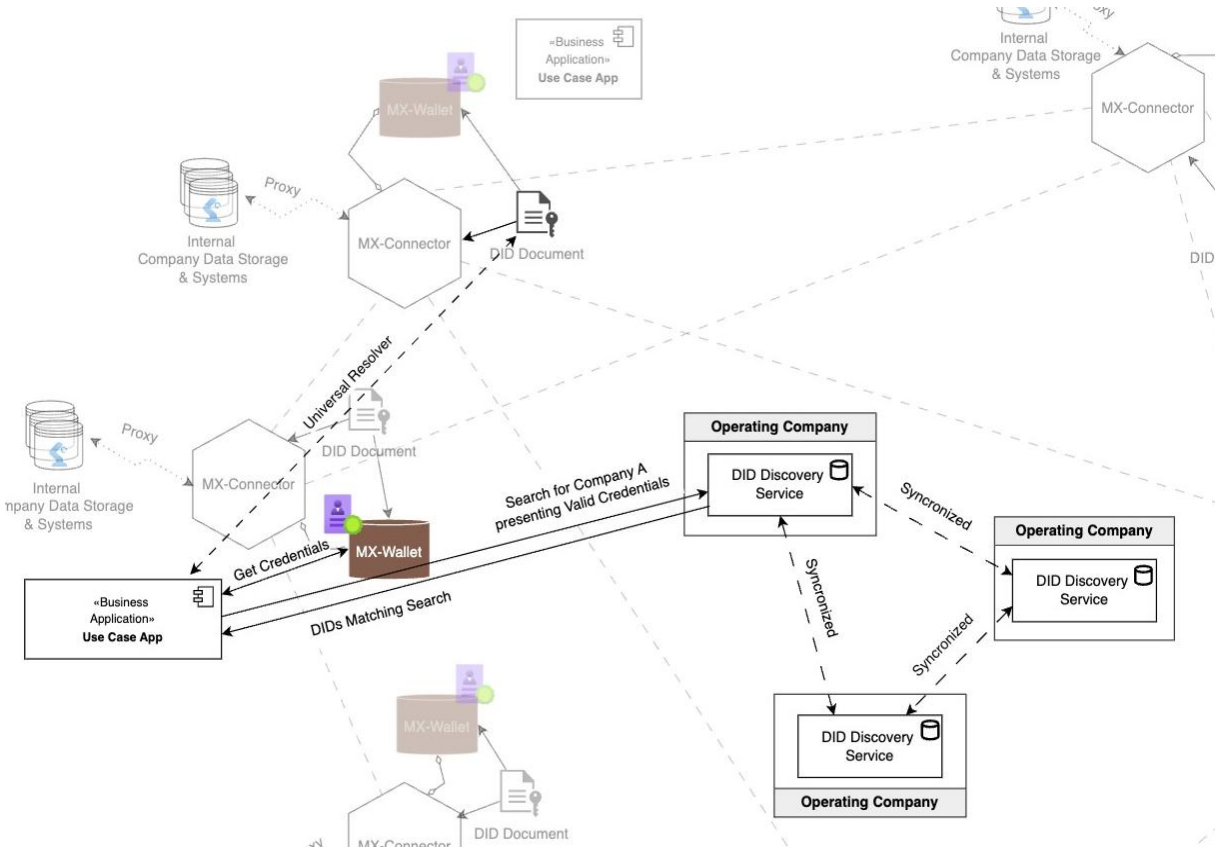


Figure 8 DID search by consumer business application & DID document resolution via did:web

5.6 Step 3: Data Exchange

1. Search the available systems and offers visible for you.
    - Using the DSP protocol and DCP the MX-Connector will filter the systems which you do not have access, so it will not be displayed for you.
    - Any system (AAS Server, OPC-UA Server, Business Application, etc) can be configured on “runtime” at the MX-Connector.
2. Once the Business Application selected & negotiated the access to a specific system and accepted the conditions of their provider partner, they will be able to access the systems using an Access Key.
    - Which application to be selected will depend on the “use case” specification and needs
    - More than one system can be accessible in parallel.
    - It will be proxied to the systems, so they will not be visible/exposed to the consumers because of security reasons.

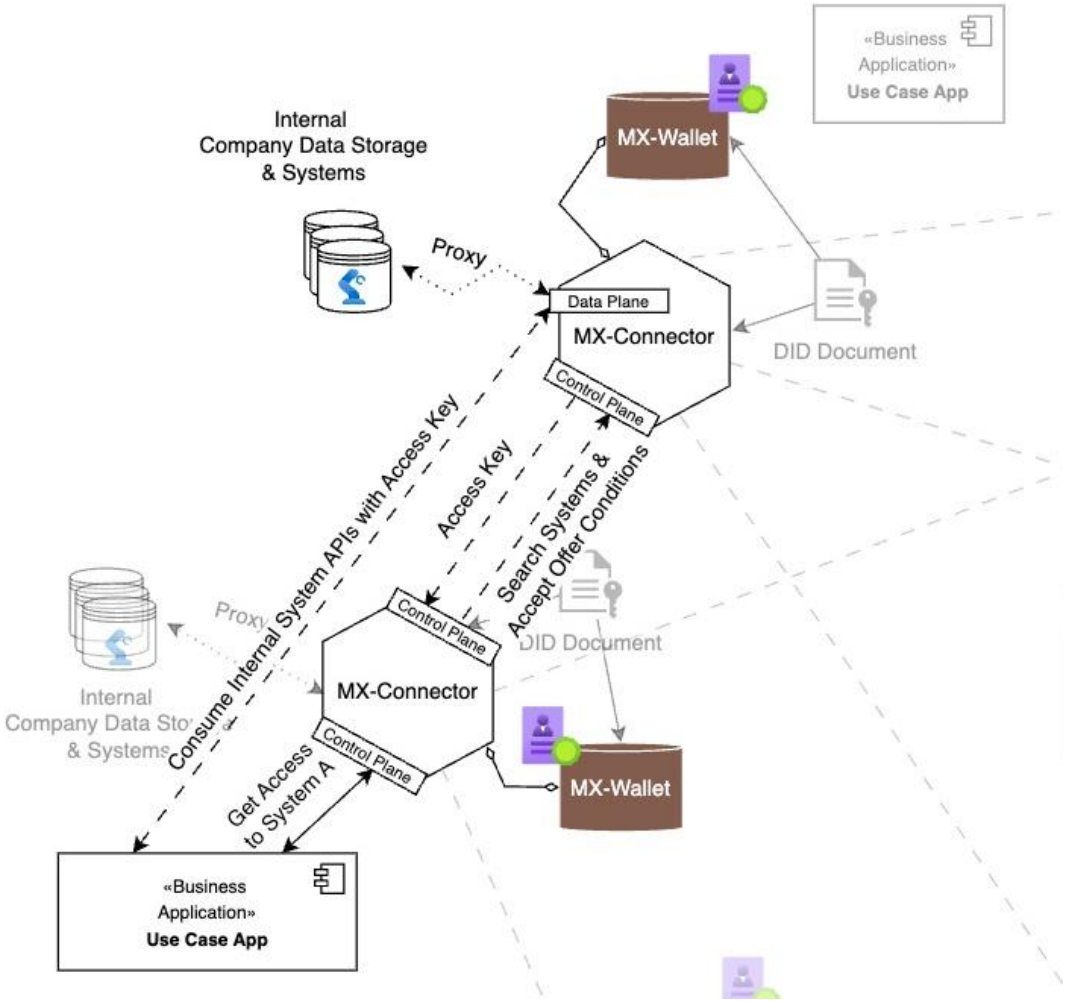


Figure 9 Data Exchange triggered by Data Consumer Business Application

Searching and accepting the System A usage conditions, being able to access the internal systems configured at the provider MX-Connector via the data plane proxy.

5.7 Step 4: Scale it.

By using this architecture for discoverability, the business applications can execute a decentral discovery by reusing their dataspace “membership” credentials to authenticate themselves and demonstrate their roles using claims (Verifiable Credentials), it is not in scope how these credentials are obtained.

It is scalable for all the different participants, facilitating them to find new customers and partners to do the data exchange and provide their services. Example use cases to use this would be PCF Calculation service providers, MAAS Services providers, Digital Product Passport Service Providers, etc.

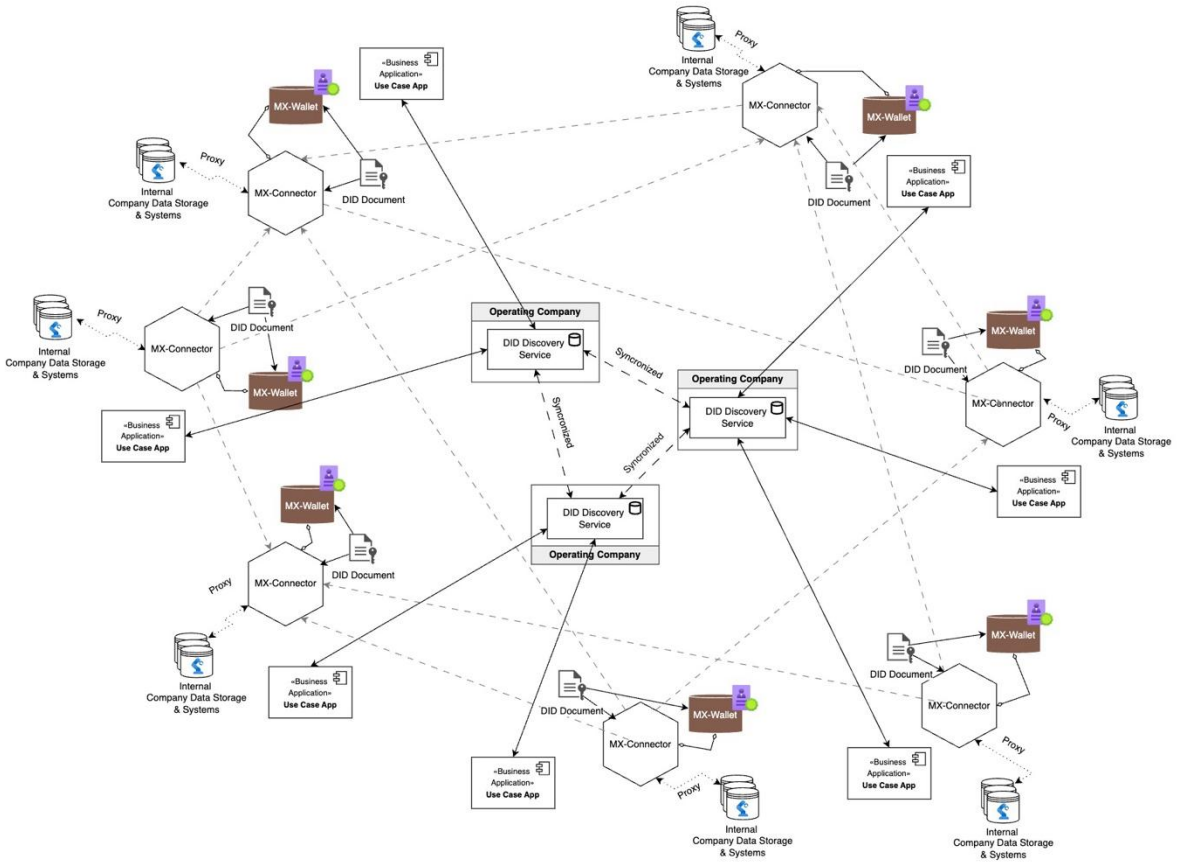


Figure 10 Scaled architecture to all dataspace participants.

Several dataspaces can synchronize their DID discovery services to make sure that inter dataspaces the participants are findable. It would be required to every dataspace to define if their members can be discoverable for other dataspace participants or not.

Disclaimer: There is currently no technical specification for this discovery mechanism, as a future line of work, an Eclipse Tractus-X Kits could be published with a more detailed implementation of the DID Discovery Service.

6 Overview of Data Space Governance, Functionalities and Services

6.1 Data Space Governance

The goal of dataspace governance is to create an ecosystem where stakeholders can safely and efficiently share data, unlocking its full potential while ensuring ethical and legal compliance.

6.2 Governance Structure based on IDSA-Rulebook

Data space governance can be defined on different layers. Those are inspired by the Design Principles for Data Spaces, where data space experts teamed up to define cross-sectoral principles for building data spaces.

IDSA-rulebook defines roles and processes within the data space related to the definition, creation, processing, and use of data.

6.3 General Governance Framework

The governance framework defines the structure, processes, and rules that guide how participants interact, share, and manage data within a dataspace.

6.4 Roles and Responsibilities

Roles and responsibilities within a dataspace governance framework define how different stakeholders interact, ensuring accountability and smooth operation. Key roles include Governing authority, Data providers, Data consumer, Data stewards, Service providers, Certifiers.

7 The Requirements for the Data exchange architecture

This to-be data exchange architecture shall accomplish the following:

1. Provide the following capabilities based on the Dataspace Support Center:
    - Interoperability
    - Trust & Security
    - Scalability
    - Data Sovereignty
2. Build on the standards from entities such as Gaia-X, Catena-X (e.g tractus-x kits), Platform Industrie 4.0, IDTA, SCI 4.0, OPC Foundation and the IPCEI-CIS.
3. Extend and expand these standards and results where necessary to:
    - accommodate connectivity down to the shop floor, which was not part of the Catena-X scope.
    - accommodate industry specific requirements.

Especially the last point reflects the fact, that while the results from the Catena-X project are not technologically limited to the Automotive industry, they have been designed to cover the specific needs of that industry with a focus on German OEMs. Working with companies outside this group has quickly shown, that additional requirements exist – both for the data exchange between companies (horizontal) and the data exchanged within a company (vertical).

8 The MX-Port Model

“Extending and expanding” will most likely mean that we must deal with different requirements that affect various parts of the existing architecture, and which can be on very different levels.

- From the perspective of a manufacturing company, there are two different supply chains:
- Supply chain regarding the **product** of the manufacturing company
  - All deliveries from suppliers that are **integrated** into the manufacturing company's product
  - Application scope of Catena-X
- Supply chain regarding the **production system** of the manufacturing company
  - All deliveries from suppliers that are needed to **build** and **operate** the manufacturing company's production system

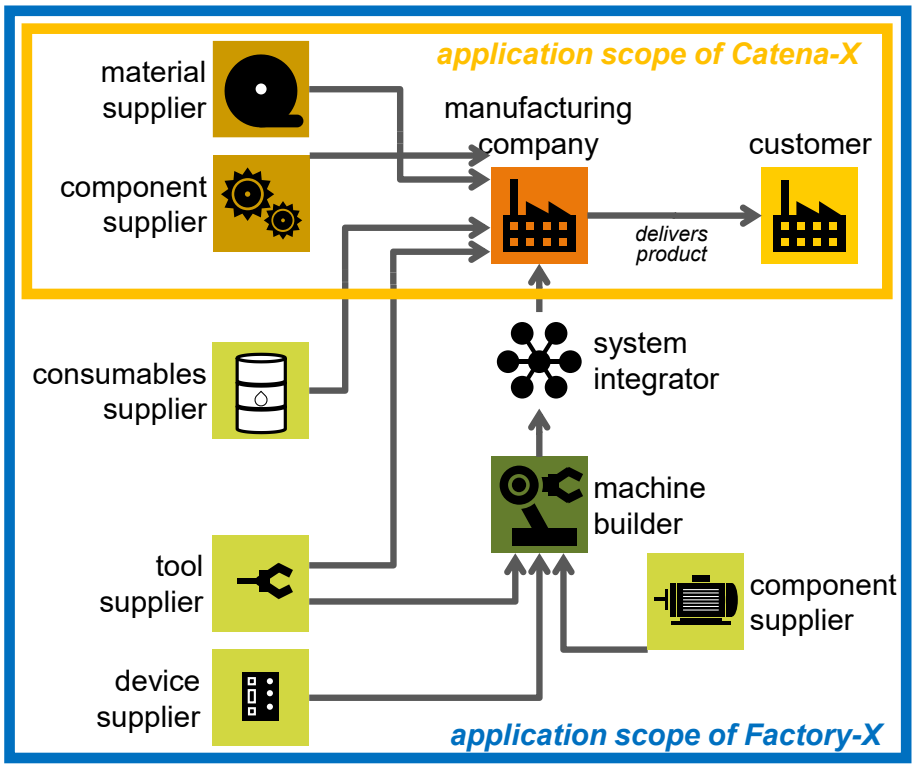


Figure 11 factory-x scope expansion

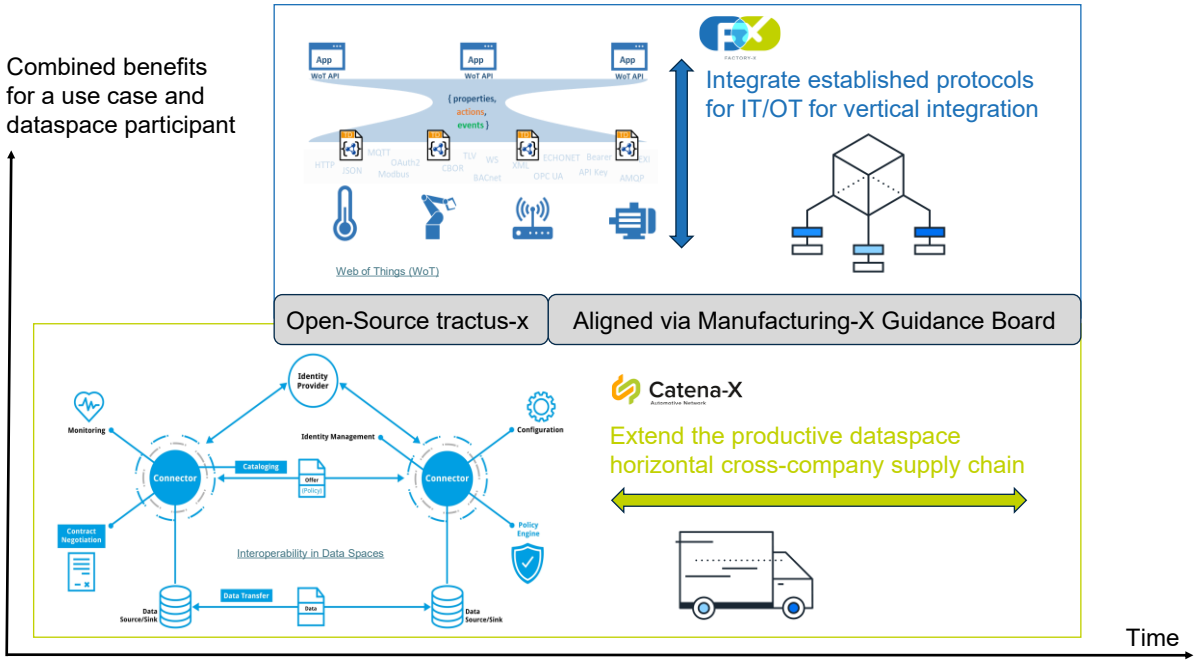


Figure 12 factory-x extending integration

To be able to structure these requirements logically and to find a way to understand, where exactly they are affecting the existing architecture, we have decided to define a concept which we call the „ MX-Port concept “. The MX-Port concept enables that:

- Business applications are integrated in a uniform manner.
- Existing software applications can be integrated without having to change them on the use-case-function-level.

The MX-Port is a structure defining logical layers similar to the OSI or RAMI Model.

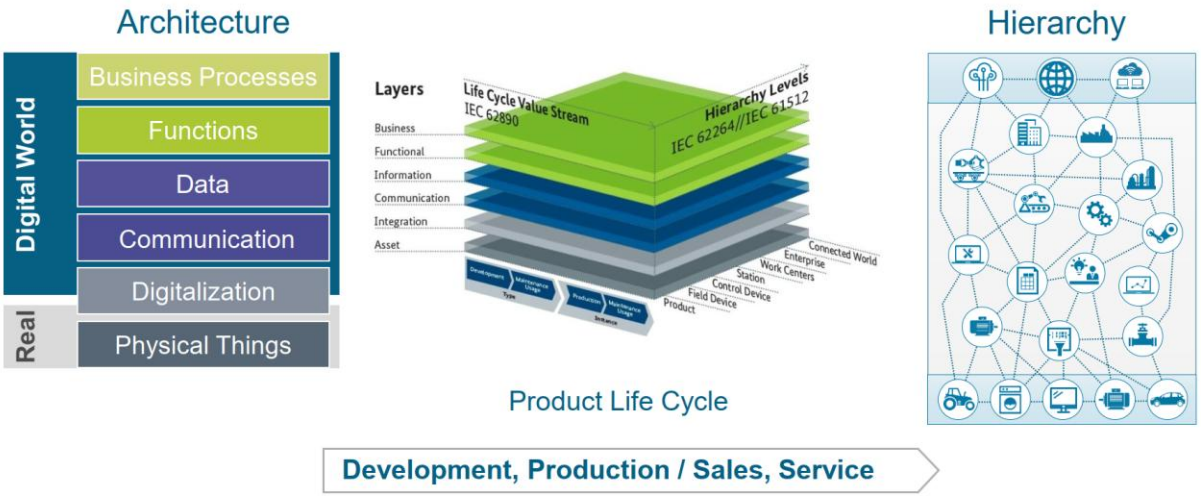


Figure 13 RAMI 4.0 Architecture Physical Objects to Dataspace

The MX-Port concept structures the complete technical data exchange stack, from the data source to the exchange within or between companies in the following 5 layers:

	Layer	Purpose
L5	Discovery	. . . is used to find offerings like data, partner or business applications
L4	Access & Usage Control	. . . is used to ensure that data providers can define the data access and usage themselves as well as restrict the access and usage of the provided data.
L3	Gate	. . . is used to exchange data in a uniform way
L2	Converter	. . . Enables the data that needs to be exchanged to use one semantic model
L1	Adapter	. . . enables any business application to use the MX-Port

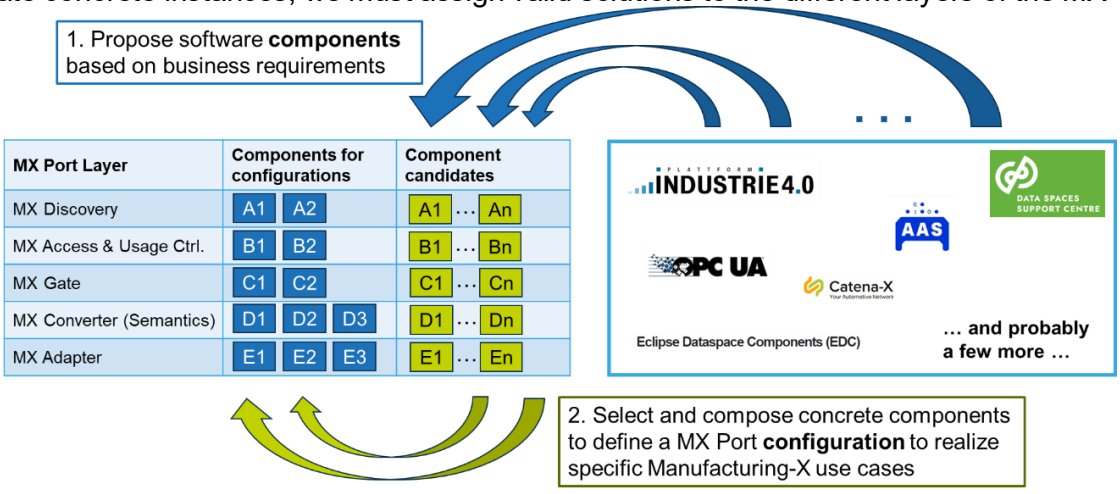
A clear consequence of this concept is that going forward there will be multiple configurations of the MX-Port concept, consisting of different software components. However, they will be structured identically and therefore enable interoperability according to the interoperability levels

- Data Interoperability,
- Intra-Data Space Interoperability,
- Cross-Data Space Interoperability,

as recommended by the Dataspace Support Center (https://dssc.eu/space/SK/812286015/3+-+Interoperability+and+Data+Quality).

9 Description of the shelf system: Working with the MX-Port

To create concrete instances, we must assign valid solutions to the different layers of the MX-Port.



This is done in a 2-step process:

Figure 14: Creation of MX-Port configurations (Source Factory-X)

In Step 1, requirements for solutions are typically made by use case owners based on concrete business, functional, commercial or other requirements. These solutions are most likely coming from a set of existing industry standards.

In Step 2, these proposals are validated against the required capabilities mentioned under (1.) in The Requirements:

- Interoperability
- Trust & Security
- Scalability
- Data Sovereignty

The proposals with the best fit will be selected as an MX-Port configuration.

- However, it is important to note that not all approved solutions can be combined freely amongst each other. There will be several implementations of the MX Port by different solutions and service providers.

10 MX-Port Configuration 1 based on Catena-X: “Hercules”

The first configuration is an adaptation (realized in Factory-X) of the current “Catena-X Architecture” to the MX-Port, which is briefly described in figure 5. Main element is the implementation of the DSP/DCP protocols for cross-company data sharing. We call this configuration “Hercules”.

	Layer	**MX-Port “Hercules”**
L5	Discovery	Data Space Protocol
L4	Access & Usage Control	Decentralized Claims Protocol => AAS Security
L3	Gate	AAS-REST
L2	Converter	AAS Submodels
L1	Adapter	Application specific

Figure 11 MX-Port configuration "Hercules" (Source Factory-X)

Hercules describes a B2B exchange in between two systems which understand the same protocols. AAS Security is also needed for the asset level access control, which is done at the AAS-REST level, where the MX-Connector uses a company internal Oauth2 to get access to the AAS-REST APIs via a proxy, which is agnostic to what DSP & DCP define. DSP is agnostic to which data type is exchanged after the access keys are obtained.

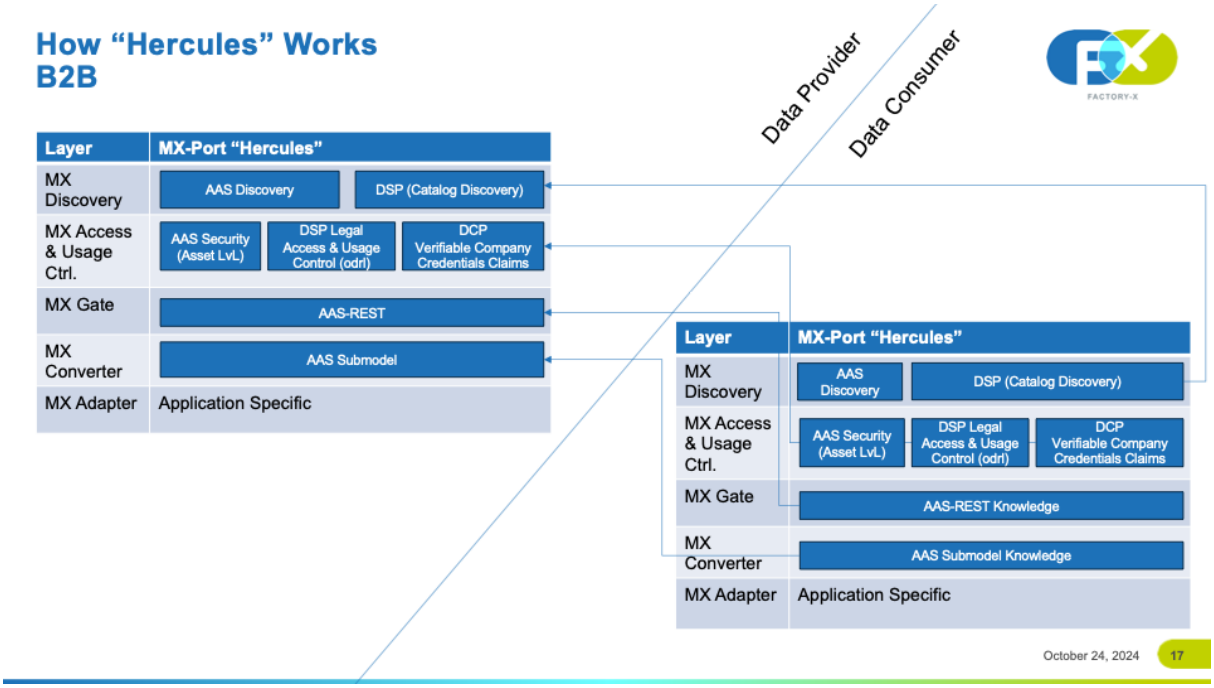


Figure 15: Hercules Data Exchange

10.1 Catena-X MX-Port Configuration Approach

It is important to note that Catena-X does not impose any “configuration” limitations on how gate services can be used. In Catena-X, it is possible to connect any Gate—regardless of the specific use case—to the discoverability, access, and usage control layers. These Gates can be AAS-REST, OPC-UA REST, or business applications from various use cases. Each of these can define their own data models using the open-source Eclipse SAMM meta models and attach these models to the AAS or OPC-UA registries. As already demonstrated[3], the Catena-X Data Models are available at the OPC-UA Companion Specs library can be used.

Catena-X aims to achieve dataspace and use case interoperability, so no vertical integrations are limited at “deployment” level. Since at runtime they can be discoverable by each use case business application. Each use case can specify which system to select/usage, under each condition and when. Additionally other discovery mechanisms & authentication mechanism are allowed to be used like the AAS Security for setting security restrictions at asset level & AAS Discovery (AAS Lookup) for finding the different Assets at the AAS-Rest. This is a benefit from the DSP implementation (MX-Connector) which allows business applications in runtime to select which system/data endpoint, if their company has access to it & accept the usage conditions, because the MX-Connector remains agnostic of the implementation or data format, it only requires a simple HTTP endpoint, and can be extended to MQTT, WebSockets, TCP or any other transfer protocol, since DSP is extendable.

10.2 The Catena-X Implementation

Using Dataspace Protocol (DSP) & Decentralized Claims Protocol (DCP) for authorization and authentication, Catena-X allows a decentral data exchange and access to services configured at Runtime. The access and usage permissions are handled using self-sovereign identities

[3] https://opcfoundation.org/wp-content/uploads/2025/08/OPCF-Catena-X-Architecture-Whitepaper-v1.0.pdf

which are stored in wallets. In the case of Catena-X the MX-Connector implementation utilized is the Eclipse Tractus-X Eclipse Dataspace Components Connector (TX-EDC Connector). The MX-Connector can manage the access and usage control of the services in runtime, so both OPC-UA or AAS Servers or Business Applications can coexist and be accessible by consumer connectors on runtime. It is defined by each use case when to access one or another

The architecture of dataspaces specified at the International Dataspace Association[4] is of Data Consumer & Data Providers, the data provider shares the data beforehand allowing certain “Access & Usage Permissions” to its systems. Additionally, an Oauth2 IDP can be used by the company to set additional permission to “Assets” using AAS Security (IEC 63278 / IDTA), so that the permission can derive until asset level. This authorization is then delegated to the Application behind the connector, which would verify if the claims provided are matching with the authorization configured to the specific asset.

Protocol	Component	Reference Implementations (FOSS + COTS)
DSP	MX-Connector	Tractus-X EDC Connector, SoviCore Connect, Connect & Integrate, Dataspace OS, more implementations.
DCP	MX-Wallet	Tractus-X Identity Hub, SAP DIM Wallet, more implementations[5].

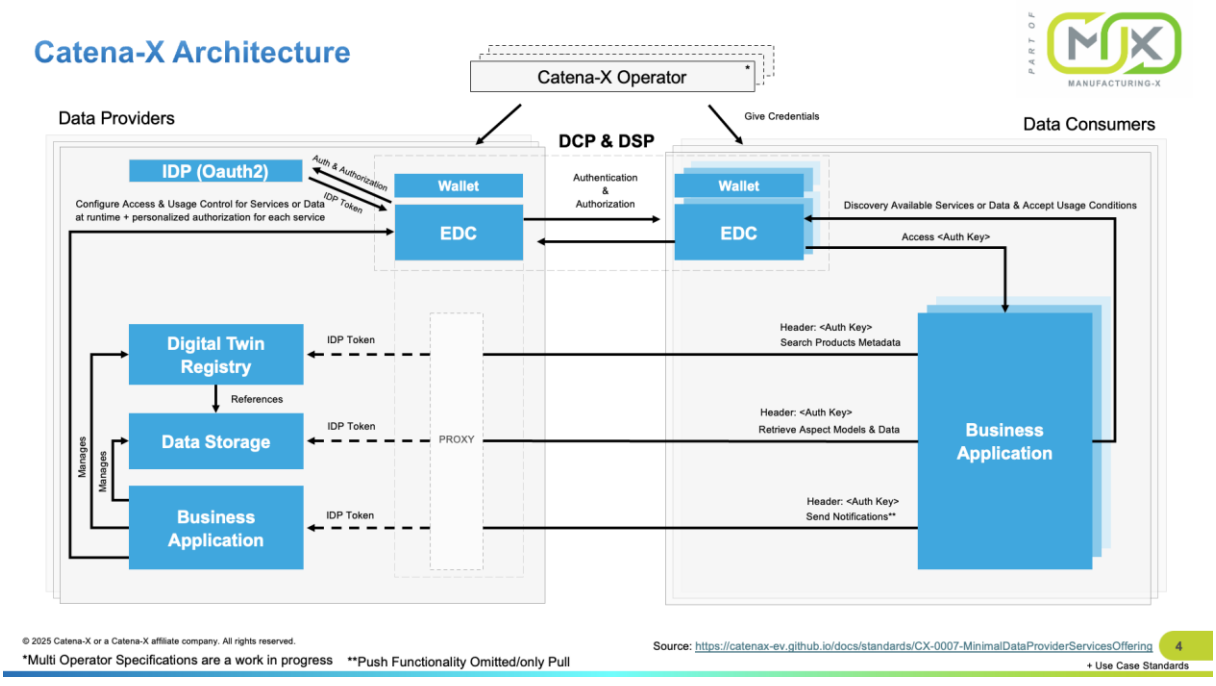


Figure 16 Catena-X Architecture

DSP & DCP are just protocols, and do not define how the implementation is taking place. However, if an implementation of DSP & DCP would take place they will be like the official reference implementation of these two protocols: the Eclipse Dataspace Components project.

[4] https://internationaldataspaces.org/why/data-spaces/
[5] https://www.cofinity-x.com/apps?case=core-setup&page=1

Which provides a code framework for building Connectors (EDC Connector), Identity Wallets (Identity Hub) and more. In the case of Catena-X the Eclipse Dataspace Components framework is used to build a “instance” version of the connector, in this case the Tractus-X EDC, as described in the EDC known friends, it provides an extension of the EDC Connector for “Manufacturing-X” dataspaces that are based on the Catena-X data ecosystem. The Tractus-X EDC focuses on the automatization of the data exchange and contract negotiation without human interaction. Additionally, it offers several optimizations like the “Endpoint Data Reference” (EDR) interface which simplifies the data negotiation and transfer mechanism, handling token callback for the business applications. It provides also a token refresh handler, an optional BPN-DID resolution service for easier identification of the partners and “restricts” the usage of “odrl” policies based on legal requirements, provided by several company lawyers, which stablished the governance/regulatory framework from Catena-X, enabling the data exchange in a data ecosystem, via this EDC Connector, to be done with legal coverage. Additionally, this EDC Connector offers a deployment configuration via Helm Charts and an extensive architecture documentation from Business/Adoption Level to Development/Operation Level in the Eclipse Tractus-X Connector KIT. Currently the Eclipse Tractus-X EDC Connector as described in this ADR is being enabled for Multi-Dataspace usage and extension, with the focus on Manufacturing-X projects.

10.3 Digital Twin Registry

In Catena-X provides a decentral Digital Twin Registry (dDTR) (AAS-REST) system which each company is responsible to operate. As specified at the Catena-X Standard CX-0002 it is built according to the IDTA Asset Administration Shell v3.0 Part 2: API Specifications.

Protocol	Component	Reference Implementations (FOSS + COTS)
AAS	AAS-REST Registry	Tractus-X Digital Twin Registry[6], BASYX[7], AAS-Suite[8], FA³ST, + more implementations

This are the following normative references used in the Catena-X Standard CX-0002 for AAS-REST:

- Specification of the Asset Administration Shell - Part 1: Metamodel. V3.0, April 2023, IDTA number: 01001-3-0 On IDTA Content Hub (direct link)
- Specification of the Asset Administration Shell - Part 2: Application Programming Interfaces. V3.0, April 2023, IDTA number: 01002-03-1 On IDTA Content Hub (direct link)

Named as “Digital Twin”, the AAS can be abstracted for a specific functionality when handling “component” assets, allowing an easier usage by use cases like “Traceability”. Having it named in an abstract way, give advantages when integrating OPC-UA & AAS, since both would match the Digital Twin concept.

[6] https://github.com/eclipse-tractusx/sldt-digital-twin-registry

[7] https://github.com/eclipse-basyx

[8] In Development: https://github.com/eclipse-tractusx/aas-suite/tree/main

10.4 Semantic Modelling

At Catena-X, each use cases are responsible for specifying their own meta models, which can then be placed on Digital Twins (AAS), OPC-UA, or provided by any Business Applications (PCF, DPP, etc). For that as specified in the standard CX-0003, the Eclipse Semantic Modeling Framework (ESMF) is used, which allows interoperability with the IDTA AAS Submodel Templates, and flexibility for every use case to combine, specify and standardize their own Aspect Meta Model data structures. For that Semantic Aspect Meta Model (SAMM) is used, see here all the open source Tractus-X aspect models, which can be reused and expanded by each dataspace initiative (since it is an open source project). All the models are modeled in “.ttl” and extension from “.rdf” and can generate different instance objects like “.json” (example), “.xml” (example), “.aasx” (example) and others, providing schemas (example) that can be validate the syntax.

10.5 Tractus-X Connector as MX-Connector

The Tractus-X EDC Connector was built with the intention of proving a reference implementation and an open-source interoperability collaboration point for all Manufacturing-X, based on the work done at the Catena-X Consortia and further Catena-X e.V. work. With the MX-Connector based on the EDC Framework, which implements the Dataspace Protocol (DSP), and the MX-Wallet (based on the Identity Hub reference implementation from the EDC Framework) which implements the Decentralized Claims Protocol (DCP) we are able to achieve interoperability and stablish a common company to company (B2B) interface across dataspaces. Currently as described in this ADR[9] which was published from contributors of Factory-X, Construct-X, Semiconductor-X and Catena-X, the Eclipse Tractus-X Connector will support multi-dataspace configurations which can be defined by each Manufacturing-X dataspace on a structured way.

[9] https://github.com/eclipse-tractusx/tractusx-edc/blob/main/docs/development/decision-records/2026-01-07_multi-dataspace-support/README.md

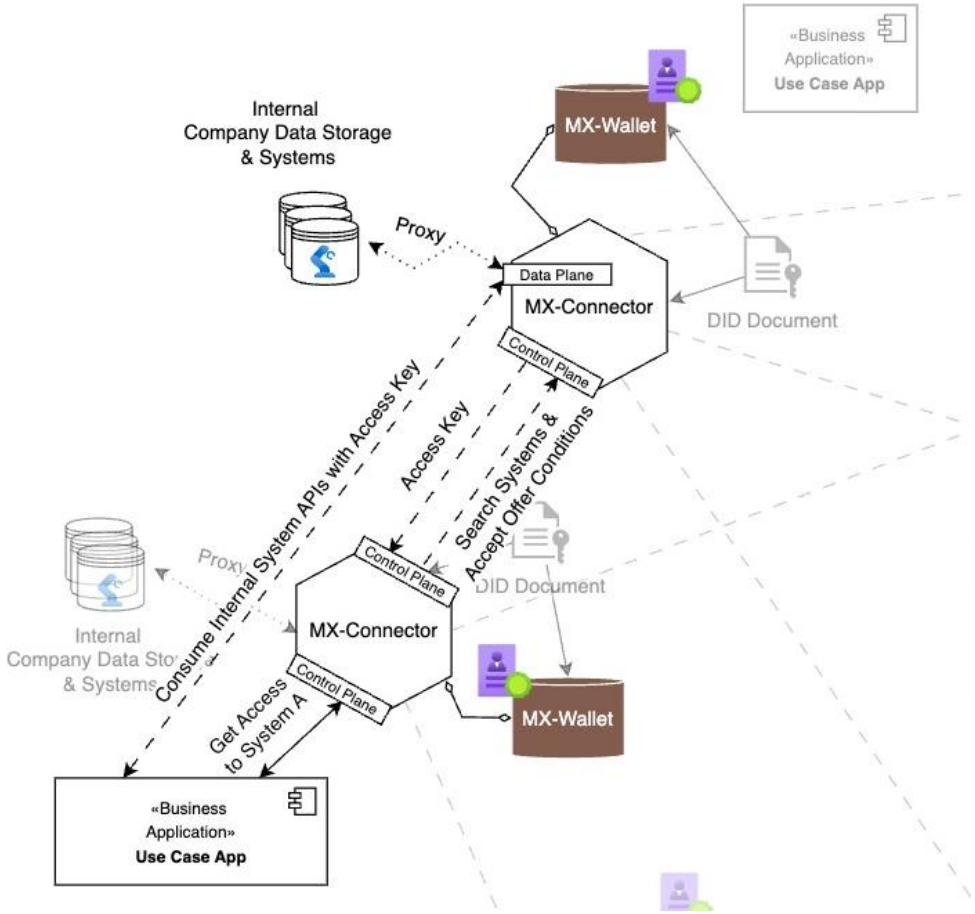


Figure 17 Data Exchange context with MX-Connector & MX-Wallet for DSP & DCP

Having a consumer business application which is built with the requirements from a specific use case like (PCF, DPP or others), the MX-Connector (TX-EDC) is able to indicate to the Business Application (BA) which services are available at runtime (OPC-UA, AAS Server, another BA, etc), so depending on the use cases and what is visible for your company at the provider connector it will be able to retrieve data from different services based on your company identity and which agreements you have accepted.

10.6 Complexity Reduction for Easy Dataspace Adoption

A common critic from service providers to the dataspace technologies like (DSP & DCP) is that the learning curve and technological adoption complexity is advanced, and that is due to the fact that most adopters start implementing the functionality directly by the protocol description, which is very complex for dataspace beginners.

“Start developing / adopting a dataspace application directly by the DSP/DCP protocols, is like in the first time you want to develop a WebApp, you start by re-developing the HTTP protocol interactions on the byte level, instead of just using a library and a browser! It is clearly complex!”

So, with the objective to reduce the complexity of the usage of the MX-Connector, MX-Wallet, AAS-REST/ dDTR, OPC-UA and other technologies, especially for Small and Medium Enterprises (SMEs), an open-source Software Development KIT (SDK) was developed and is

available for integration at business applications, providing use case agnostic integration. technologies for data provisioning and data consumption. This SDK is the Tractus-X SDK which can be integrate by various use case applications, it is based on the concept of the Industry Core, providing interoperability in between use cases across Dataspaces. One first reference implementation which uses the TX-SDK is the Industry Core Hub for example.

Component	Language	Reference Implementation
SDK	Python	Tractus-X SDK[10]

It would be an opportunity for Manufacturing-X to extend this SDK and provide different “Adapters” & “Converters” for easing their vertical integration with internal company systems (e.g. ERP, DB, Cloud, etc).

10.6.1 What is the Tractus-X SDK?

The Eclipse Tractus-X SDK is a modular use case agnostic library crafted by the dataspace building community for the community. It facilitates developers on their tasks of developing use case applications, speeding the development and reducing the complexity of using the several dataspace components which Eclipse Tractus-X offers.

It makes maintenance easy on a long run and enables companies to produce their own dataspace ready applications faster and easier for certification. Allowing the developer to combine the "Building Blocks" in the way he desires to fulfil the requirements he has.

The Tractus-X SDK is built replicating what the Industry Core aims to provide: Interoperability for the use cases and reduction of development cost when adopting new use cases. It allows small and medium enterprises to integrate this in their existing business applications and CI/CD pipelines to dataspace technologies.

It was developed in Python to facilitate the understanding of the algorithms and the code. It is available in PyPi[5] and can be used in multiple scenarios:

- CI/CD Pipelines
- Jupiter Notebooks (AI, Data Analytics)
- Scripting
- Microservices (FastAPI, Flask)
- Cloud (Lambdas)

It is a great benefit when Artificial Intelligence (AI) comes into play, allowing data to be retrieve from multiple partners in a dataspace under “legal” conditions in an automatized way using DSP & DCP. More documentation can be found in the TX-SDK Specification.

11 MX-Port Configuration 2 based on requirements from Factory-X: “Leo”

This chapter is based on the document FX-0045 FX-UC-MX-Port-Configuration-Leo.docx, Version 1.0, September 22nd, 2025, source: https://factory-x.org/downloads/. The text has some editorial changes and has been condensed.

[10] Available in PyPi: https://pypi.org/project/tractusx-sdk/

11.1 Motivation of MX-Port configuration “Leo”

Factory-X will develop a digital ecosystem for factory outfitters and factory operators and considers a **large and diverse** range of machine builders, component suppliers, factory operators and software application providers. Therefore, Factory-X is moving beyond a “one-size-fits-all” approach based on the concept of a modular MX-Port, see [1]. The modular MX-Port enables software applications to be integrated in a uniform manner and existing software applications can be integrated without having to change them.

The modular MX-Port has a layered structure with different functional manifestations per layer and a use case, or a data ecosystem can configure a specific MX-Port according to its needs. For more details see [2] and [3]. In a first step, Factory-X uses the modular MX-Port to realize an **MX-Port configuration “Leo”** and an **MX-Port configuration “Hercules”**, see Figure 18 for illustration.

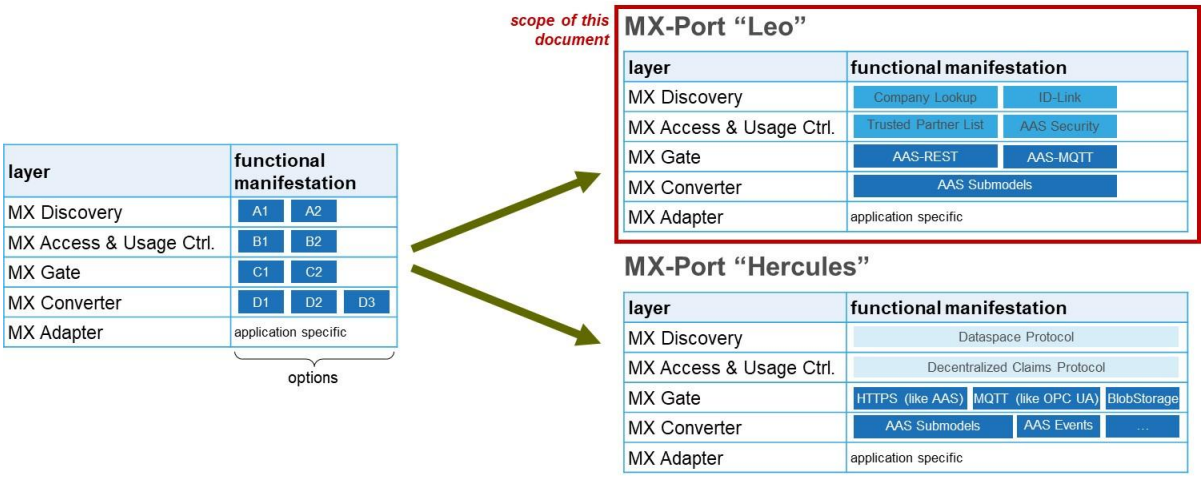


Figure 18: Using the modular MX-Port to realize the MX-Port configurations “Leo” and “Hercules”

The MX-Port configuration “Leo” is compliant with IEC 63278, see [4] / 61406, see [5] / IDTA and uses the Asset Administration Shell (AAS) as integration technology for cross-company data sharing[11].

The purpose of this chapter is to describe the MX-Port configuration “Leo”. The document describes (logical) concepts and no implementation aspects. It is feasible regarding different technical implementations and implementation technologies[12]. The aim of the document is to be understandable even for non-software architects. In particular, the product owner of the Factory-X use cases should be able to evaluate the contents of this document regarding the impact on their use case.

This document continues the Factory-X Use Cases Application Guide, see [2], and describes a design decision to implement the technical view of the Factory-X use cases (based on MX-Port) using the AAS concept. To put it simple, business applications acting as responders are implemented by an AAS server, and business applications acting as requesters are implemented by an AAS client.

[11] The MX-Port concept is designed to be used for both intra-company and cross-company data exchange. For intra-company data exchange, “lightweight” concepts can be used for the MX Discovery and MX Access & Usage Control layers.

[12] It is the task of the Factory-X architecture team to make suggestions as to the extent to which reuse of existing implementations is possible.

11.2 Stepwise approach of MX-Port configuration “Leo”

Factory-X aims to ensure that **as many** factory outfitters and factory operators **as possible** submit to these general rules. Therefore, the general rules must be designed in such a way that the ratio of necessary investment to expected benefit is **economically attractive** for as many companies as possible. A **balance** must be struck so that the entry barrier is **not set too high** – otherwise there is a risk that not enough companies will submit to the general rules – but also **not too low** – otherwise there is a risk that these general rules do not simplify cross-company data sharing sufficiently.

Due to the different starting positions and goals of the individual companies, Factory-X pursues a solution approach in the form of **successive steps building on each other** (roadmap for the companies). The individual companies can initially focus on the step whose implementation offers them the most suitable cost/benefit ratio regarding their individual starting position and goal. After implementing the selected step, companies have the option of implementing further steps based on this to achieve further benefits through additional investments.

Figure 19 illustrates successive steps building on each other of Factory-X. Note that the steps are modular in the sense that step 2 and step 3 can be swapped. A key requirement emerging from the Factory-X use cases is that cross-company data sharing is possible if a data provider provides an AAS server or a data consumer provides an AAS client in accordance with the specifications of IEC 63278 / IEC 61406 / IDTA.

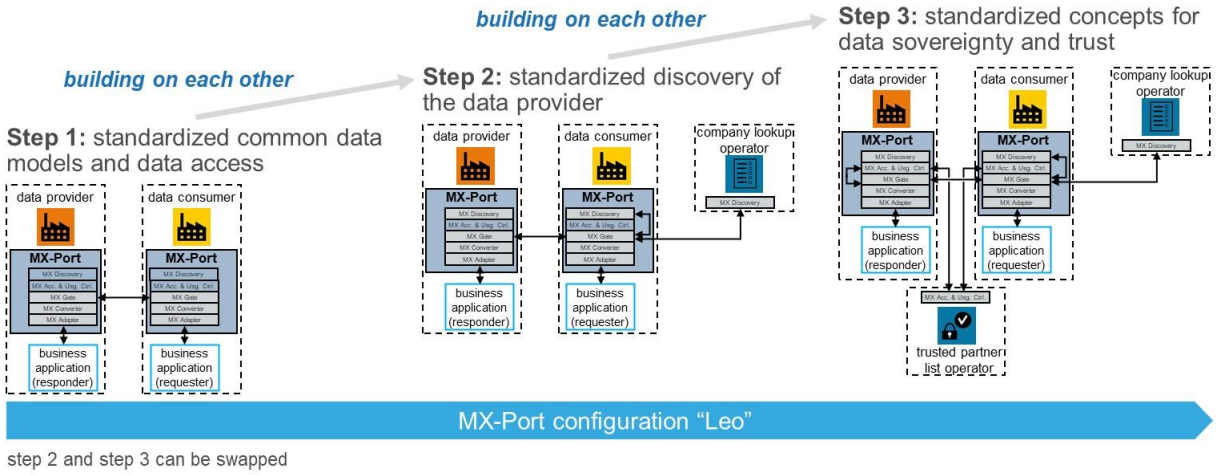


Figure 19: MX-Port configuration “Leo” paves the way for companies to be able to share data with many partners in the future (illustration)

- Step 1: standardized common data models and data access: The necessary requirements regarding the discovery of data provider, the data sovereignty of the data provider, and mutual trust of data provider and data consumer will be clarified among the affected companies individually, as is the case today.
- Step 2: standardized discovery of the data provider: The necessary requirements regarding the data sovereignty of the data provider, and mutual trust of data provider and data consumer will be clarified among the affected companies individually, as is the case today.

- Step 3: standardized concepts for data sovereignty and trust: The basic concept is a list of trusted partners, which can be maintained by the data provider or a 3rd party operating company. The list of trusted partners can be implemented in various forms and there are various options the list can be maintained. It still needs to be analyzed in more detail which of these options will be implemented prototypically in the Factory-X project.

The MX-Port configuration “Leo” addresses the implementation of all steps 1 to 3.

11.2.1 Step 1 standardized common data models and data access

Initial Situation: Manufacturing companies are increasingly feeling the pressure to make data available for various purposes and partners (suppliers, customers, authorities, etc.) in a computer-processable format. However, many manufacturing companies (>90%) are currently unable to make their diverse internal data available in a way that others can easily understand and process. Often, the data that they initially want to share with other partners is public or available only in a proprietary format.

Why: Step 1 creates the conditions for manufacturing companies to make the necessary, but sometimes significant, investments so that they can gradually implement the increasing requirements.

What: Manufacturing companies gradually convert internal data into a uniform representation that supports an explicit encoding of semantics utilizing standardized data models, so that the data becomes **understandable in terms of content.** Furthermore, they implement standardized interfaces for providing access to data according to these data models, so that the data becomes **easily accessible** through well-defined access paths at a suitable granularity.

How: Focus on MX Gate, MX Converter, and MX Adapter. Adapters play the role of mediating between proprietary forms of access to legacy systems and the desired harmonized access methods. Converters transform payloads of adapted messages to the representation form that adheres to the standardized common data models, both syntactically and semantically. Gates expose the thus converted information to the outside communication partner that conforms with the MX-Port ensuring standardized common data access.

11.2.2 Step 2: standardized discovery of the data provider

Initial Situation: The manufacturing companies providing data want to determine for themselves whom and under what conditions they make their data available. They have established solutions in place to secure their own data and want to use these existing solutions to share data with companies and partners with whom they already have established business relationships. They are developing initial business cases for cross-company data sharing and are testing market entry with selected pilot customers and partners; they therefore initially have no need to share data with many companies and partners. However, companies are increasingly faced with the burden of administering their established solutions. Therefore, they want to be able to organize discovery and administration information consistently across companies.

Why: Step 2 allows the data providers to make themselves and their capabilities known to data consumers by registering themself and their capabilities in a standardized way. Step 2 creates the opportunity for manufacturing companies to share sensitive data with other companies based on existing solutions while maintaining their data sovereignty, but to reduce the administrative effort of established solutions.

What: Manufacturing companies that want to provide data use the solutions they use to secure their own data and negotiate interactions with other companies and partners bilaterally and they offer external software applications standardized access to their own data or software applications. In addition, companies reduce the administrative effort of their established solutions through standardized discovery and administration information across companies. Especially when sharing data with existing partners, they can be informed about configuration changes in a uniform and automated manner and can also easily integrate new partners from a technical perspective. A standardized discovery can be deployed centrally and at any data consumer allowing the data provider to register itself and its capabilities. The data provider has full control over what information is shared and who can access it, what is available centrally, what locally with restricted access at the data provider and what is not shared. Step 2 enables mixed operation with Step 1 in the sense that companies submitting to the rules underlying Step 2 can also share data with companies based on the rules of Step 1.

How: Focus on MX Discovery and company-specific implementation of FX Access and Usage Control.

11.2.3 Step 3: standardized concepts for data sovereignty and trust

Initial Situation: Manufacturing companies are increasingly sharing their data with more companies and partners and are recognizing the increasing complexity of their specific solutions because bilaterally negotiated interactions and individually defined access and usage policies are reaching their limits in terms of distribution and scalability. They are increasingly understanding the advantages and benefits of 3rd party operating companies for identification and authentication, but do not want to be locked in by a specific 3rd party operating company. Companies are also increasingly understanding the advantages and benefits of a tightly knit consortium regarding onboarding **new** companies and partners.

Why: Step 3 creates the opportunity for manufacturing companies to extend their specific solutions based on bilaterally negotiated interactions to scale to many companies and partners.

What: Manufacturing companies use a list of trusted partners and integrate their existing identity and access management systems into this concept. This allows identification and authentication to be standardized across companies while still allowing companies to continue using their existing identity and access management systems. In addition to the advantages of this technical standardization, this list of trusted partners can also be maintained by a 3rd party operating company of their own choice. In this case, the onboarding of new business partners can also be managed centrally by the 3rd party operating company and companies must answer the question of what level of trust they want to achieve and which procedural issues they are willing to leave to such a 3rd party operating company. Step 3 enables mixed operation with Step 2 in the sense that companies submitting to the rules underlying Step 3 can also share data with companies based on the rules of Step 2 or Step 1.

How: Focus on MX Access and Usage Control with onboarding, identification and authentication by one or multiple 3rd party operating companies.

11.3 Asset Administration Shell

This document considers the **concept** of AAS, and not its implementation. The basis for these considerations is the internationally agreed standard IEC 63278-1, see [4]. Figure 20 shows the overview of the AAS and related entities as considered in this document. This document supplements the terminology of IEC 63278-1 with the concept of an AAS server. An AAS server is a software service that manages a set of AASs, understood as a concept, and not as an implementation. For reasons of symmetry, the term AAS client is also used, but this is a synonym for AAS user application.

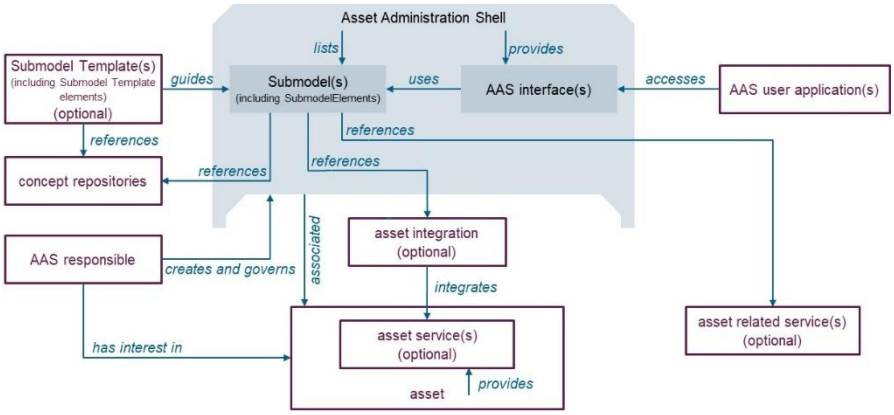


Figure 20: Detailed overview of Asset Administration Shell and related entities, see [4]

11.4 Application of AAS in MX-Port configuration “Leo”

This chapter describes how the concepts of business applications, legacy applications, MX-Port as described in [2] are conceptually mapped to the AAS concepts shown in Figure 20.

If business or legacy applications want to exchange data, according to [2], one business or legacy application acts as requester and the other one as responder. The MX-Port configuration “Leo” is characterized by the following design decision:

- A business or legacy application acting as requester shall be implemented by an **AAS client** wrapping the business or legacy application. This means that the AAS client requests data by accessing the AAS interfaces of the AASs managed by an AAS server.
- A business or legacy application acting as responder shall be implemented by an **AAS server** connected to the business logic of the business or legacy application and mapping to its internal data model. This means that the AAS server provides the requested data in the form of AASs/Submodels/SubmodelElements and, for this purpose, provides the appropriate AAS interfaces for the managed AASs.

It is now the responsibility of the individual Factory-X use cases to make the following decisions:

- What are the **assets** considered in the use case?

- What are the AASs associated to the assets including the Submodels and Submodel-Elements of the AASs in the use case?
- Which AAS user applications will be provided?
- Which asset related services, asset integration and asset services will be provided?
- Which Submodel templates and concept repositories are used?

11.4.1 Identification of assets and AASs

By choosing AAS as the integration technology for the MX-Port configuration “Leo”, exchanged data always relates to an asset. Each asset has an asset ID as a unique identifier in accordance with IEC 61406, which in the case of physical assets can be applied as a label to the asset. The asset ID does not change when ownership of the asset is transferred. This is illustrated in Figure 21 by the fact that the component that the machine builder integrates into its machine has the same label as the component supplied by the component supplier, and the machine supplied by the machine builder has the same label as the machine used by the factory operator.

With their component or machine, the component supplier or machine builder will deliver selected information about their component or machine, which the machine builder or factory operator can integrate into their own AASs. This is illustrated in Figure 21 by the fact that there can be multiple AASs for an asset, which are governed by different AAS responsibles and are therefore colored differently. These AASs therefore have different AAS IDs. Information about a component or machine is delivered once. If information needs to be synchronized after delivery, the application is responsible for this. IEC 63278-4 describes various ways to accomplish this.

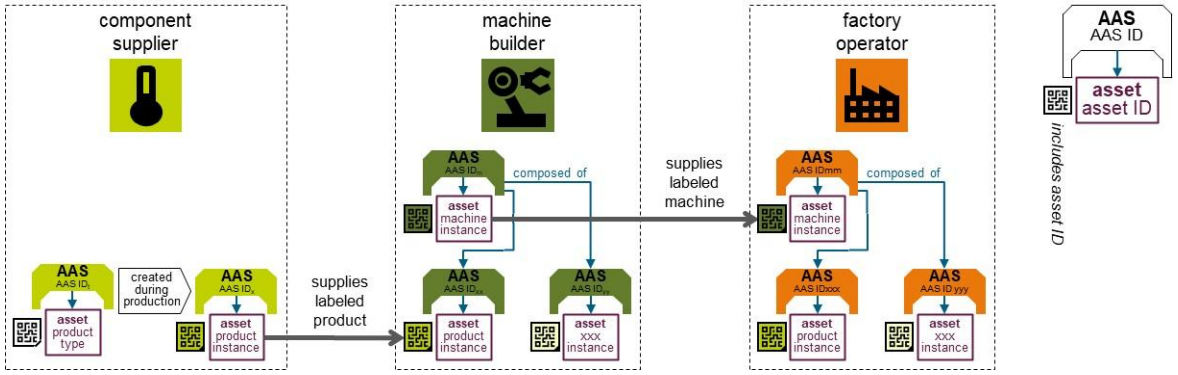


Figure 21: Illustration of asset IDs and AAS IDs

Note: Whether the machine supplier discloses the installed components to the factory operator depends on the business strategy of the machine supplier

11.4.2 Overall technical setup of MX-Port configuration “Leo”

Figure 22 provides an overview of the technical entities considered within the MX-Port configuration “Leo”. The technical entities are structured into the level’s business/legacy applications and shared services according to the “Foundational Framework for Manufacturing-X”.

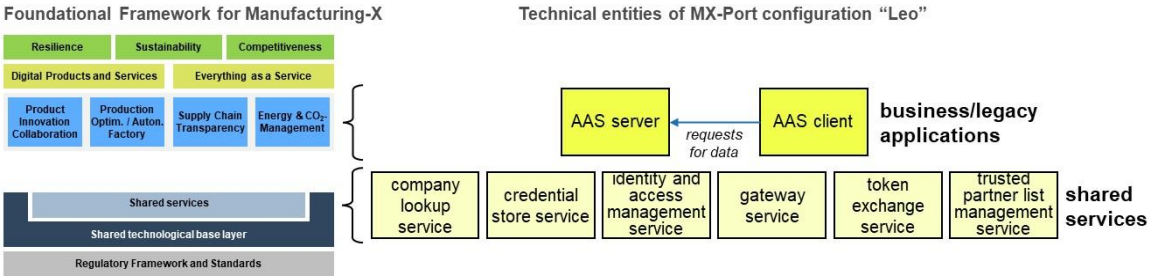


Figure 22: Overview of core technical entities of MX-Port configuration “Leo”

Figure 23 shows the overall technical setup for the MX-Port configuration “Leo”. On the left side the technical view according to [2] is shown. On the right-hand side the logical implementation of the MX-Port configuration “Leo” based on the concept of AAS is illustrated. It shows abstract software services and illustrates their association to the logical elements on the left-hand side.

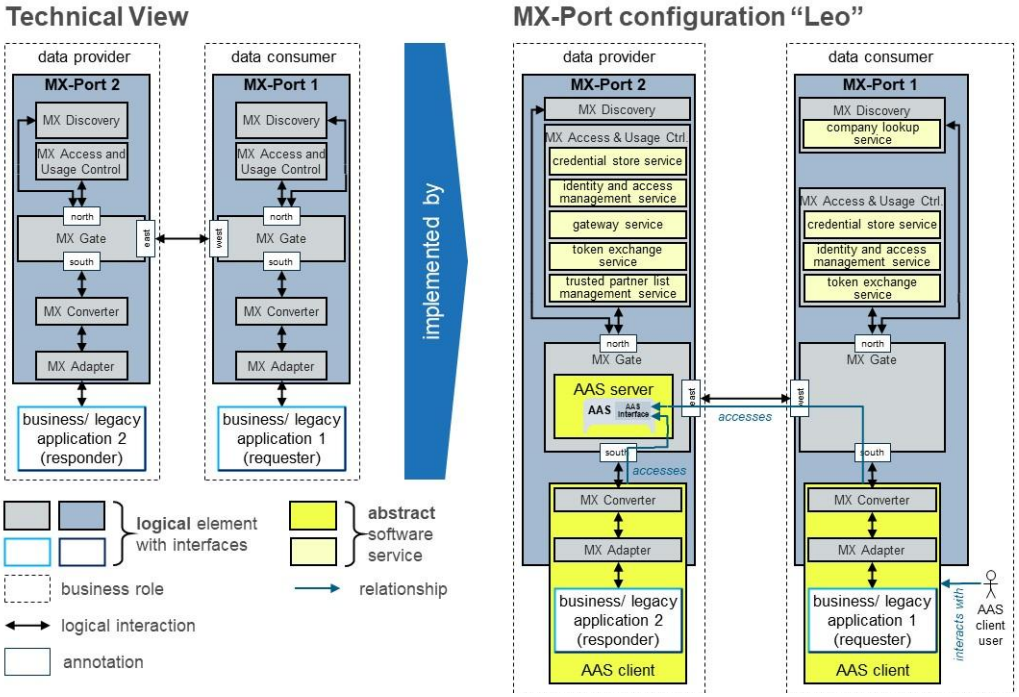


Figure 23: Overall technical setup of MX-Port configuration “Leo”

The logical implementation of MX Gate is detailed in chapter “MX Gate”; the logical implementation of MX Discovery is detailed in chapter “MX Discovery”; the logical implementation and operation of MX Access and Usage Control is detailed in chapter “MX Access and Usage Control”. Note that the MX-Port configuration “Leo” does not address the logical implementation of MX Converter and MX Adapter.

11.4.3 High-level cross-company workflow

For cross-company data exchange, the MX-Port configuration “Leo” is based on a high-level workflow that is divided into two basic steps.

Note that the MX-Port configuration “Leo” also supports access to public data without any access control. In this case **MX Access and Usage Control** is not required.

Initial setup: before a requester can access a responder, the following activities are necessary:

- There is a legal contract between the data provider and data consumer. This is an activity outside the scope of this document.
- The responder provides its company lookup information. This activity is logically associated with **MX Discovery** and is further detailed in chapter “MX Discovery”.
- The responder assigns access and usage rights for its data. This optional activity is logically associated with **MX Access and Usage Control** and is further detailed in "Authorization".
- The requester manages credentials, that the responder can technically verify. There are various ways in which these credentials can be issued. This optional activity is logically associated with **MX Access and Usage Control** and is further detailed in “Management of credentials”.
- The requester manages the public key of the responder so that the responder can sign the provided data, and the requester can validate the signature. This optional activity is logically associated with **MX Access and Usage Control** and is further detailed in "Data accountability".
- Data request: concrete access to asset data provided by a responder from a requester follows the following steps:
- The requester uses a company lookup service to find the information on where to find the software services of the responder and excludes spoofing. This activity is logically associated with **MX Discovery** and is further detailed in chapter 4.
- The requester provides a token to the responder, which the responder can verify. There are various ways how the requester receives the token. The requester uses the token for requesting access to the required data. There are various ways of verification by the responder. This optional activity is logically associated with **MX Access and Usage Control** and is further detailed in "Authentication".
- The responder checks whether the requester has access rights. This optional activity is logically associated with **MX Access and Usage Control** and is further detailed in "Authorization".
- The responder signs the data to be provided. This optional activity is logically associated to **MX Access and Usage Control** and is further detailed in "Data accountability".
- The responder provides the data to the requester, which is addressed by **MX Gate**. Additionally, this activity is logically associated with **MX Access and Usage Control** and is further detailed in "Authorization". Optionally, the responder can also link usage rights to the provided data, see "Usage control".

11.4.4 Requesting information from an AAS server

If an AAS client has access to an AAS server and requests specific information hosted by the AAS server, the MX-Port configuration “Leo” supports the following possibilities:

- The AAS client knows the asset ID and requests an AAS or Submodel/ SubmodelElements of an AAS.

- The AAS client specifies criteria, and requests all AASs or Submodel/ SubmodelElements of AASs meeting these criteria.

Requesting information from an AAS server based on asset IDs or AAS IDs is addressed by [7] and IEC 63278-5. Requesting information from an AAS server based on specified criteria expressed in a dedicated query language is currently in discussion at IDTA, see [9].

Application example

- The data consumer recognizes the discovery interface of an AAS server of a data provider based on a previously defined configuration and requests the required data from the data provider. This can be, for example, engineering tools that exchange engineering data.

11.4.5 Cross-company data exchange

Figure 23 describes a cross-company data exchange between business/legacy applications. The AAS client accesses the AASs of the AAS server via the AAS interface, which is passed through the two MX Gates. Note that these two MX Gates are logical objects only. The access shown in Figure 23 is from the AAS client directly to the AAS interface of the corresponding AAS.

11.4.6 Company internal data exchange

Figure 24 describes based on Figure 23 a company internal data exchange between business/legacy applications, typically provided by different software suppliers. The AAS client accesses the AASs of the AAS server via the AAS interface, which is passed through the MX Gate[13].

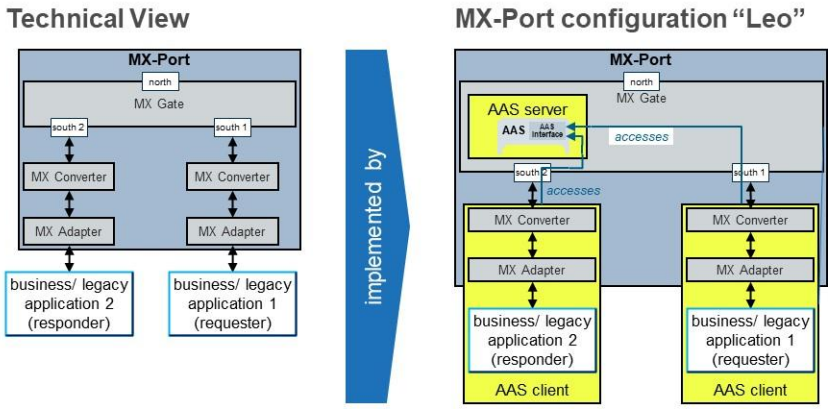


Figure 24: Company internal data exchange between business applications[14]

[13] Two MX-Ports can also be used for company internal data exchange, like shown in Figure 23. For cross-company data exchange, two MX-Ports are used for governance reasons.

[14] For a company internal data exchange a discovery concept for business applications and sometimes also access and usage control concepts are needed, but “lightweight” concepts for the MX Discovery and MX Access & Usage Control layers are often sufficient.

11.4.7 OPC-UA as integrated technology

In the case that the business/legacy application 1 in Figure 24 is an OPC-UA client and the business/legacy application 2 in Figure 24 is an OPC-UA server, Figure 24 illustrates a special case of company internal data exchange, where OPC-UA is used as an integrated technology.

11.5 MX Discovery

11.5.1 General

MX Discovery has the following tasks in the context of the MX-Port configuration “Leo”:

- An AAS client requests information on where to find the AAS server of a known data provider.
- An AAS client requests information about all companies that provide a specific capability. Examples of capabilities include providing a production technology or offering a product with certain properties.

These tasks are not within the current scope of AAS and must therefore be further developed and implemented prototypically within Factory-X.[15]

11.5.2 Company lookup information

Every company acting as a data provider must define its specific company lookup information:

- A company shall specify its company information, based on which a company lookup service provides the company lookup information.
- A company can specify which capabilities it offers to other companies. How these capabilities should be specified must be further elaborated.
- A company shall specify how another company can access the company's software services.

The conventions the company information shall follow, how capabilities shall be specified and how access can be specified must be further elaborated[16].

11.5.3 Request for finding the AAS server of a known data provider

For this task there are company lookup operators each operating a company lookup service providing the necessary company lookup information when a data provider is specified by its company information. A data consumer may operate its own company lookup service.

[15] Note that discovery of AASs and their Submodels/SubmodelElements is part of MX Gate, and not MX Discovery.

[16] There is need for a standard specifying the company lookup information for the MX-Port configuration “Leo”. An example on implementation level is ID-Link (IEC 61406), nevertheless, this document describes the concept only.

The data provider shall make the discovery information of the AAS server operated on its behalf available to all company lookup operators that are of its interest.

Figure 25 illustrates the conceptual approach of requesting for information on where to find the AAS server of a known data provider in the context of the MX-Port configuration “Leo”. In this case, the company lookup information managed by the company lookup service does not need to specify any capabilities that the company offers to other companies.

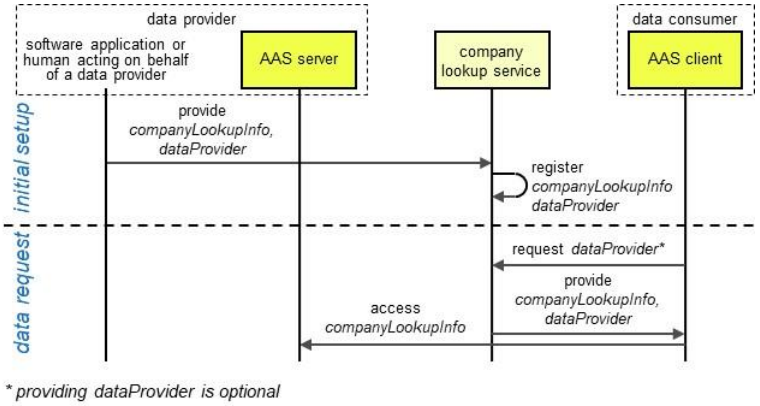


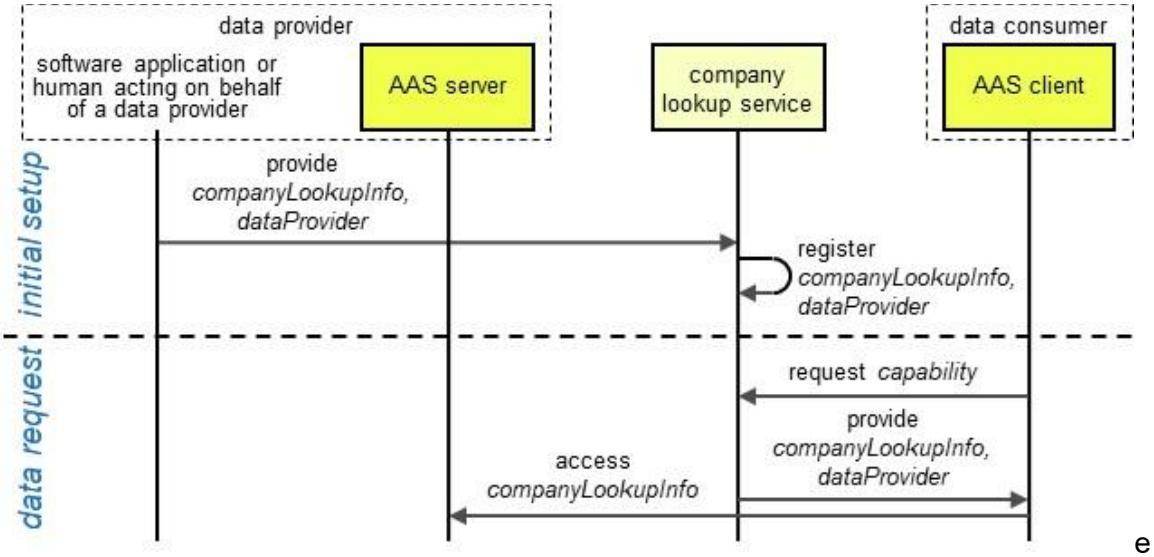
Figure 25: Illustration of requesting information on where to find the AAS server of a known data provider

Application example

- The data provider delivers a product and equips it with machine-readable company lookup information, for example, a QR code according to IEC 61406, i.e. www.dummy.com/discovery?asset_id=12345, for the AAS server operated on its behalf. In this case, the company lookup service is a software service that makes the delivered machine-readable company lookup information available, for example, initiated by a human scanning the QR code. The provision of the company lookup information is part of the delivery of the product. In this case, no data provider is provided for the “requests” of the AAS client shown in Figure 25.

11.5.4 Request for finding companies providing a specific capability

The internal setup is analogous to the request for information on where to find the AAS server of a known data provider, however, the capabilities provided must now also be specified in the company lookup information of the individual companies. In a data request, it is not the data provider that is specified, but the capability that the data provider provides, so that the company lookup service can provide all AAS servers of companies providing the requested-capability.



e

Figure 26.

Figure 26: Illustration of requesting for all companies providing a specific capability

Application example

- “Broadcast search” according to Requirement #14 can be implemented based on this approach. All AAS servers meeting the specific criteria register themselves at the company lookup service.

11.6 MX Access and Usage Control

11.6.1 General

This document focuses on “service to service” communication between data provider and data consumer. “Service on behalf of a human to service” communication is only illustrated by an example, “human to service” communication is not addressed in this document.

In addition to the case where there is no MX Access and Usage Control in the case of publicly available information, the MX-Port configuration “Leo” considers two different expansions stages:

- In the first expansion stage, the data consumer receives the credentials directly from the data provider. This expansion stage addresses step 1 according to Figure 19. In this expansion stage, neither a gateway service nor a token exchange service is required. The advantage of this expansion stage is that no changes are necessary on the data provider side, thus enabling a quick and easy introduction to cross-company data sharing. However, as the number of relationships between data providers and data consumers who want to share data increases, the effort required for onboarding new partners and for managing the credentials provided by the data provider becomes increasingly significant.
- In the second expansion stage, the data provider uses a list of trusted partners. This expansion stage addresses step 3 according to Figure 19. The data consumer must be added to the trusted partner list and provide suitable credentials to this list. Both the

data provider and the data consumer can use their own credentials. The advantage of this expansion stage is that the trusted partner list conceptually separates the onboarding of new partners from the operational exchange of tokens. This allows onboarding to be managed centrally by a 3rd party trusted partner list operator without requiring any changes to credential management by data consumer and data provider.

The list of trusted partner can be implemented in various forms and there are various options which of the required shared services according to Figure 22 are operated by the data provider and data consumer and which shared services are operated by a 3rd party shared service operator. It still needs to be analyzed in more detail which of these options will be implemented prototypically in the Factory-X project. In this respect, the descriptions of the second expansion stage in "Management of credentials" and “Authentication” are merely to be seen as examples, where the data provider uses a gateway service and a token exchange service to verify the credentials provided by the data consumer.

11.6.2 Management of credentials

The purpose of credential management is to enable the data consumer to provide credentials for authentication to the data provider, see 5.3, which the data provider can verify.

Figure 27 illustrates credential management in the first expansion stage.

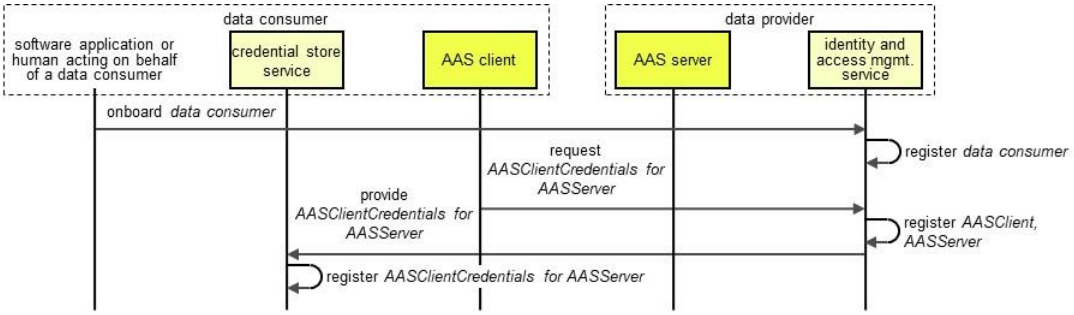


Figure 27: Management of credentials in the first expansion stage

Figure 28 illustrates as an example credential management in the second expansion stage.

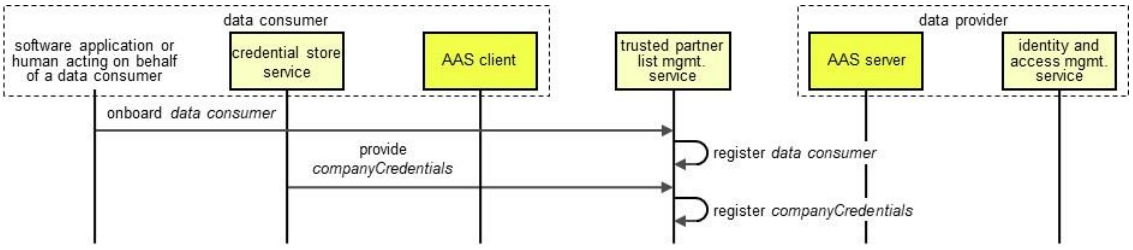


Figure 28: Management of credentials in the second expansion stage (example)

Authentication

The purpose of the authentication is to enable the data consumer to receive a token that the data provider can verify.

Figure 29 illustrates authentication in the first expansion stage.

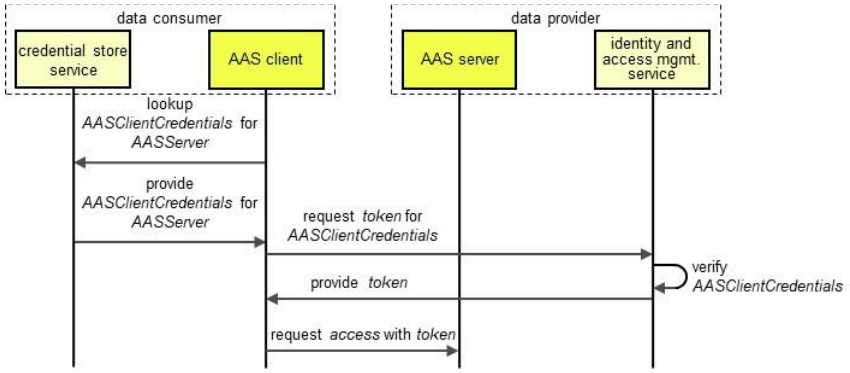


Figure 29: Authentication in the first expansion stage (example)

Figure 30 illustrates as an example authentication for a “service to service” communication in the second expansion stage.

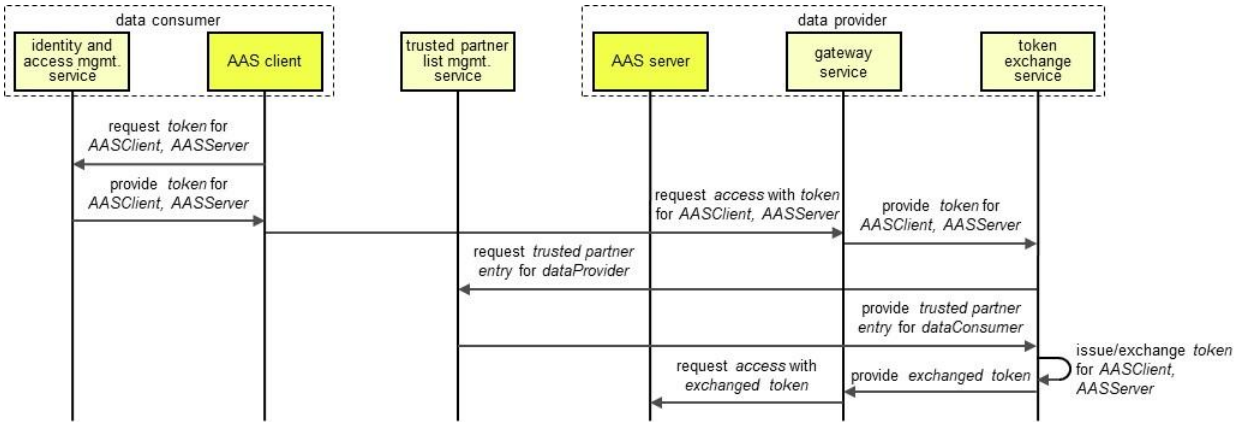


Figure 30: Authentication for “service to service” in the second expansion stage

Figure 31 illustrates as an example authentication for a “service on behalf of a human to service” communication in the second expansion stage.

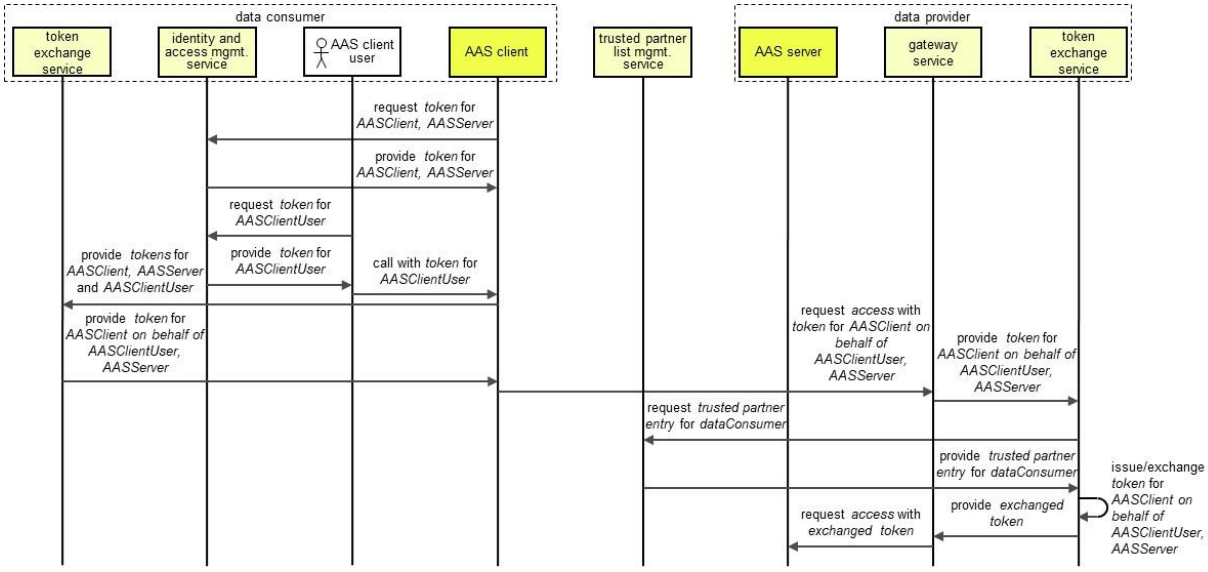


Figure 31: Authentication for “service on behalf of a human to service” in the second expansion stage (example)

Authorization

Authorization requires an initial setup in which a data provider stores the access policies for the data provided by an AAS server. Access policies are specified according to IEC 63278-3 and [8].

For a specific data request, the data consumer provides a token, in which a set of assertions is stored. The identity and access management service of the data provider verifies the token. If the verification is successful, the AAS server then checks whether access to the data should be granted based on the assertions stored in the token. If access should be granted, the data is transmitted to the data consumer.

Figure 32 illustrates the authorization.

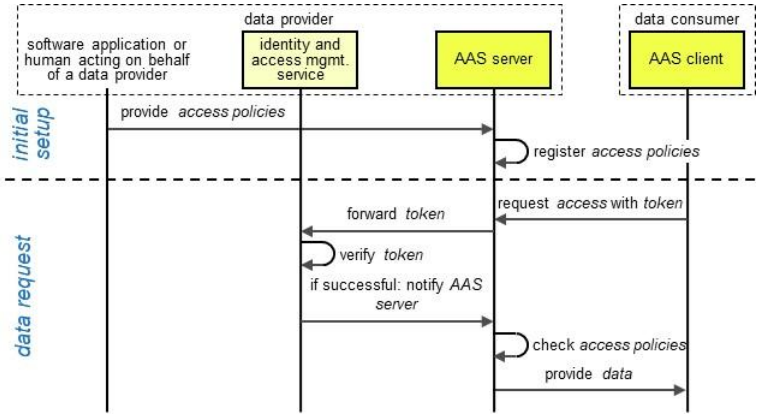


Figure 32: Authorization

Usage Control

The MX-Port configuration “Leo” supports the description of usage policies and the association of usage policies when providing data. For this purpose, in an initial setup the data provider stores the usage policies for the data provided by an AAS server. Usage policies are specified according to IEC 63278-3 and [8]. It is still in discussion whether the provision of usage policies will be implemented prototypically in the Factory-X project.

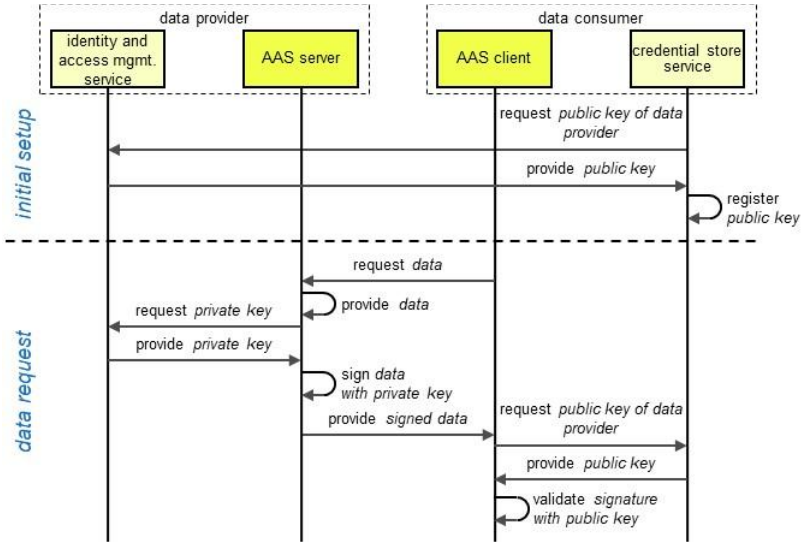
Conceptually the MX-Port configuration “Leo” offers monitoring and reporting of provided data. As a result, a data consumer runs a high risk of being sued if it does not adhere to the usage rights formulated in the contract.

The MX-Port configuration “Leo” does not support usage control in the sense that after data has been made available, it can be technically enforced that the data is only used under compliance with certain terms of use. Examples of such terms of use are prohibiting the copying of provided data or the transfer of provided data to other legal entities.

Data accountability

The MX-Port configuration “Leo” assumes that data provider and data consumer operate a public key infrastructure, meaning that data provider and data consumer each manage a public and a private key in their identity and access management service. On this basis, a data provider can sign provided data so that the data consumer can be sure that the data has not been tampered with.

Figure 16 illustrates the signing of data; it should be noted that the workflow depicted in Figure 15 is intertwined with the workflow shown in Figure 16.



11.6.3 References for MX-Port configuration “Leo”

[1] Factory-X: MX-Port Concept, https://factory-x.org/wp-content/uploads/MX-Port-Concept-V1.00-1.pdf

[2] Factory-X: Factory-X Use Cases: Application Guide, https://factory-x.org/wp-content/uploads/Factory-X-Application-Guide.pdf

[3] Factory-X: FX Integration Architecture V1.1, FX Integration Architecture V1.1.pdf (Factory-X internal)

[4] IEC 63278-1: ASSET ADMINISTRATION SHELL FOR INDUSTRIAL APPLICATIONS – Part 1: Asset Administration Shell structure

[5] IEC 61406: Identification Link – Unambiguous biunique Machine-Readable Identification

[6] Plattform Industrie 4.0: The Dataspace for Everybody, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/aas-dataspace4everybody.pdf?__blob=publicationFile&v=6

[7] IDTA: Specification of the Asset Administration Shell Part 2: Application Programming – IDTA Number: 01002 https://industrialdigitaltwin.org/wp-content/uploads/2023/06/IDTA-01002-3-0_SpecificationAssetAdministrationShell_Part2_API_.pdf

[8] IDTA: Specification of the Asset Administration Shell Part 4: Security – IDTA Number: 01004 https://industrialdigitaltwin.org/wp-content/uploads/2025/06/IDTA_01004-25-01_AAS-Specification_Part4_Security.pdf

[9] IDTA Query language: https://industrialdigitaltwin.io/aas-specifications/IDTA-01002/v3.1/query-language.html

12 MX-Port Configuration 3 based on requirements from Factory-X: “Orion”

Orion is built on the same Catena-X concepts as Hercules, with a dedicated focus on information exchange via OPC UA. It implements an MX port concept that combines OPC UA and OPC UA Companion Specifications with Dataspace Protocol (DSP) and Decentralized Claims Protocol (DCP) mechanisms, enabling interoperable and governed data exchange across organizational boundaries.

At its core, Orion enables the cross-company exchange of live shopfloor information. It is designed to leverage existing OPC UA-based data sources and make them accessible beyond company borders in a secure, authorized, and standardized manner. This includes the continuous provision of machine-level and asset-level data, support for external condition monitoring and analytics, as well as authorized bidirectional communication with industrial equipment, such as remote control or remote maintenance scenarios.

Orion is particularly suited for use cases where OPC UA information is already available or can be integrated with state-of-the-art technology. By relying on OPC UA as a shared protocol and semantic foundation, Orion avoids additional effort caused by technology mismatches or proprietary data conversions. Instead, information models are defined using OPC UA Companion Specifications, which are freely accessible, widely adopted, and developed in close collaboration with experts from machine and plant manufacturing domains. This ensures semantic consistency, long-term maintainability, and alignment with industry best practices.

From an architectural perspective, Orion represents a B2B-oriented exchange model between systems that are interoperable by design. Access and usage control are realized through a layered approach that combines DSP/DCP-based governance—covering policy management, trust establishment, and credential exchange—with the native security capabilities of OPC UA. While DSP and DCP provide legally governed and policy-driven authorization across organizational boundaries, OPC UA enforces transport-level encryption, authentication, authorization, and runtime usage control directly at the asset level.

Together, these mechanisms enable a secure, semantically rich, and scalable approach to cross-company industrial data exchange, positioning Orion as a robust foundation for interoperable B2B scenarios in Catena-X–aligned ecosystems.

	Layer	MX-Port “Orion”
L5	Discovery	Data Space Protocol
L4	Access & Usage Control	Decentralized Claims Protocol => OPC UA Security
L3	Gate	OPC UA Binary / OPC UA MQTT (JSON)
L2	Converter	OPC UA Information Model (with Companion Specification)
L1	Adapter	Application specific

12.1 MX Converter and MX Adapter

The MX Converter and MX Adapter are explicitly out of scope for the Orion core specification. Orion deliberately assumes that participating systems exchange information based on a shared semantic and protocol-level understanding, rather than relying on centralized or intermediary data transformation components.

At the core of this approach is OPC UA (Open Platform Communications Unified Architecture). OPC UA is a platform-independent, service-oriented industrial communication standard that combines secure communication, rich information modeling, and semantic interoperability within a single, unified framework.

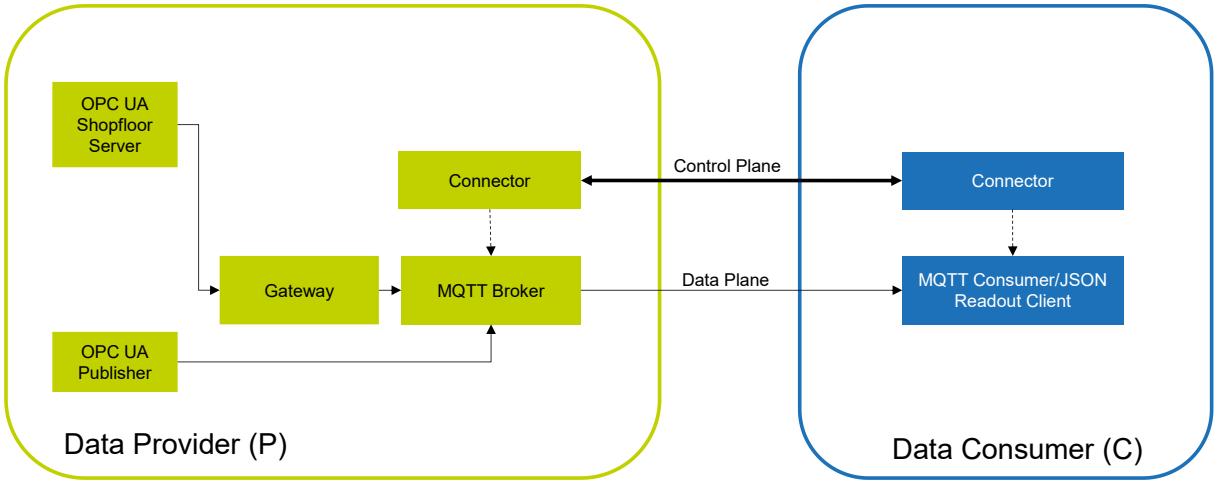
To establish this semantic alignment, Orion relies on OPC UA Companion Specifications. Companion Specifications are standardized, domain-specific information models defined on top of the OPC UA core specification. They describe data structures, relationships, and semantics for specific industries or use cases (e.g. machines, assets, production orders, or quality data). By using Companion Specifications, both parties in a B2B exchange agree on a common, machine-interpretable data model, thereby eliminating the need for proprietary mappings or format conversions.

As a result, MX Converters and MX Adapters are considered vendor-specific and non-essential in the Orion context. In many applications, an OPC UA server is already available—at least in a local setup with reduced security requirements—and can be leveraged directly as the initial integration baseline. From an Orion perspective, it can therefore be assumed that an OPC UA server is available as a primary data source or can be retrofitted in accordance with state-of-the-art implementations and best practices.

From an architectural standpoint, Orion enforces a clear separation between transport and governance concerns and payload semantics. The Orion layers L3–L5 operate independently of the concrete payloads exchanged at the Gate level. Policy enforcement, credential exchange, trust establishment, and access control are thus handled orthogonally to the data models themselves. This approach allows Orion to remain payload-agnostic, while still enabling a fully interoperable, secure, and semantically rich B2B data exchange.

12.2 OPC UA Pub/Sub

In the OPC UA Pub/Sub scenario, data distribution is realized in an event-driven and message-oriented manner. The payload structure is fully defined by the Data Provider and must comply with the requirements of OPC UA Specification Part 14 (OPC 10000-14). This includes, in particular, the definition of DataSets, FieldMappings, and the chosen serialization format. Currently, JSON encoding is the only encoding defined within Orion for OPC UA Pub/Sub. The Orion architecture is designed to be extensible, allowing additional encodings to be specified in the future as requirements evolve.



The payload is based on a clearly defined OPC UA information model, ideally derived from an OPC UA Companion Specification. Semantic meaning of the data is fully contained within the OPC UA model, while the transport layer remains decoupled from the payload semantics.

The security requirements defined in Layer L4 for OPC UA must be implemented directly within the MQTT broker. The MQTT broker is responsible for the authentication and authorization of both publishers and subscribers. A token-based authentication mechanism (e.g. OAuth 2.0 / JWT) is recommended in order to:

- enable seamless integration with existing IAM and Dataspace mechanisms,
- support short-lived credentials and policy-based access control.

In addition, topic-based access control mechanisms must be applied to enforce usage control at the message level.

Recommendation OPC UA Pub/Sub with a OPC UA Server

If only a classic OPC UA Client/Server implementation is available on the data source side, a converter from OPC UA Client/Server to OPC UA Pub/Sub is required.

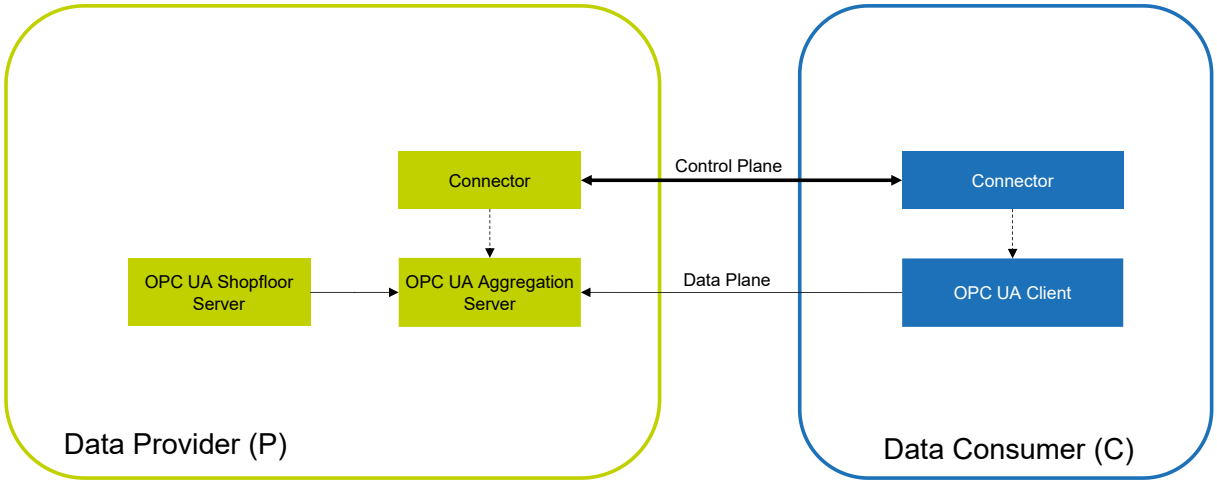
This role can be fulfilled by an OPC UA Pub/Sub gateway, such as an umati gateway or comparable components.

The converter:

- reads data via the OPC UA Client/Server interface,
- maps the data to the defined DataSets,
- publishes the data via MQTT in accordance with OPC UA Pub/Sub.

12.2.1 OPC UA Client/Server (Binary)

In the OPC UA Binary (Client/Server) scenario, the OPC UA server acts as the central data source and provides a standardized OPC UA interface with the required services, such as Read, Write, Browse, Subscribe, and Method Calls. The OPC UA server implements a consistent information model, preferably based on one or more OPC UA Companion Specifications. All relevant business objects, states, and relationships are represented within the server’s information model and made accessible to clients. The security requirements defined in Layer L4 for OPC UA must be implemented directly within the OPC UA server.



This includes, in particular:

- certificate-based authentication (X.509),
- encrypted communication using Secure Channels and Security Policies,
- role-based access control (RBAC).

In future also the token-based authentication can be part of Orion. Currently this authentication approach is not common.

Role management defines which clients are allowed to access specific nodes and which OPC UA services (Read, Write, Subscribe, Method Calls) are permitted.

Recommendation for Productive Environments:

For production deployments, it is strongly recommended to introduce an aggregation or chain server between the shop-floor OPC UA Server and the connector. This intermediate component provides a hardened security boundary, reduces the attack surface within the OT environment, and enables a controlled separation between operational infrastructure and the dataspace integration layer.

Both variants—OPC UA Pub/Sub and OPC UA Client/Server (Binary)—are fully supported and equally valid integration options within the Orion context. The key difference lies in the responsibility for security and access control:

- In the Pub/Sub model, a significant portion of the security logic is delegated to the MQTT broker.
- In the Client/Server model, security and access control are fully handled by the OPC UA server itself.

In both cases, Orion remains payload-agnostic at the higher layers (L3–L5), while semantic interoperability and security are consistently implemented using established OPC UA mechanisms.

12.2.2 MX Access and Usage Control

Access and usage control in the Orion configuration builds on the coordinated use of the Dataspace Protocol (DSP), the Decentralized Claims Protocol (DCP), and OPC UA. DCP provides the foundation for decentralized identity and claims management and enables self-sovereign identity concepts through wallet-based credentials. DSP processes these claims

within machine-readable contracts, forming the basis for authorized data access across organizational boundaries.

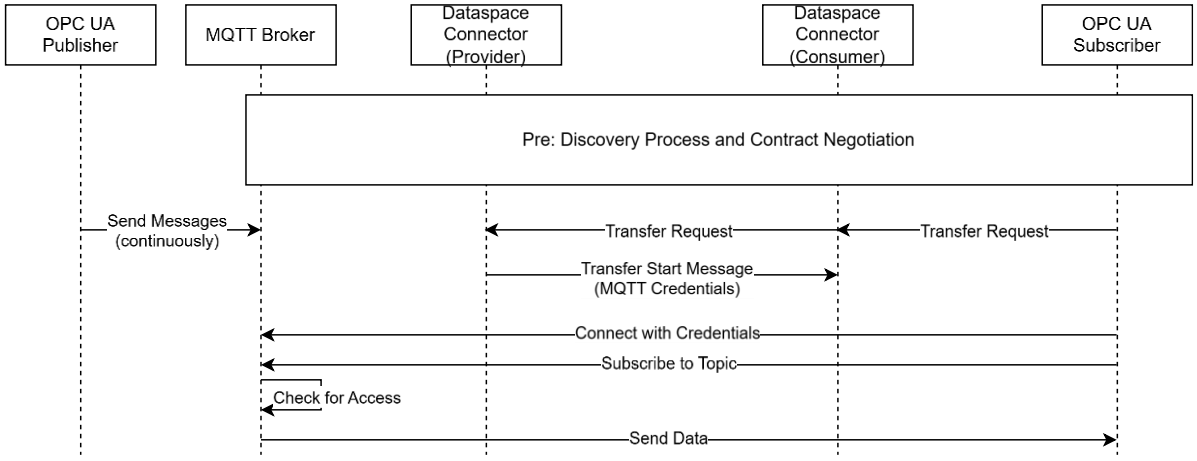
OPC UA itself provides a robust security framework for encrypted data transport, authentication, and authorization. In Orion, these native OPC UA security capabilities are combined with DSP/DCP-based identity and contract management. DSP/DCP ensure trusted identification and legally governed authorization, while OPC UA enforces encryption and runtime authorization at the asset level.

Consequently, the final authorization decision is not executed within the connector but directly in the respective OPC UA system. Data access control is enforced either by the OPC UA Server (for Client/Server communication) or— in Pub/Sub scenarios—by the MQTT broker. The EDC only transmits the information required to enable access, not the actual process data. Data exchange therefore occurs directly between the consuming system and the OPC UA endpoint, while the connector merely provides the required access parameters in the TransferRequestMessage.

As the technical foundation of the reference implementation, the Tractus-X EDC provides the runtime capabilities for Access & Usage Control. This includes the management of permissions and roles, automated contract negotiation, token processing, and the handling of legally validated ODRL-based policies as defined in the Catena-X governance framework.

12.2.3 OPC UA Pub/Sub

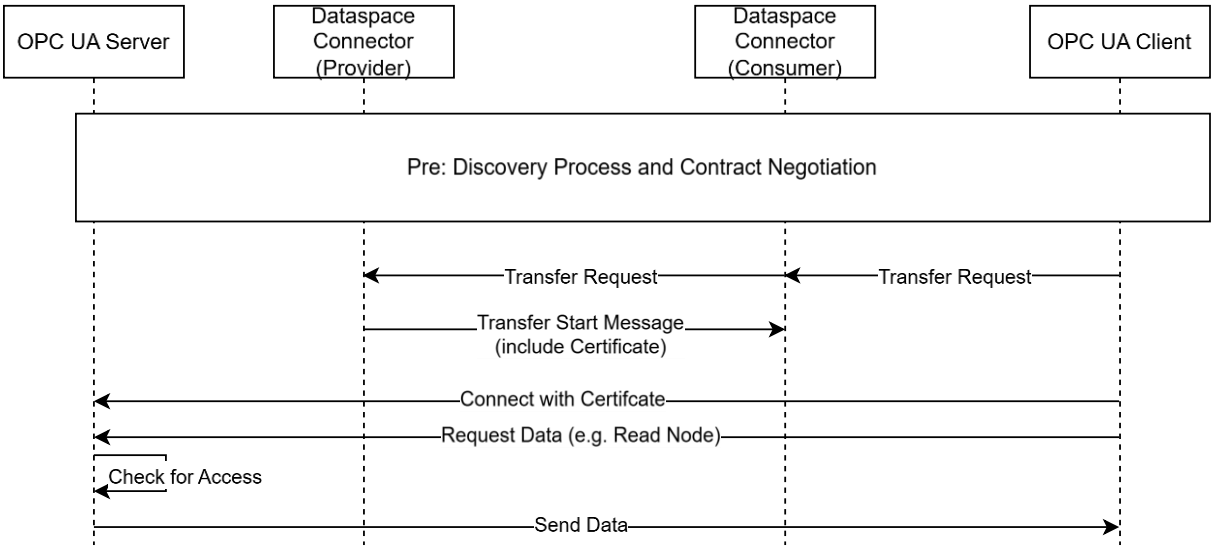
For Pub/Sub-based data exchange, the endpoint properties defined via the Dataspace Protocol must allow the data provider to establish a connection to a consumer-side MQTT broker (username/password or token-based) and continuously transmit publish messages. From a security and governance perspective, it is recommended to rely on short-lived tokens and refresh them regularly via the connector to avoid long-term credential exposure.



12.2.4 OPC UA Binary

OPC UA Binary natively offers comprehensive security and authorization mechanisms, including role-based access control and authentication via passwords, X.509 certificates, or tokens.
In the Orion configuration, password-based authentication should be avoided wherever possible. Instead, certificates or tokens are transmitted from the provider connector to the consumer via the Transfer Start Message. In parallel, the provider connector updates the

corresponding roles and permissions in the OPC UA Server so that the consumer can authenticate directly with the server using the supplied credentials. This ensures that access is strictly limited to the permissions associated with the assigned role.



12.2.5 MX Discovery

The Discovery layer in the Orion configuration is built on the Dataspace Protocol (DSP) / Decentralized Claims Protocol (DCP) like the “Hercules” Configuration. Together, these protocols establish a decentralized mechanism for identifying business partners, retrieving service catalogs, and resolving the technical endpoints required for cross-company data exchange.

The reference implementation for this Discovery layer is the in Factory-X extended Tractus-X EDC, which offers a fully DSP-compliant connector framework. It provides standardized logic for catalog retrieval, contract negotiation, and the issuance and handling of Endpoint Data References (EDRs), enabling consuming applications to seamlessly resolve and access the correct data endpoints.

Within this process, business partners are discovered based on their published DSP artifacts, and access to their catalog APIs is authorized using the credentials and claims exchanged via DCP. This ensures a consistent enforcement of access and usage policies across organizational boundaries.

The catalog objects themselves include Distribution entries that indicate the available data transport mechanisms.

For Orion, this typically includes MQTT for OPC UA Pub/Sub via MQTT and OPC UA Binary for traditional Client/Server communication. Additionally, the asset metadata contains OPC UA–specific technical properties, such as supported server profiles. These metadata elements enable consuming systems to identify the appropriate endpoint and communication profile automatically, ensuring that data can be located and accessed reliably within the dataspace.

13 Comparison of MX-Port configurations with business requirements (qualities)

Source: FX-0089 Factory-X MX-Port-vs-Qualities.docx

Business Requirements (FX North Star Qualities) Quality Definition	MX-Port Hercules	MX-Port Leo	MX-Port Orion
Interoperability			
Business Application User View (As a digital ecosystem particpant, I want to)			
Collaborate with all other data ecosystem participants (also from other data spaces and business spaces).	Generally speaking, Hercules is compatible with all dataspaces building on DSP & DCP. Use-cases building on it must still make sure that the the Policy Constraints, Credential Schemas, Issuers, Business APIs (like AAS) and semantics (like submodel templates) align.	MX-Port Leo represents one MX-Port interface specification to enable cross-organizational data exchange within F-X dataspace. Within F-X I can interact with all participants using MX-Port Leo. I can interact with all participants using MX Hercules, then my application has to implement the MX Port Hercules as well. The use of AAS on the MX Converter and Gate level ensures	Orion is compatible with all dataspaces building on DSP & DCP. Use-cases building on it must still make sure that APIs (like OPC UA) and semantics (like Companion Specifications) align.

		semantic interoperability on the data level.	
I want to model data for exchange with all my business partners only once--independent of their industry or geographic location.	This is the use-cases' responsibility. Hercules is compatible with any HTTP API and thus, with all AAS-Profiles and Submodel Templates	The use of AAS on the MX Converter and MX Gate levels ensures data-level interoperability. The use cases are aligned in their AAS submodels and application, thereby enabling semantic interoperability	This is primarily the responsibility of the use-case. OPC UA and OPC UA Companion Specifications on the MX Converter and MX Gate levels ensure syntactic and semantic interoperability.
Use uniform processes with all other data ecosystem participants for comparable tasks.	Yea, that's kind of the point of protocol-based interaction. The great thing about Hercules is that the spec and implementation for the upper layers is pretty complete.	Processes are defined and agreed upon by the use cases. Use case members agree upon data models and workflows. MX-Port Leo serves as common interface to enable the respective implementation of these processes.	The processes are defined in DSP, DCP and OPC UA/OPC UA Companion Specifications.
Be not locked in by a specific business application provider.	That, also, is an inherent quality of protocol-based cybernetics. Consequently, Hercules delivers this.	The application of AAS and AAS security ensures that components of different vendors (open source as well as commercial components) can be used	Orion does not use proprietary standards or technologies.

		and are interoperable.	
Be not locked in by a specific operating company.	The only technical process that requires a third party like an operating company is identity issuance and establishment of trust relationships. There is no technical necessity to only have one. Everything else is a question of governance.	An operating company can be used to manage trust relationships within the dataspace. MX-Port Leo per se does not restrict to one specific operating company (i.e., multiple operating companies can be used). In addition, MX-Port Leo also supports bi-lateral trust establishment between partners. Hence, there is per-se no dependency on one specific operating company	The only technical process that requires a third party like an operating company is identity issuance and establishment of trust relationships. There is no technical necessity to have one. Everything else is a question of governance.
Business Application Provider View (As a provider of applications to the digital ecosystem, I want to)			
Set and use the standards that are relevant for me (as defined within the FX-Project).	Standard-setting is an activity that is out of scope for a technical implementation.	We do not define standards in the project and only make use of open standards like for intercompany data exchange AAS IEC 63278 and ID Link IEC 61406.	We do not define standards in the project and only make use of open standards like IEC 62541 and DSP/DCP.

Be able to choose the level of interoperability that is right for me.	Hercules defines ADRs on several levels. When choosing to implement only the Gate, there's no interoperability guarantee end-to-end. In general (and this is true for all configurations): These "levels" are mutually incompatible - if one party is "level1" and the other one "level2", the latter won't be able to access the former. And suddenly, you're not only expecting everyone to support one stack but three.	MX-Port Leo supports multiple configurations for establishing trust between partners or participants. In the first configuration, trust is established bilaterally between Consumers and Providers. Additionally, trusted third parties can serve as trust anchors, enabling decentralized identity management by allowing each partner to retain control over their own identity. Semantic interoperability is achieved by adhering to the IEC 63278 AAS.	Orion supports multiple communication patterns like OPC UA binary, MQTT and HTTP as well as Publish/Subscribe and Polling. Semantic interoperability is achieved by adhering to IEC 62541 (OPC UA) and Companion Specifications.
Business Application User View (As a digital ecosystem particpant, I want to)			
Continue to use existing infrastructures and established procedures, to the extent possible.	Implementations of Hercules (like factoryx-edc) support the integration of company-internal technologies such as AAS over oauth2. There is no need to overhaul existing IT-systems	One goal of MX-Port Leo is the integration into the existing IT infrastructure of each partner, by using the partners identities and applying widely	OPC UA is an internationally established standard with a large number of vendors and implementations for all kinds of systems and customers.

	- they will usually have to be integrated though.	accepted and used standards and protocols.	
Find and interact with existing and new business partners.	Existing business partners are identified via dids. A did is enough to discover all relevant endpoints that a client may need to exchange data.	Finding business partners and their offerings in the ecosystems is supported via the MX Discovery layer of MX-Port Leo. All business partner can register themselves, have full control on what they share.	Existing business partners are identified via DIDs. A DID is enough to discover all relevant endpoints that a client may need to exchange data.
Secure my investment in the installed base.	It depends on what a participant is invested in. If this alludes to OPC UA and AAS, upgrading those interfaces to be Dataspace-ready is easy.	The MX Adapter allows connecting legacy applications to the dataspace.	Legacy applications can be connected to the dataspace using the MX Adapter. For OPC UA with Companion Specification, no specific adaptation is required.
Business Application Provider View (As a provider of applications to the digital ecosystem, I want to)			
Integrate into my installed base.	It depends on what a participant has in their installed base. If this alludes to OPC UA and AAS, upgrading those interfaces to be Dataspace-ready is easy.	The MX Adapter allows connecting legacy applications to the dataspace.	Legacy applications can be connected to the dataspace using the MX Adapter. For OPC UA with Companion Specification, no specific adaptation is required.

Start with a low-level starter package and optional additional packages that can provide more complex functions.	There's a set of open-source components that are free and ready to use. If a participant requires more convenience or has specific requests, there's already today an ecosystem of commercial vendors.	MX-Port Leo defines three steps with a low entry level (i.e., "low-level starter package") for Step 1. Step 2 and Step 3 add further functionality for discovery of business partners as well as more sophisticated access and usage control for higher scalability.	There's a set of open-source components that are free and ready to use. If a participant requires more convenience or has specific requests, there already is an ecosystem of commercial vendors available today. Usage of MX-Port Orion builds on company internal use of OPC UA and Companion Specifications as a prerequisite. Additional functionality can be built on top of that seamlessly.
Trust & Security			
Business Application User View (As a digital ecosystem participant, I want to)			
Be certain that my business partners are actually the ones they pretend to be.	Taken care of by ADR-002 and -003 that correspond largely to CX-0018 and CX-0149.	Yes, all participants identify themselves with their identity, the identities can be verified.	Handled according to ADR-002 (Cross-Company Authorization and Discovery) and ADR-003 (Authentication for Dataspace Participants) that correspond largely to CX-0018 and CX-0149.
Divide my business partners into different “trust classes” and then	Taken care of by ADR-003 in conjunction with the constraint-and-credential profile of	The Trusted List approach is intentionally designed to provide	Data access for different data consumers can be assigned by the data provider

treat them accordingly.	each Dataspace, implemented in factoryx-edc and dataspace-protocol-lib	flexibility for onboarding business partners with varying trust levels, if required. At present, however, all partners are managed with the same trust level.	down to the node-level or based on OPC UA-profiles.
Be sure that the data I get is unchanged or unadulterated.	The question is _how sure_ does a client want to be. If you trust TLS, then yes: all traffic is TLS encrypted according to the base protocols. Adding signatures to business-payloads can be implemented by use-cases.	Yes, all data transfer can be encrypted end to end by TLS and additionally the data integrity can be ensured by a signature.	Orion uses asynchronous Encryption (TLS / OPC UA Security) - as End to End Encryption and Message based Encryption.
Divide my data into different “confidentiality levels” and then treat them accordingly.	Taken care of by ADR-003 in conjunction with the constraint-and-credential profile, implemented in factoryx-edc and dataspace-protocol-lib	The MX-Port Leo access control is based on the attribute-based access control as defined by AAS Security.	This is a core EDC-Functionality implemented in Orion.
Be sure that my data is always safe from unauthorized access (according to its confidentiality level).	There is no such thing as _always safe_. Participants are free to use secure technologies in an unsecure manner.	The MX-Port Leo access control is based on the attribute-based access control as defined by AAS Security. Secure development and operation are in the responsibility of	Orion uses asynchronous Encryption (TLS / OPC UA Security) - as End to End Encyption and Message based Encyption. Secure development and operation are in the responsibility of the application provider.

		the application provider.	
Business Application Provider View (As a provider of applications to the digital ecosystem, I want to)			
Be able to continue to use existing business partner directories, including their identification and authentication mechanisms.	Existing identifiers like VAT-IDs, DUNS-numbers or Catena-X BPNs can be facilitated via Verifiable Credentials.	MX-Port Leo allows to integrate existing partners' identity and credential management systems to realize cross-organizational authentication and access control.	Integration of existing identifiers like VAT-IDs, DUNS-numbers or Catena-X BPNs can be facilitated via Verifiable Credentials.
Data Sovereignty			
Business Application User View (As a digital ecosystem participant, I want to)			
Determine myself with whom I share my data.	Yes, see ADR-002 and ADR-003 or CX-0018 and CX-0149, respectively.	Based on the verified identity of the requester, the data provider has full control on the access rights to his data.	Access is controlled by the data provider and handled according to ADR-002 (Cross-Company Authorization and Discovery) and ADR-003 (Authentication for Dataspace Participants) or CX-0018 and CX-0149, respectively.
Exchange my data only if there is comprehensible regulation of what is to be done with the data.	This can be facilitated by ADR-002. To satisfy this requirement fully though, business partners would have to agree how to digitally represent such regulation as odrl-	MX-Port Leo assumes that "terms of use" are accepted prior to any data exchange, the provider will only share data then.	This can be facilitated by ADR-002 (Cross-Company Authorization and Discovery). To satisfy this requirement fully though, business partners would

	constraints and add that to the constraint-and-credential profile of Factory-X.		have to agree how to digitally represent such regulation as ODRL-constraints and add that to the constraint-and-credential profile of Factory-X.
Control the actual use of my data.	Depends on what kind of use is meant. It's not in scope to magically make already-transferred data disappear. when it comes to stopping access to an API or signaling/executing the end of a sharing agreement, that's implemented and standardized.	The MX-Port configuration “Leo” does not support usage control in the sense that after data has been made available, it can be technically enforced that the data is only used under compliance with certain terms of use . Examples of such terms of use are prohibiting the copying of provided data or the transfer of provided data to other legal entities.	Orion controls granting, restricting or terminating continued data access but not the usage of data once it has been downloaded by the data consumer.
Be able to restrict the use of my data at any time.	Is possible, just like announcing this and allowing the client to fail gracefully.	The data provider can anytime revoke the access to its data. The MX-Port configuration “Leo” does not support usage control in the sense that after data has been made available.	Orion provides a mechanism for detailed, role-based restriction of data-access. After that, there is no automated usage control. See OPC UA - Core, Part 3, PermissionType.

Monetize the sharing of my data.	possible via ODRL constraints, would have to be specified more precisely	This is currently out of scope of MX-Port Leo. MX-Port Leo may in future provide functions to support monetarization, like providing an audit trail of user activities.	Possible via ODRL constraints, would have to be specified more precisely
Business Application Provider View (As a provider of applications to the digital ecosystem, I want to)			
Control the technology that is essential for my business - no lock-in by a 3rd party.	The only technical process that requires a third party like an operating company is identity issuance and establishment of trust relationships. There is no technical necessity to only have one. Everything else is a question of governance.	The use of AAS and the adherence to the AAS standard ensures, that components of different vendors (open source as well as commercial components) can be used and are interoperable and exchangable.	The only technical process that requires a third party like an operating company is identity issuance and establishment of trust relationships. There is no technical necessity to only have one. Everything else is a question of governance.

14 Comparing MX-Port with an alternative architecture for the DSP & DCP case. (Hercules & Orion)

The MX-Port, if built like a system, requires multiple configurations to be generated for every case at “deployment” time. Restricting the supported applications and semantics which are allowed, you cannot reuse layers, you always will need a totally new configuration. To As an alternative, in order to foster interoperability, by not using the MX-Port, but rather only requiring the usage of the MX-Connector allows and a MX-Wallet, it would allow on “runtime” the configuration of the system security (access & usage control), endpoints (gates) and leave use case specific which “data semantic” to use (converter) and how to compile it (adapter).

SoSo, by not using the MX-Port, with the MX-Connector you will have the possibility of having both “AAS” + “OPC-UA” + “Use Cases Specific Business Applications” running on parallel and identifiable if the access permission (policies) is matching to your identity or the use case agreement you signed. The only limitation would that Leo technologies would not be supported on its current state, since the Access methods would not be harmonized.

15 Glossary

Term	Definition	DSSC Definition	Standard Definition
AAS	Asset Administration Shell, a concept for representing assets in the digital world.		
Business value proposition		A description of the way an organization creates, delivers, and captures value. Such a description typically includes for whom value is created (customer) and what the value proposition is.Typically, a tool called business model canvas is used to describe or design a business model, but alternatives that are more suitable for specific situations, such as data spaces, are available.	
Connector		Technical component that is run by (or on behalf of) a participant and that provides participant agent services, with similar components run by (or on behalf of) other participants.	Device providing connection and disconnection to a suitable mating component. A connector has one or more contact elements
Cross Data Space data Exchange	The cross-dataspace data exchange requires a common approach to achieve		

	interoperability when it comes to a “cross company, cross dataspace” use cases like for example the Digital Product Passport. Therefore, there needs to be some common ground and “resolvable” artifacts in between the Manufacturing-X dataspaces.		
Data Consumer	An entity that retrieves and uses data from a data provider.		
Data Provider	An entity that offers and shares data to be consumed by data consumers.		
Data Space Governance	The governance framework defines the structure, processes, and rules that guide how participants interact, share, and manage data within a dataspace.	framework of policies, processes, and standards that ensure effective management, quality, security, and proper use of data within an organization.	
Data Space Intermediary		A service provider who provides an enabling service or services in a data space. In common usage interchangeable with ‘operator'.	
Data Space Support Center (DSSC)	Provides definitions and support for data space interoperability and data quality.		
Data Transfer	The process of sending data from one system to another.		

Dataspace Protocol (DSP)	The Dataspace Protocol is a specification designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. This specification defines the schemas and protocols required for entities to publish data, negotiate Agreements, and access data as part of a federation of technical systems termed a Dataspace.		https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1/
Decentralized Claims Protocol (DCP)	A protocol used for authorization and authentication in dataspaces. It consists of a set of protocols for asserting participant identities, issuing verifiable credentials, and presenting verifiable credentials using a decentralized architecture for verification and trust.		https://eclipse-dataspace-dcp.github.io/decentralized-claims-protocol/v1.0.1/
Derecho	References the legal framework ensuring compliance with data protection regulations.		
Description shelf system	To create concrete instances, we must assign valid solutions to the different layers of the MX-Port. This is done in a 2-step process: In Step 1, requirements for solutions are typically made by use case owners based on concrete business,		

	functional, commercial or other requirements. These solutions are most likely coming from a set of existing industry standards.		
Digital Product Passport	A digital record containing precise information related to a product's history and lifecycle		
Discoverability	The ability to find and access offered services and data.		
Discovery Service			Service to find unknown resources, entities or services based on a specification of the desired target
eIDAS	Electronic Identification, Authentication, and Trust Services in the EU.		
ID-Link	Discovery Level L5		Electropedia references ID-Link in IEC 61406-1:2022, which enables access to product data (e.g. via QR-code, NFC or RFID), effectively underpinning DPP functionality.
OPC-UA	Open Platform Communications Unified Architecture, a protocol for industrial automation.		Defined in IEC 62541 via Electropedia CDD as the industrial automation protocol standard. It's a cross-platform, extensible architecture providing secure data exchange, discovery services (Part 12), PubSub,

			historical access, and device interoperability.
Partner Discovery	The process of finding and verifying partners for data exchange.		
Pull/Push Transfer		1. A data transfer initiated by the consumer, where data is retrieved from the provider. 2. A data transfer initiated by the provider, where data is sent to the consumer.	
Resolvable Identities	Unique credentials that can be resolved and understood across different data spaces.		
Security	Measures to protect data and systems from unauthorized access or compromise.		
Trusted issuers	Entities recognized as credible for issuing verifiable credentials		
Cross-Interoperability	Interoperability is a strategic goal for Manufacturing-X and a core technical element of the MX-Port concept. In practical terms, interoperability would mean for “Small Motor Inc.” that they will have • To register, identify and authenticate themselves only once to be able to	The ability of participants to seamlessly access and/or exchange data across two or more data spaces. Cross-data spaces interoperability addresses the governance, business and technical frameworks to interconnect	Defined as the ability of two or more systems or applications to exchange information and to mutually use the information exchanged.

	collaborate with companies from different industries, • To model its data only once for a given use case, • To use only one technology stack (MX-port configuration, see below) to realize the “Shared-Service-Box” that allows the use of the required protocols, connectors etc., • The free choice in selecting a business application for a use case from several providers.	multiple data space instances seamlessly. Explanatory Text: Inter-data space interoperability is an alternative term, and both terms can be used interchangeably.	
Cross-dataspace		A specific setting in which participants of multiple data spaces create value (business, societal or environmental) from sharing data across these data spaces.	
Data sovereignity	Ensures clear guidelines on data ownership, compliance, and security	DSSC refers to “Data sovereignty & trust building blocks”, enabling participation in a data space while	

		preserving ownership and policy control.	
Data Space Infrastructure		A technical, legal, procedural and organisational set of components and services that together enable data transactions to be performed in the context of one or more data spaces.	Blueprint v2.0 outlines a multi-layered, modular reference architecture. It includes logical, functional, and technical layers with defined roles (data providers, consumers, intermediaries, etc.)
Decentralisation	Decentralization in data-sharing ecosystems distributes control over data storage, access, and distribution across multiple entities rather than a central authority, enhancing data ownership, privacy, and security. It reduces single points of failure, improves scalability, and increases system resilience. However, in regulated industries, centralized control is necessary for dataspace registration to meet strict security standards.	In the DSSC Blueprint (0.5 to v2.0), decentralisation is central to building a trusted architecture for data spaces. It underpins a shared and distributed governance model, avoiding centralized control over data, access, and usage policies	
Standardisation	The establishment of common protocols, formats, and guidelines for compatibility and interoperability.		
Eclipse Tractus-X KIT (Keep it Together)	KIT, short for Keep It Together, is an open-source toolbox with comprehensive documentation that enables multiple stakeholders (Business, Solution Providers, Developers) to build interoperable		https://eclipse-tractusx.github.io/documentation/kit-framework#what-is-a-kit

	applications compatible with the Eclipse Tractus-X dataspace technologies, and support the compliance with industrial standards from standarization organizations (Catena-X e.V., IDTA, ISO/DIN, EDWG, Manufacturing-X, etc.) and in some cases enable regulatory compliance.		
FOSS (Free and Open-Source Software)	Free and open-source software (FOSS) is software available under a license that gives users the right to use, share, modify, and distribute the software – modified or not – to everyone and provides the means to exercise those rights using the software's source code. FOSS is an inclusive umbrella term encompassing free software and open-source software.		
COTS (Commercial-off-the-shelf)	Commercial-off-the-shelf or commercially available off-the-shelf (COTS) products are packaged or canned (ready-made) hardware or software, which are adapted aftermarket to the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.		

15.1.1 Terms and Definitions from MX-Port configuration “Leo”

Basic terms and definitions

asset: physical or non-physical entity that has value to a human or an organization [IEC 63278]

AAS: standardized digital representation of an asset [IEC 63278]

AAS user application: abstract software application which accesses an AAS via its AAS interface for usage by humans or for automatic processing [IEC 63278]

AAS server: abstract software service managing a set of AASs and providing the AAS interface[17] [own definition]

AAS client: synonym for AAS user application

software application: software functional element specific to the solution of a problem [IEC 63278]

software service: software functional element that provides the functionality through interfaces [IEC 63278]

business role: set of characteristics of a legal entity to exhibit a set of required behaviors [[2], based on IEC 63283-1]

human/organizational role: set of characteristics of a human/organization to exhibit a set of required behaviors [based on IEC 63283-1]

business application, legacy application: synonym for abstract software application

shared service: synonym for abstract software service designed to be used cross use cases[18]

subject: human or legal entity or technical system

human: living natural person with individual rights and responsibilities

legal entity: entity recognized by law as having rights and responsibilities

technical entity: thing designed by a human having a distinct existence

Business roles

data provider: legal entity providing data[19] on a request of a data consumer

data consumer: legal entity requesting data

AAS server operator: legal entity operating an AAS server on behalf of a data provider

AAS client operator: legal entity operating an AAS client on behalf of a data consumer

[17] An AAS server provides logical interfaces for the administration of AASs, the administration of Submodels and an AAS- and Submodel-repository according to IEC 63278-5. In terms of [7] an AAS server provides the logical interfaces for Discovery Interface, AAS Registry Interface, AAS Interface, Submodel Registry Interface and Submodel Interface.

[18] According to [2] a shared service is designed and developed by Factory-X “Kernel & Basis Services”. It is operated by an operator of shared service, see **Fehler! Verweisquelle konnte nicht gefunden werden.**, and can be used by different business applications. A purpose to design and develop shared services is the reuse across use cases. A shared service can be provided by a shared service provider in compliance with the requirements of Factory-X “Kernel & Basis Services and the governance body.

[19] A data provider has the rights to use and provide the data.

company lookup operator: legal entity operating a company lookup service

trusted partner list operator: legal entity managing a list of trusted partner entries

governance body: legal entity providing governance

standardization body: legal entity developing a standard and having the authority to do this

certifier: legal entity creating a certificate regarding compliance

standardization community: organization of different business stakeholders pursuing a common standardization goal

supporting service: legal entity providing services, for example consulting services or development services

shared service provider: legal entity providing or licensing a shared service

shared service operator: legal entity operating a shared service

business application provider: legal entity providing or licensing a business application commercially

business application operator: legal entity operating a business application commercially

Human/organizational roles

AAS client user: human belonging to a data consumer and interacting with an AAS client

Technical entities

company lookup service: abstract software service managing a list of company lookup information

company lookup information: information provided by a company describing how another company can access software services of the company

credential store service: abstract software service managing credentials in a secure way[20]

credential: technical entity associated to a subject enabling verification that the subject is what it claims to be

identity and access management service: abstract software service issuing and proving on request credentials and token

token: credential for a set of assertions

gateway service: abstract software service which establishes a connection between several abstract software services

token exchange service: abstract software service receiving a token and providing another token

trusted partner list management service: abstract software service managing a list of trusted partner entries

trusted partner entry: information provided by a partner and managed by a legal entity describing that the partner is considered trustworthy by the legal entity

IMPRINT

[20] A wallet is an implementation of a credential store service.

Publisher (to be deleted for internal use)

Manufacturing-X Guidance Board

Manufacturing-X Guidance Board

Project Office Manufacturing-X (to be deleted for internal use)

Open Industry 4.0 Alliance Implementation GmbH

Willy-Brandt-Platz 6

81829 Munich, Germany

Version History

March 2026 – Version 1.0 (First Release)

Authors

Mathias Brunkow Moser - Catena-X Automotive Network e.V.

Frank Wolter - Siemens AG

Eric Schmidt - VDMA

Per-Henrik Addicks - SAP SE

PART OF MANUFACTURING-X

Funded by the European Union NextGenerationEU

Supported by: Federal Ministry for Economic Affairs and Climate Action on the basis of a decision by the German Bundestag