FACTORY-X

Factory-X Requirements of Use Cases

Ulrich Löwen

PART OF MANUFACTURING-X

Funded by the European Union
NextGenerationEU

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

Classification of requirements

Clarification request

- TP2 requests for specific additional information to understand discussions in TP4
- Typically, priority “very high”

Quality requirements

- Requirements setting guardrails for all normative architecture decisions in the future
- Future ADR proposals shall align with these requirements

Specific MX-Port requirements

- Requirements associated to one or more specific layer of the MX-Port concept

Process requirements

- Requirements setting guardrails for processes to be followed

TP2 is the subproject 2 covering all Use Cases in Factory-X
TP4 is the subproject 4 developing the technical base (MX-Port Configuration)

Overview of Factory-X Requirements

Req. No.	Title	Short description
		requirement purpose
1: quality requirement	Operation of Shared Services	To avoid lock-in, mandatory shared services shall not be operated by only one specific operating company
2: clarification request	MX-Port Conformance	Functional, interface, and conformance specification
3: quality requirement	MX-Port Modularity	Provision of individual constituents of MX -ort by different software providers
4: quality requirement	MX-Port Usability	Easy definition of interfaces and implementation of functionality of MX Port so that it can be mastered by SMEs
5: MX Discovery	Access link	How to manage MX Port Discovery Information
6: MX Access & Usage Ctrl	Identity issuing	How to manage MX Port Identity
7: MX Access & Usage Ctrl	Certification authority	How to enable trust and verification
8: clarification request	MX Port – DSP and DCP	Explain relationship between MX-Port and DSP/DCP on conceptual level
9: quality requirement	Cloud architectures	Considering best practices for cloud architectures
10: clarification request	Shared Services	Framework to discuss business impact of ADRs
11: quality requirement	AAS implementation	Asset Administration Shell usage in the use cases
12: MX Access & Usage Ctrl	Authorization	How to give access to data
13: MX Gate	Notification	Sending/publishing notifications to one or multiple recipients
14: MX Discovery	Broadcast search	Search for companies, applications or products with specific characteristics
15: process requirement	Testbed	Testbed (infrastructure) incl. Hackathons for use cases
16: process requirement	AAS Submodel templates	Guardrails for the proper usage of AAS Submodel Templates
17: MX Access & Usage Ctrl	Usage control	Dealing with usage rights for data offerings
18: MX Access & Usage Ctrl	Public data	No access control necessary
19: MX Access & Usage Ctrl	Restricted data	Protective mechanism defined by data provider

FACTORY-X

MX Access and Usage Control Overall considerations

Overall business requirements
Justified by Factory X North Star

- Each company shall be able to operate its own system in which it manages its own identities*)
  - Scalability: Continue to use existing infrastructures and established procedures, to the extent possible
  - Scalability: Secure my investment in the installed base
  - Scalability: Be able to access and use the data ecosystem, appropriate (cost, time & quality) to my company structure (size, product, market, …)
  - Interoperability: Set and use the standards that are relevant for me
- A solution shall be designed in such a way that the identities*) managed in the systems of the individual companies should not be duplicated
  - Scalability: Be able to access and use the data ecosystem, appropriate (cost, time & quality) to my company structure (size, product, market, …)
- The access to a solution shall be as open as possible, a lock-in by a commercial 3rd party legal entity should be avoided
  - Interoperability: Be not locked-in by a specific operating company
  - Scalability: Have no restriction on access by application providers
- The costs for integration and operation of a solution shall not be higher than the benefit it provides (this is a matter of course)

*) subject of identities can be legal entities, humans or technical systems (for example a machine or a software service)

Overall scenarios on business level

Scenarios on business level

- Scenario 1 “public data”
- Scenario 2 “restricted data” based on protective mechanism defined by data provider
- Scenario 3 “restricted data” based on protective mechanism, on which data provider and data consumer have agreed
  - In general, there are different solutions to such solutions, for example “federated identities” approaches or “self sovereign identities” approaches

Underlying justification by Factory X North Star

- Trust & Security: Divide my business partners into different “trust classes” and then treat them accordingly
- Trust & Security: Divide my data into different “confidentiality levels” and then treat them accordingly
- Interoperability: Be able to choose the level of interoperability that is right for me

Link to Factory X North Star

- The scenarios describe **requirements** for (probably three different) **functional manifestations** of MX Access & Usage Control

Cross-company data exchange
MX Access & Usage Control – high level description

Scenarios on business level

Scenario 1: Requirement #18

- As **data consumer**, I want to receive public data from a data provider without being affected by any access control mechanism
- As **data provider**, I want to provide public data to a data consumer without being affected by any access control mechanism

Scenario 2: Requirement #19

- As **data consumer**, I want to receive data from a data provider that is made available to me when I identify myself with an identity provided by the data provider
- As **data provider**, I want to provide data to data consumer provider, when the data consumer identifies himself with an identity provided by myself

Scenario 3: Requirement #6, #7

- As **data consumer**, I want to receive data from a data provider that is made available to me when I identify myself with an identity managed by myself; to do this, the data provider needs a mechanism to authenticate my identity
- As **data provider**, I want to provide data to a data consumer, when the data consumer identifies himself with an identity managed by himself if there is a mechanism that I can authenticate the identity

Requirement #1

Operation of Shared Services – To avoid lock-in, mandatory shared services shall not be operated by only one specific operating company

quality requirement

Requirement #1: Operation of Shared Services

To avoid lock-in, mandatory shared services shall not be operated by only one specific operating company

Illustration

	mandatory shared service	optional shared service
operation open to any certified operating company		
operation only by one specific operating company	*lock-in by operating company*	

Initial situation

- Shared services are **designed** and prototypically developed by TP4 and can be used by business applications
- Shared services can be **provided** by a shared service provider in compliance with the requirements of TP 4 and the governance body
- Shared services can be **operated** by a shared service operator in compliance with the requirements of TP 4 and the governance body
- There can be mandatory shared services (i.e., a business application shall use the shared service) and optional shared services (i.e., a business application can use the shared service)

Problem statement

- To avoid lock-in, mandatory shared services shall not be operated by only one specific operating company

Boundary conditions

- -

Requirement #2

MX-Port Conformance – Functional, interface, and conformance specification

clarification request

clarification requests are not published externally

Requirement #3

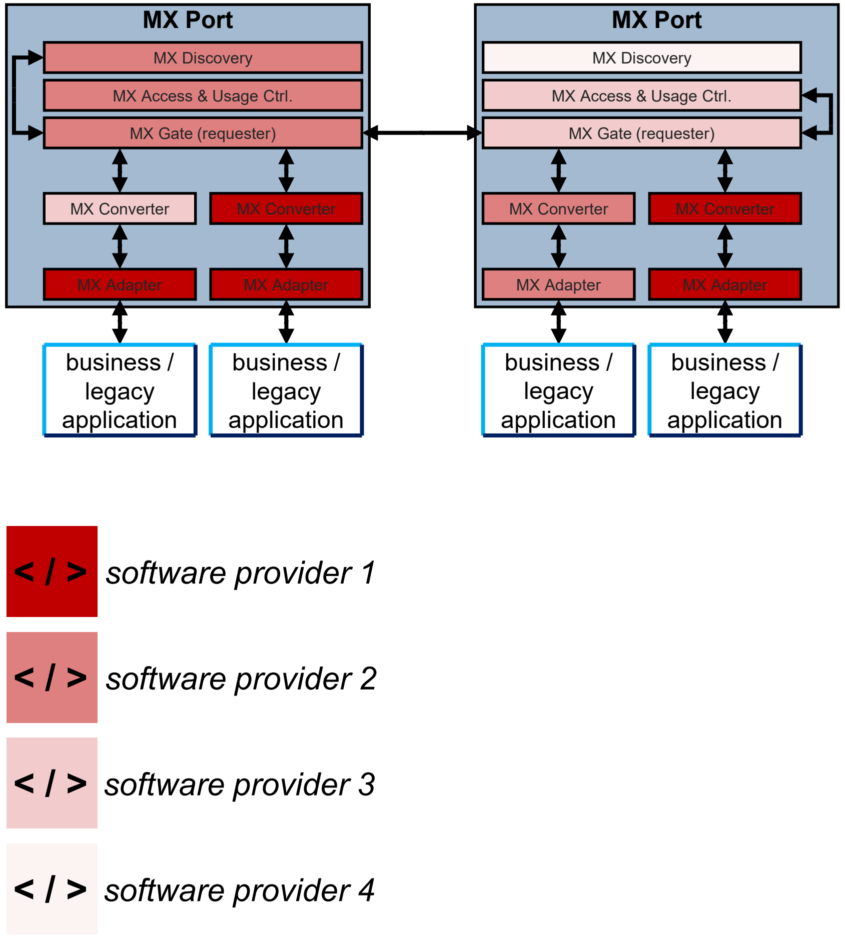
MX-Port Modularity – Provision of individual constituents of FX Port by different software providers

quality requirement

Requirement #3: MX-Port Modularity

Provision of individual constituents of MX-Port by different software providers

Illustration (example)



MX Port
MX Discovery
MX Access & Usage Ctrl.
MX Gate (requester)
MX Converter
MX Converter
MX Adapter
MX Adapter
business / legacy application
business / legacy application
MX Port
MX Discovery
MX Access & Usage Ctrl.
MX Gate (requester)
MX Converter
MX Converter
MX Adapter
MX Adapter
business / legacy application
business / legacy application
< / > software provider 1
< / > software provider 2
< / > software provider 3
< / > software provider 4

Initial situation

- Conceptually, MX-Port is modular and consists of various constituents (MX Discovery, MX Access & Usage Control, MX Gate, MX Converter, MX Adapter)

Problem statement

- It shall be possible that the individual constituents can be provided from **different** software providers

Boundary conditions

- The current modularization should be critically reviewed again
  - MX Access & Usage Control should be renamed, because “access control” and “usage control” address different concerns and the term “usage control” has a different meaning in the general community
- If the individual constituents are provided by different software providers, they must be integrated into an MX-Port as part of a system integration

Requirement #4

MX-Port Usability – Easy definition of interfaces and implementation of functionality of MX-Port so that it can be mastered by SMEs

quality requirement

Requirement #4: MX-Port Usability

Easy definition of interfaces and implementation of functionality of MX-Port so that it can be mastered by SMEs

Initial situation

- A key aspect of a company's technological sovereignty is to master the technologies essential to its own business
- Companies should therefore be enabled to decide for themselves which constituents of an MX-Port they want to provide themselves and where they want to use 3rd party service providers
- This is a fundamental prerequisite for broad acceptance of Factory-X

Problem statement

- Both the definition of the interfaces of the constituents of an MX-Port and the implementation of the functionality on an implementation technology shall be so simple that it can be mastered by SMEs

Boundary conditions

- The definition of the interfaces of the constituents of an MX-Port should be based on an established international standard

Requirement #5

Access Link – How to manage MX-Port Discovery Information

MX Discovery

Requirement #5: Access Link
How to manage MX-Port Discovery Information

Initial situation

- There is an asset provider and an asset user who want to automatically exchange selected or all data about the asset
- In addition, there are other stakeholders who are interested in the asset, e.g., an engineering or service provider commissioned by an asset user and may also modify or extend the data of the asset during the lifecycle or the asset
- Each stakeholder interested in an asset manages selected or all data about the asset under the own responsibility
- The asset provider provides the asset user with computer-processable data about the asset in the form of “asset identification information”
- Based on the “asset identification information”, a stakeholder who is interested in the asset can establish the association between the asset and the data about the asset managed under the own responsibility
- There are already legal contracts negotiated between the stakeholders concerned regarding their interests in the asset (rights and obligations of the stakeholders concerned)

Problem statement

- The following ways of determining the computer-processable data about the asset in the form of “asset identification information” provided by the asset provider shall be supported
  - The “asset identification information” is applied by the asset provider to a physical asset in the form of an optoelectronic computer-readable font; a human shall be able to read this font with an appropriate reading device (provided that the physical conditions allow access to this font at all)
  - The “asset identification information” is applied by the asset provider to a physical asset in the form of a human-readable font; a human shall be able to manually enter this font into an appropriate input device (provided that the physical conditions allow access to this font at all)
  - Based on knowledge, a human can use information from other sources (for example the “asset identification information” from other assets or databases) to determine the required “asset identification information” and to do an appropriate selection of data.
  - Based on proper versioning or other labeling means, a software service can find the relevant data
- For possible solutions, it shall be elaborated what a legal entity shall do once to be able to use this solution and what shall be ensured during operation that the solution can be operated
- For possible solutions, technical, regulatory and economic aspects shall be considered

Boundary conditions

- The data about an asset held by a stakeholder under the own responsibility should follow a standard established in the market (e.g., IEC 63278 Asset Administration Shell)
- The computer-processable data about the asset in the form of “asset identification information” should follow a standard established in the market (e.g., IEC 61406-1 Identification Link)
- A solution is favored in which the one-off costs and the costs during operation are as low as possible
- The access to a solution should be as open as possible, a lock-in by a commercial 3rd party legal entity should be avoided
- The costs for integration and operating of a solution shall not be higher than the benefit it provides (especially regarding solutions already established on the market)

Backup Requirement #5: Access Link Examples of possible solutions

Federated solution

- Each legal entity operates a local “discovery registry”
- Standardized format of “asset identification information”
  - The “asset identification information” can also be included in the information that is passed on by the provider of the asset to the user of the asset, e.g., as part of a Submodel of the AAS

Evaluation [according requirements]

- No central 3rd party required; no additional costs during operation
- Agreement on a standardized format of “asset identification information”
- Register the “asset identification information” in the own “discovery registry” as part of the contract conclusion between stakeholders interested in the asset

Central registry

- Operating a central “discovery registry” where every company must register its own “asset identification information” or the extension of a given asset ID during lifecycle

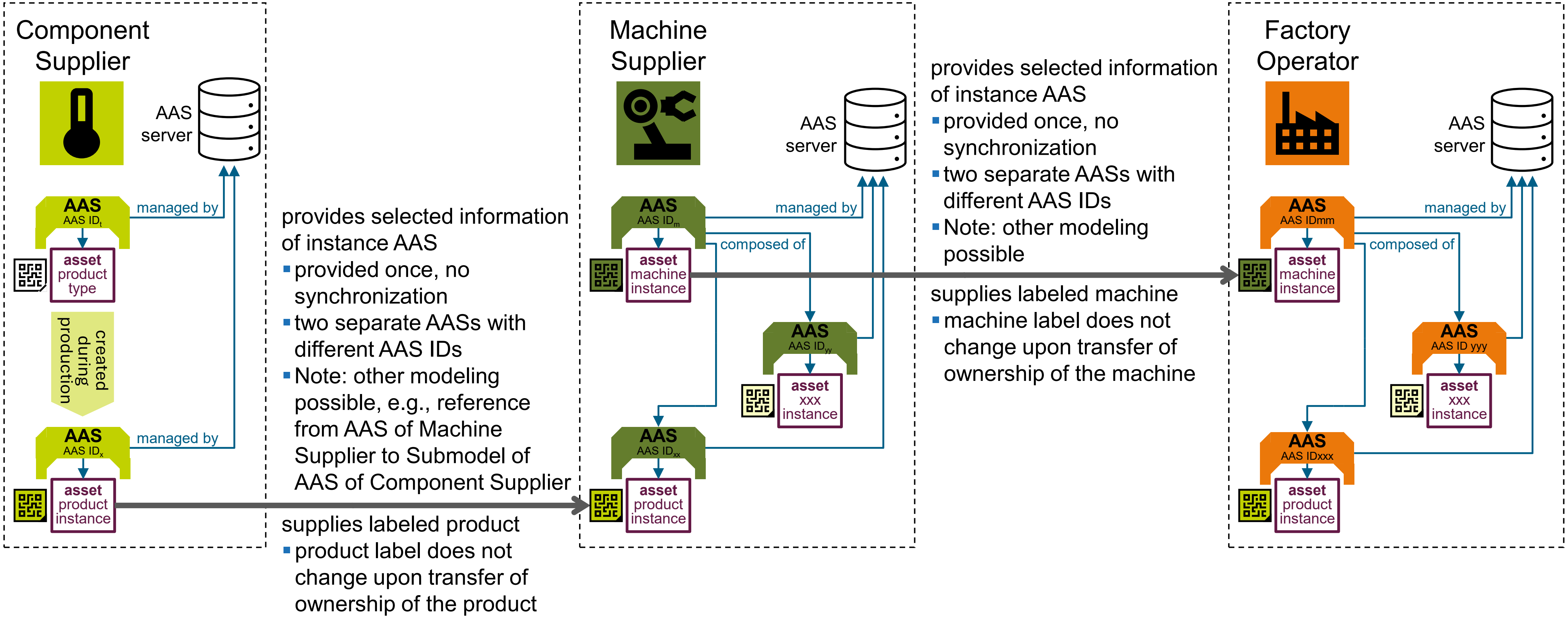
Evaluation [according requirements]

- Central 3rd party necessary (lock-in to be discussed)
- To be clarified: who operates the central registry and at what cost to the user
- Agreement on a standardized format of “asset identification information”
- Register the access link in the central “discovery registry” as responsibility of asset provider

Boundary condition

- A central “discovery registry” shall be designed that a company can protect any know-know or IP that it considers worthy of protection when registering

Backup Requirement #5: Access Link
Illustration of AAS ID (IEC 63278) and Asset ID (IEC 61406)



provides selected information of instance AAS

- provided once, no synchronization
- two separate AASs with different AAS IDs
- Note: other modeling possible, e.g., reference from AAS of Machine Supplier to Submodel of AAS of Component Supplier

supplies labeled product

- product label does not change upon transfer of ownership of the product

provides selected information of instance AAS

- provided once, no synchronization
- two separate AASs with different AAS IDs
- Note: other modeling possible

supplies labeled machine

- machine label does not change upon transfer of ownership of the machine

- Typically, the case when product is serialized, and instance specific information is created during production

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

Requirement #6

Identity Issuing – How to manage MX-Port Identity

MX Access & Usage Control

Requirement #6: Identity Issuing
How to manage MX-Port Identity

Initial situation

- There are companies that want to collaborate with each other and exchange digital data automatically
- For these purposes, the companies need machine-readable identities that shall be globally unique

Problem statement

- Legal entities shall be enabled to obtain globally unique machine-readable identities from an **identity issuer**
- For possible solutions, it shall be elaborated what a legal entity shall do once to be able to use this solution and what shall be ensured during operation that the solution can be operated
- For possible solutions, technical, regulatory and economic aspects shall be considered

Boundary conditions

- The machine-readable identities should follow a standard established in the market
- A solution is favored in which the one-off costs and the costs during operation are as low as possible
- The access to a solution should be as open as possible, a lock-in by a commercial 3rd party legal entity should be avoided
- In specific use cases, there will be requested additional services regarding machine-readable identities, e.g., the authentication of identities, but the solution should be designed in such a way that additional services can be retrofitted and can be optionally booked

Backup Requirement #6: Identity Issuing Examples of possible solutions

Federated solution

- As part of the contract conclusion, the companies involved publish to each other their own identities, for example based on a globally unique company identity
- Standardized format of identities of legal entities

Evaluation [according requirements]

- No central 3rd party required (unless implied by the standard)
- No additional costs during operation (unless implied by the standard)
- Agreement on a standardized format of identities of legal entities
- Not prepared regarding offering additional services regarding identities

Neutral identity issuer

- Determination of a (new or established) identity issuer, where each company obtains its own identity

Evaluation [according requirements]

- Central 3rd party necessary (lock-in to be discussed)
- To be clarified: who operates the identity issuer and at what cost to the user
- Agreement on a standardized format of identity
- Identity issuer can offer additional services regarding identities

Requirement #7

Certification authority – How to enable trust and verification

MX Access & Usage Control

Requirement #7: Certification Authority
How to enable trust and verification

Initial situation

- Each company manages its own identities and wants to use these for cross company data sharing.
- Data exchange across companies shall be supported for the following types of subjects: technical users or human users (both, in the context of an organization, i.e., linked to a legal entity)
- So, each company can manage identities for these different types of subjects, i.e., technical users and human users. User identities can, e.g., also include attributes of legal/organizational entities and installed business applications or devices.

Problem statement

- Software applications that want to exchange data shall know the identities to manage the access to functions and data of the business applications.
- If an identity is provided to a software application, the requested company shall be able to authenticate the identity of the subject.
- Trust between two companies (requester and provider) shall be possible to be established
  - either bilaterally: both negotiate trust relationships on their own
  - or via a trusted 3rd party, company i.e., this trusted third party acts as trust anchor for the ecosystem and therewith also for all companies, which want to share data among themselves.

Constraints

- A solution should be designed in such a way that the identities of the individual companies shall not be duplicated.
- The user experience from the perspective of the different business roles (data provider, data consumer, software provider) should be considered.
- A solution is favored in which the one-off costs and the costs during operation are as low as possible.
- Authentication means shall not bound to a specific commercial 3rd party legal entity (i.e., a vendor lock-in shall be avoided, instead open standards shall be applied).
- For specific use cases, additional trust and verification services can be provided, but the solution should be designed so that these additional services can be retrofitted and booked optionally.
- There can be multiple 3rd party companies which operate respective trust/authentication services for the ecosystem.

Requirement #8

clarification request

clarification requests are not published externally

Requirement #9

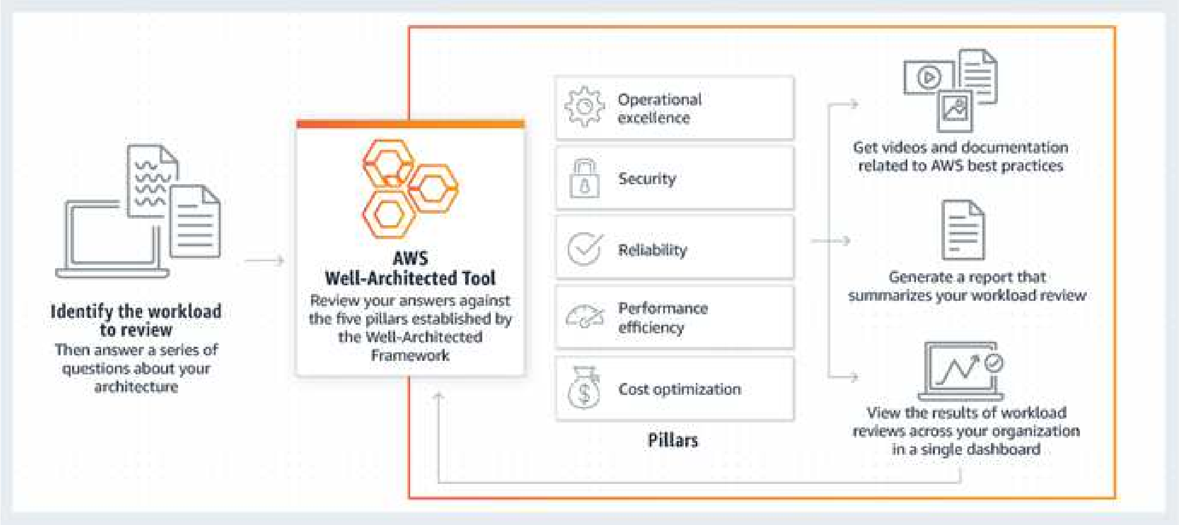
Cloud architectures – Considering best practices for cloud architectures

quality requirement

Requirement #9: Cloud architectures

Considering best practices for cloud architectures

Illustration (example)



Identify the workload to review
Then answer a series of questions about your architecture
AWS Well-Architected Tool
Review your answers against the five pillars established by the Well-Architected Framework
Operational excellence
Security
Reliability
Performance efficiency
Cost optimization
Pillars
Get videos and documentation related to AWS best practices
Generate a report that summarizes your workload review
View the results of workload reviews across your organization in a single dashboard

Initial situation

- There are already many cloud-based solutions being in practical use in the manufacturing industry
- These solution providers have come a long way to gain customers' trust in their solutions
- The providers have made these findings available to the public in best practices

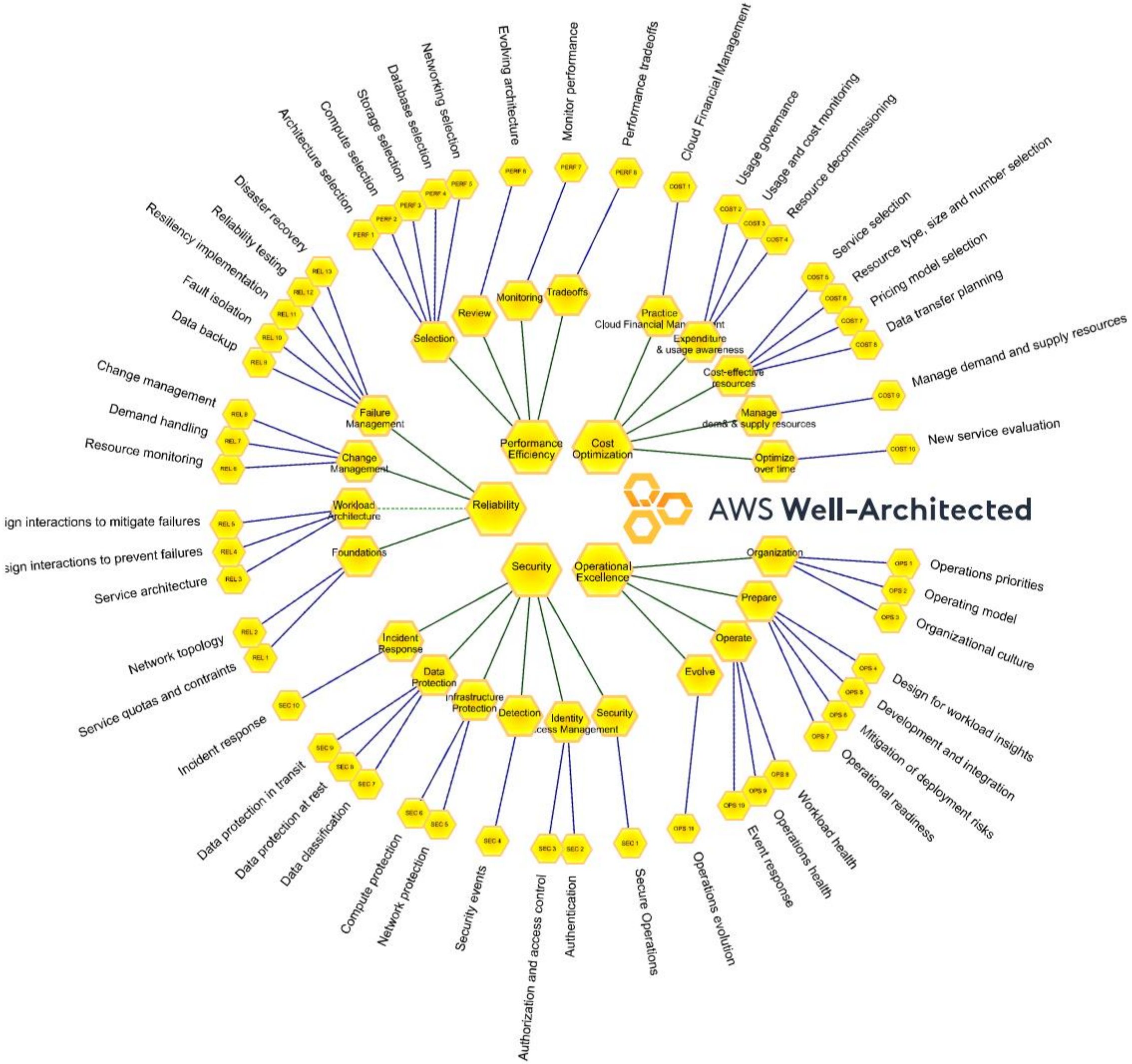
Problem statement

- TP4 shall consider best practices for cloud architectures, especially relevant, but not limited to cloud-to-cloud data exchange in terms of concept and technical implementation
- TP4 shall not prescribe solution architectures for business applications

Boundary conditions

- For an example of best practices see https://aws.amazon.com/blogs/aws/aws-well-architected-framework-updated-white-papers-tools-and-best-practices/

Backup Requirement #9



Breakdown of

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization

Source: https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.map.en.html

Requirement #10 Shared Services – Framework to discuss business impact of ADRs

clarification request

clarification requests are not published externally

Requirement #11

AAS implementation – Asset Administration Shell usage in the use cases

quality requirement

Requirement #11 AAS implementation

Asset Administration Shell usage in the use cases

Initial situation

- Many companies provide information to be shared
- An important semantic model for information in the use cases are Submodels of the Asset Administration Shell (AAS)

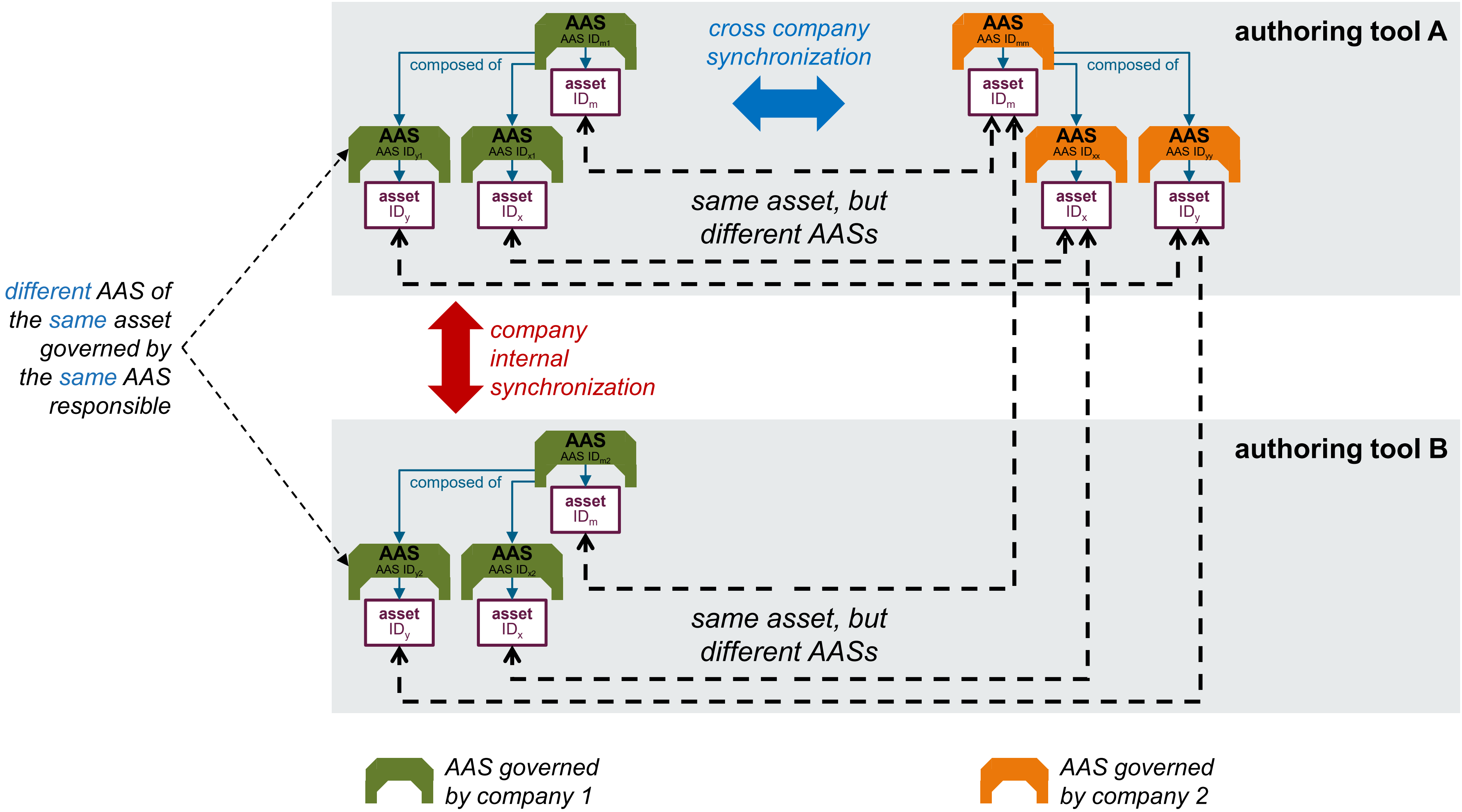
Problem statement

- The concepts for modelling assets using the AAS (according to IEC 63278 series) shall not be restricted (MX Converter)
- The access from AAS user applications (according to IEC 63278) to AASs and Submodels shall not be restricted (MX Gate to MX Gate communication)
- The concepts for describing access and usage policies for AASs, Submodels and SubmodelElements (according to IEC63278-3) shall not be restricted
- The AAS shall be expanded to include standardized discovery of AASs across companies (MX Discovery)
- The AAS shall be expanded to enable standardized identification (see Requirement #6), authentication (see Requirement #7), authorization (see Requirement #12), and usage control (see Requirement #17) (MX Access and Usage Control).

Boundary conditions

- Other semantic models like OPC UA companion specifications can exist in parallel
- Other information exchange can exist in parallel

Backup Requirement #11
Standardized conceptual object model (Illustration only)



different AAS of the same asset governed by the same AAS responsible

cross company synchronization

company internal synchronization

same asset, but different AASs

🟩 *AAS governed by company 1*

🟧 *AAS governed by company 2*

Requirement #12

Authorization – How to give access to data

MX Access &
Usage Control

Requirement #12: Authorization
How to give access to data

Initial situation

- Each company shares asset or production centric data with other companies. Data sharing is often multilateral between 3 or more companies which have a common interest to share data (e.g., asset supplier, asset operator and one or more service provider, service can be engineering, lifecycle topics including recycling, authorities like TÜV, customs ….).
- Information shared or transferred by business applications shall be accessible for authorized subjects only. A subject always belongs to a company (legal entity). It can be a natural person, a group of persons or technical system for automated workflows which can reduce the workload of persons.
- Access to data offerings can be unlimited or restricted or in addition even subject to usage rights as typically defined in product sheets and T&Cs of the involved companies since pure data can't be legally owned. (see also Requirement #17 for usage rights)
- Access to data is regulated in various EU data acts, export control and the General Data Protection Regulation (German DGVO), which need to be considered by the owner of a data offering.

Problem statement

- Each company has the sovereignty for its data offering, controls which subjects of its own and other companies can access and use it.
- Based on subjects, the companies will configure access rights to "their" data which are part of their defined offering.
- The models of access rights or role-based access are in the responsibility of the data offering companies, the models may be different for each company or business application.
- The role-based access is multidimensional. A subject may belong to more than one category of roles (human/machine; role; department, entity, country, etc.)
- It shall be possible to restrict data sharing to a particular time period.

Boundary conditions

- The solution shall be designed in such a way that the access policies to the data can be set up by the company owning the offering of the data.
- The solution shall allow a simple rule-based management of access rights based on a common model for the criticality of data to be protected (public, restricted, confidential, strictly confidential). The owner of the offering is responsible for a correct labeling or rule set which allow to protect his data. The solution shall enforce these labels or rules.
- The solution shall be compatible with the legacy applications, at best allowing the legacy applications to use the solution to check access rights and then add the access for subjects of other companies to the legacy system.
- It is assumed that a misuse of an authorized access or usage within a business application can be monitored but not necessarily prevented by the solution. (See also Requirement #17 for details on usage control)

Requirement #13

Notification – Sending/publishing notifications to one or multiple recipients

MX Gate

Requirement #13: Notification
Sending/publishing notifications to one or multiple recipients

Initial Situation

- Polling from the data consumer to the data provider (only synchronous communication available)
- Many manual mechanism and tedious processes – if any – between two companies exist
  - Example: Distributing Product Change Notifications

Problem Statement

- Notification Provider shall be able to send/publish a notification for one or multiple Notification Consumer(s)
- Notification Consumer shall be able to send a receipt to the Notification Provider acknowledging reception whenever the notification requires an acknowledgement. This receipt should arrive in reasonable time
- Case 1:
  - Notification Consumer shall be able to subscribe to a set of notifications from a Notification Provider
  - Notification Consumer and Notification Provider shall be able to unsubscribe from such a notification
- Case 2:
  - Notification Provider and Notification Consumer know each other a-priori and shall be able to send and receive notifications.
- Verification of Notification Provider, Notification Consumer and notification shall be possible (see Requirement #7)
- No other than the intended Notification Consumer of any notification shall be able to know the existence or the content of that notification

Boundary Conditions

- No additional requirements on usage control (see Requirement #17)
- A Notification Consumer can basically only be found if the Notification Consumer has agreed to be found
- A lock-in by commercial 3rd party legal entity should be avoided

Requirement #14

Broadcast search – Search for companies, applications or products with specific characteristics

MX Discovery

Requirement #14: Broadcast search

Search for companies, applications or products with specific characteristics

Initial situation

- A data/service requester needs to find a suitable data/service responder based on specific information/functionality to provide (e.g., properties of an AAS Submodel)
- Examples:
  - Finding a supplier of a product with specific properties
  - Finding a manufacturing service provider providing specific manufacturing capabilities
  - Finding a business application operator operating a business application with specific functionalities

Problem statement

- A data/service requester shall be able to address a request to all data/service responder, which have implemented the “broadcast functional solution” in the MX Discovery Layer of their MX-Port
- Therefore, the MX Discovery layer from the requester shall be able to find all MX Discovery layers from responder and check whether they have the “Broadcast functional solution” implemented
- Additionally, the MX Discovery layer shall be identifiable to confirm its capability to provide the required information or functionality.
  - E.g.: The request shall indicate a set [1..m] of properties of AAS Submodels with given property values or property ranges
- As soon as a MX Discovery request found one or more MX Discovery responders, the information/functionality exchange can start
  - E.g.: All data/service responder which have the “broadcast functional solution” implemented in their MX Discovery layer shall provide a response if the data/service responder matches the abovementioned request

Boundary conditions

- A data/service responder can basically only be found if the data/service responder has agreed to be found
- A lock-in by commercial 3rd party legal entity should be avoided
- The provider of the information/functionality should be able to verify the legal identity of the requester (Requirement #7)
- The provider of the information/functionality should be able to check the authorization of the requester (Requirement #12)
- It can be assumed the requested information/functionality is described by an AAS; the asset can be for example a product type, a capability or a software application

Requirement #15

Testbed – Testbed (infrastructure) inclusive Hackathons for use cases

process requirement

Requirement #15: Testbed
Testbed (infrastructure) inclusive Hackathons for use cases

Illustration (example)

Initial situation

- Use cases want to validate first “walking skeletons” of their business applications, but have **no infrastructure** to test or deploy them
- Use cases have **no idea / information**, …
  - which shared services are already existing and
  - how to use them (lack of hands-on experience with shared service).

Problem statement

- A **test infrastructure** with hosted shared services (MX-Port elements) shall be provided for validating Use Case “walking skeletons”
- Opportunities to get **hands-on experience** with relevant technologies (e.g., MX-Port elements such as EDC, AAS server, …) should be created, e.g., by means of hackathons

Boundary conditions

- Blueprint: Thin[gk]athon Manufacturing-X Tickets, Mon, Nov 4, 2024 at 9:00 AM | Eventbrite

Requirement #16

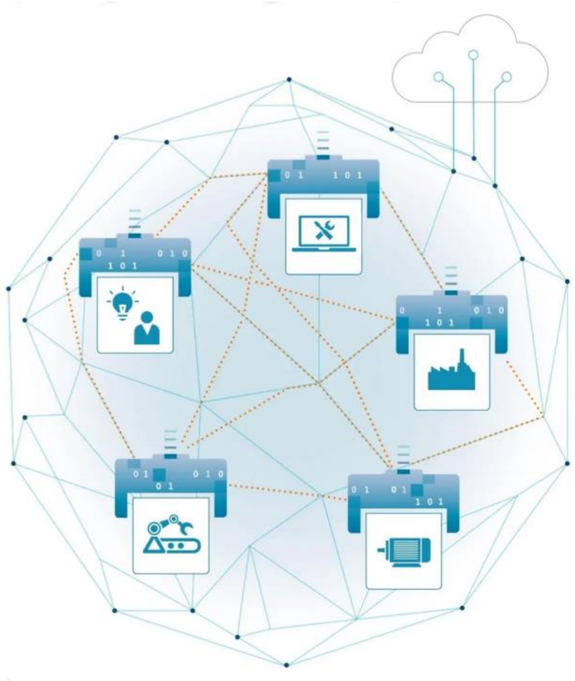
AAS Submodel templates – Guardrails for the proper usage of AAS Submodel Templates

process requirement

Requirement #16: AAS Submodel Templates

Guardrails for the proper usage of AAS Submodel Templates

Illustration (example)



Initial situation

- Several use cases want to use AAS to model asset data in a standardized form for interoperable data exchange
- Use case actors have different levels of knowledge regarding the proper use of AAS Submodels and Submodel templates

Problem statement

- A governance body shall define and maintain guidelines how to
  - develop, publish and maintain Submodel templates – it shall be addressed that the existing Submodel templates are kept consistent with each other
  - use Submodels and Submodel templates
- A governance body should define and maintain guidelines how to model complex assets (e.g., machines)

Boundary conditions

- IDTA offers consultation hours regarding AAS, especially for the development of Submodel templates by TP2
- The DAVID project, led by IDTA, coordinates the proper usage of AAS within Manufacturing-X and ensures their standardization→ BMWK - Projekt „DAVID“

Requirement #17

Usage control – Dealing with usage rights for data offerings

MX Access & Usage Control

Requirement #17: Usage Control
Dealing with usage rights for data offerings

Initial situation

- Dataspaces in general assume that there are data providers and data consumers, where the data provider has full control over its data offering which he can control via the access rights to ensure that the data offering is accessible for authorized subjects only (see Requirement #12).
- But a data provider may also want to limit the usage rights of this data offering, which is often technically not possible without big effort once the access rights are granted for another subject. (e.g., for manuals which are not allowed to be copied or redistributed to/for other legal entities)
- Usage rights are therefore typically defined in product sheets and T&Cs of the involved companies since pure data can't be legally owned.

Problem statement

- Each company has the sovereignty for its data offering and want to monitor (legally approve) how subjects are using the data offering.
- Based on subjects, the companies will define usage rights to "their" data which are part of their defined offering.
- The models for (role based) usage rights are in the responsibility of the data offering companies, the models may be different for each company or business application.
- The role-based usage right is multidimensional. A subject may belong to more than one category of roles (human/machine; entity, country, etc..).
- The usage rights are multidimensional. The subject may need to consider more than one category of rights (mass operation; storage; sharing, etc.).

Boundary conditions

- The enforcement of usage rights shall not lead to inappropriate complexity or poor usability of authorization in general. It is assumed that a misuse of an authorized usage can't necessarily be prevented by the solution (e.g., unauthorized usage, copying or forwarding of data to subjects with no access or usage rights). The solution shall therefore focus on monitoring and reporting (and a high risk to be sued) if prevention is technically impossible.
- The solution shall be designed in such a way that the usage policies for the data can be set up by the company owning the offering of the data.
- The solution shall allow a simple rule-based management of usage rights based on a common model for the criticality of data to be protected (public, restricted, confidential, strictly confidential) and predefined usage categories (e.g. unlimited machine usage and data forwarding, limited machine usage and/or data storage, read only). The owner of the offering is responsible for a correct labeling or rule set which allows to protect the usage of his data offering. The solution shall monitor or report these labels or rules.
- The solution should be a generic reuse service which is integrated or linked to the access right service. The owner of the business application may need to add a kind of "soft sensors" which help the solution to monitor misuse of data offerings.

Requirement #18

Public data – No access control necessary

MX Access & Usage Control

Requirement #18: Public data

No access control necessary

Initial situation

- Many use cases exchange public data between different legal entities
- Sometimes the legislator requires that certain data be made available free of charge (for example, security patches); there is no additional benefit for the data provider by making this data available, so the data provider will meet these requirements with minimal effort
- Data provider and data consumer have agreed on a semantic model of the data to be exchanged (“MX Converter compliant”) and the access mechanisms (“MX Gate compliant”)

Problem statement

- As a human or software application of a **data consumer** as legal entity, I want to receive public data from a software application of a data provider without being affected by any access control mechanism
- As a software application of a **data provider** as legal entity, I want to provide public data to a human or software application of a data consumer without being affected by any access control mechanism
- As a data provider and data consumer, I do not want to be forced to register at any 3rd party entity for data exchange

Boundary conditions

- A solution is necessary in which the one-off costs and the costs during operation are as low as possible
- Public data can also optionally be linked to usage policies, see Requirement #17

Requirement #19

Restricted data – Protective mechanism defined by data provider

MX Access & Usage Control

Requirement #19: Restricted data
Protective mechanism defined by data provider

Initial situation

- There are existing infrastructures where restricted data is already exchanged between legal entities
- The data provider provides a mechanism for identification and authentication, and the data consumer uses this mechanism

Problem statement

- As a human or a software application of a **data consumer** as legal entity, I want to receive data from a software application of a data provider that is made available to me when I identify myself with an identity provided by the data provider
- As a software application of a **data provider**, I want to provide data to a human or software application of a data consumer, when the human or software application of the data consumer identifies himself with an identity provided by my legal entity
- As a data provider and data consumer, I do not want to be forced to register at any 3rd party entity for data exchange

Boundary conditions

- With this approach, a data consumer must use a specific identification and authentication mechanism for each data provider; as the number of data providers increases, this will no longer be manageable in the future
- A solution is necessary in which the one-off costs and the costs during operation are as low as possible
- Restricted data can also optionally be linked to usage policies, see Requirement #17