Release – 21.03

Gaia-X Architecture Document

Imprint

Publisher

GAIA-X, European Association for Data and Cloud, AISBL
Rue Royale 94
1000 Bruxelles
www.gaia-x.eu

Authors

Gaia-X TC Working Group Provider
Gaia-X TC Working Group User
Gaia-X TC Working Group Architecture
Gaia-X TC Working Group Federation Services / Open Source Software
Gaia-X TC Working Group Portfolio
Gaia-X Technical Committee
Gaia-X Open Work Packages

Current as at

April 2021

Content editor

Anna-Maria Schleimer (Fraunhofer ISST)
Nils Jahnke (Fraunhofer ISST)

Design and production

ifok GmbH, 64625 Bensheim

Technical contact

Email: architecture-document@gaia-x.eu

Copyright

© 2021 Gaia-X, European Association for Data and Cloud, AISBL

This document is protected by copyright law and international treaties. You may download, print or electronically view this document for your personal or internal company (or company equivalent) use. You are not permitted to adapt, modify, republish, print, download, post or otherwise reproduce or transmit this document, or any part of it, for a commercial purpose without the prior written permission of Gaia-X, European Association for Data and Cloud, AISBL. No copying, distribution, or use other than as expressly provided herein is authorized by implication, estoppel or otherwise. All rights not expressly granted are reserved.

Third party material or references are cited in this document.

Content

1

Overview

1 Overview

1.1 Introduction

Gaia-X aims to create a federated open data infrastructure based on European values regarding data and cloud sovereignty. The mission of Gaia-X is to design and implement a data sharing architecture that consists of common standards for data sharing, best practices, tools, and governance mechanisms. It also constitutes an EU federation of cloud infrastructure and data services, to which all 27 EU member states have committed themselves[1]. This overall mission drives the Gaia-X Architecture [2].

The Gaia-X Architecture identifies and describes the concepts of the targeted federated open data infrastructure as well as the relationships between them. It describes how Gaia-X facilitates interoperability and **Interconnection** between all participants in the European digital economy, with regard to both data and services.

This draft for the Gaia-X Architecture addresses stakeholders from industry, the public sector, science and other stakeholders. It replaces the former architecture document Gaia-X: Technical Architecture, Release – June 2020[3].

1.2 Objectives

This document describes the top-level Gaia-X Architecture model. It focuses on conceptual modelling and is agnostic regarding technology and vendor. In doing so, it aims at representing the unambiguous understanding of the various Gaia-X stakeholder groups about the fundamental concepts and terms of the Gaia-X Architecture in a consistent form at a certain point in time. It forms the foundation for further elaboration, specification, and implementation of the Gaia-X Architecture. Thus, it creates an authoritative reference for the Gaia-X **Federation Services** specification.

The Gaia-X Architecture Document is subject to continuous updates reflecting the evolution of business requirements (e.g. from dataspace activities in Europe), relevant changes in regulatory frameworks, and the advancements regarding the technological state of the art.

1.3 Scope

The Gaia-X Architecture document describes the concepts required to set up the Gaia-X Data and **Infrastructure Ecosystem**. It integrates the **Providers, Consumers**, and Services needed for this interaction. These Services comprise ensuring identities, implementing trust mechanisms, and providing usage control over data exchange and **Compliance** – without the need for individual agreements.

The Gaia-X Architecture document describes both the static decomposition and dynamic behaviour of the Gaia-X core concepts and Gaia-X **Federation Services**.

Details about implementing the **Gaia-X Ecosystem** are to be defined elsewhere (see **"Architecture of Standards"**).

At present, automated contracts, legal binding, monitoring, metering as well as billing mechanisms, amongst others, are not within the scope of this document.

[1] European Commission. (2020). Towards a next generation cloud for Europe. https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[2] Federal Ministry for Economic Affairs and Energy. (2019). Project Gaia-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-Gaia-X.htm

[3] Federal Ministry for Economic Affairs and Energy. (2020). Gaia-X: Technical Architecture: Release - June, 2020. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/Gaia-X-technical-architecture.html

The Gaia-X Architecture document includes a glossary which identifies and defines those terms that have a distinct meaning in Gaia-X, which may slightly deviate from everyday language, or have different meanings in other architectures or standards.

1.4 Audience and Use

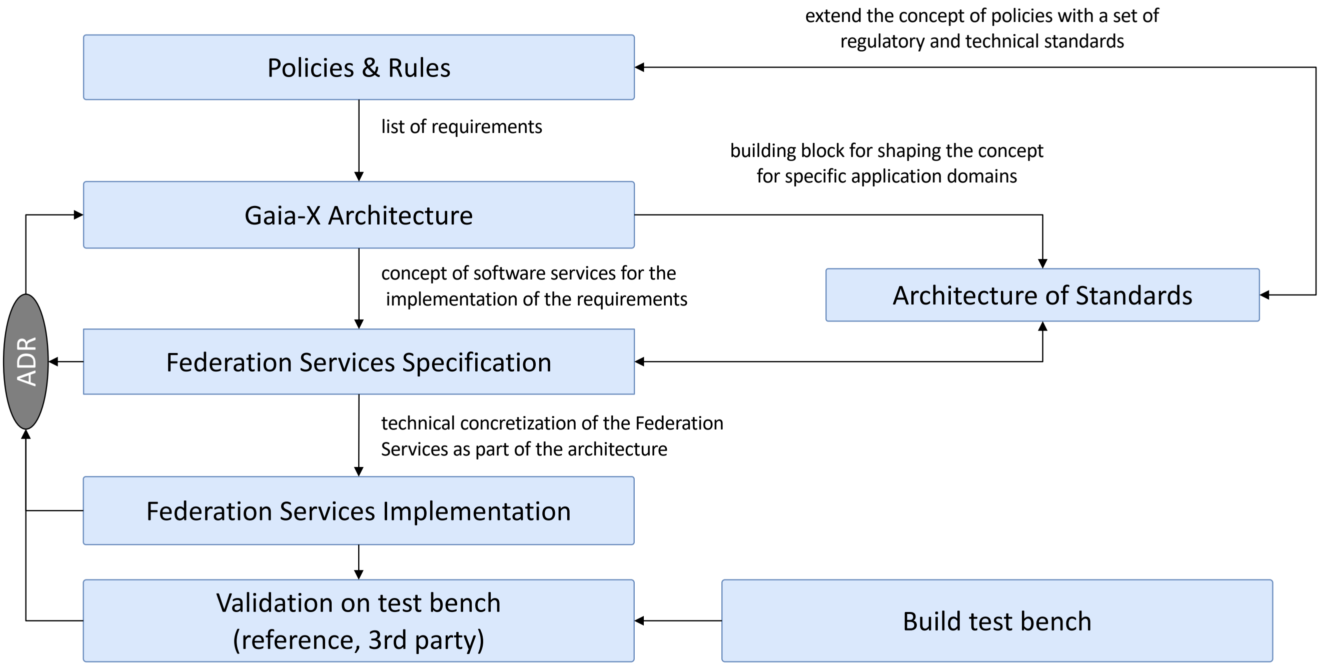
The Gaia-X Architecture document is directed towards all Gaia-X interests and stakeholder groups, such as Gaia-X AISBL members, Hub participants, and employees of companies or individuals interested in learning about the conceptual foundation of Gaia-X.

It should be used as an entry point to get familiar with the fundamental concepts of Gaia-X and their relationship between each other and as a reference for elaboration and specification of the Gaia-X Architecture.

1.5 Relation to other Gaia-X Documents

The present document is prepared by the Working Group "Architecture" within the Technical Committee, of which roles and responsibilities will be documented in the Operational Handbook (yet to be published). Additional **Compliance**-relevant information will be outlined in the documents on "Policies & Rules" as well as **"Architecture of Standards"**. The **Federation Services** specification, which is also the basis for the upcoming open source implementation adds details the **Federation Service** functionalities as well as the upcoming test bench.

Figure 1: Relation to other Documents



extend the concept of policies with a set of regulatory and technical standards
Policies & Rules
list of requirements
building block for shaping the concept for specific application domains
Gaia-X Architecture
concept of software services for the implementation of the requirements
Architecture of Standards
ADR
Federation Services Specification
technical concretization of the Federation Services as part of the architecture
Federation Services Implementation
Validation on test bench (reference, 3rd party)
Build test bench

1.6 Architecture Governance and Next Steps

The Gaia-X Architecture document contains contributions from various Gaia-X Working Groups. It is the linking pin to the associated artefacts, providing the top-level conceptual model definitions that are the basis for further specification and implementation. Changes (Request for Change or Errors) are managed in the Architecture Decision Record (ADR) process documented in a collaboration tool [4]. A more elaborated version of this Gaia-X Architecture document will be released in June 2021. This will allow contributions from all Gaia-X members.

1.7 Architecture Requirements

The architecture is utilized to address the following requirements:

- **Interoperability of data and services:** The ability of several systems or services to exchange information and to use the exchanged information mutually.
- **Portability of data and services:** Data is described in a standardised protocol that enables transfer and processing to increase its usefulness as a strategic resource. Services can be migrated without significant changes and adaptations and have a similar quality of service (QoS) as well as the same **Compliance** level.
- **Sovereignty over data:** Participants can retain absolute control and transparency over what happens to their data. This document emphasises a 'privacy-by-design' approach to comply with the EU's data protection provisions, this document.
- **Security and trust:** Gaia-X puts security technology at its core to protect every **Participant** and system of the **Gaia-X Ecosystem** (security-by-design). An **Identity** management system with mutual authentication, selective disclosure, and revocation of trust is needed to foster a secure digital **Ecosystem** without building upon the authority of a single corporation or government.

This architecture describes the technical means to achieve that, while being agnostic to technology and vendors.

1.8 Architecture Design Principles

The architecture underlies the following design principles:

- **Federation:** Gaia-X specifies federated systems of autonomous entities, tied together by a specified set of standards, frameworks, and legal rules.
- **Decentralization:** The federation principle supports decentralization and distribution within a network of Gaia-X **Participants**.
- **Openness:** Gaia-X enables an open **Ecosystem**, which means that everyone who adheres to the Gaia-X principles is welcome to participate in the community. Further, the specification and documentation of Gaia-X technologies and architectures will be openly available. Gaia-X is aware that these technologies are evolving and is open to future innovation and standards.
- **Transparency:** The technical steering and roadmap of Gaia-X is publicly available, and technology choices will be made in order to encourage distribution of collaboratively created artefacts under OSD[5] compliant open source licenses[6].

[4] Gaia-X AISBL. Architecture Decision Record (ADR) Process: GitLab Wiki. https://gitlab.com/Gaia-X/Gaia-X-technical-committee/Gaia-X-core-document-technical-concept-architecture/-/wikis/home

[5] Open Source Initiative. The Open Source Definition (Annotated). https://opensource.org/osd-annotated

[6] Open Source Initiative. Licenses & Standards. https://opensource.org/licenses

2

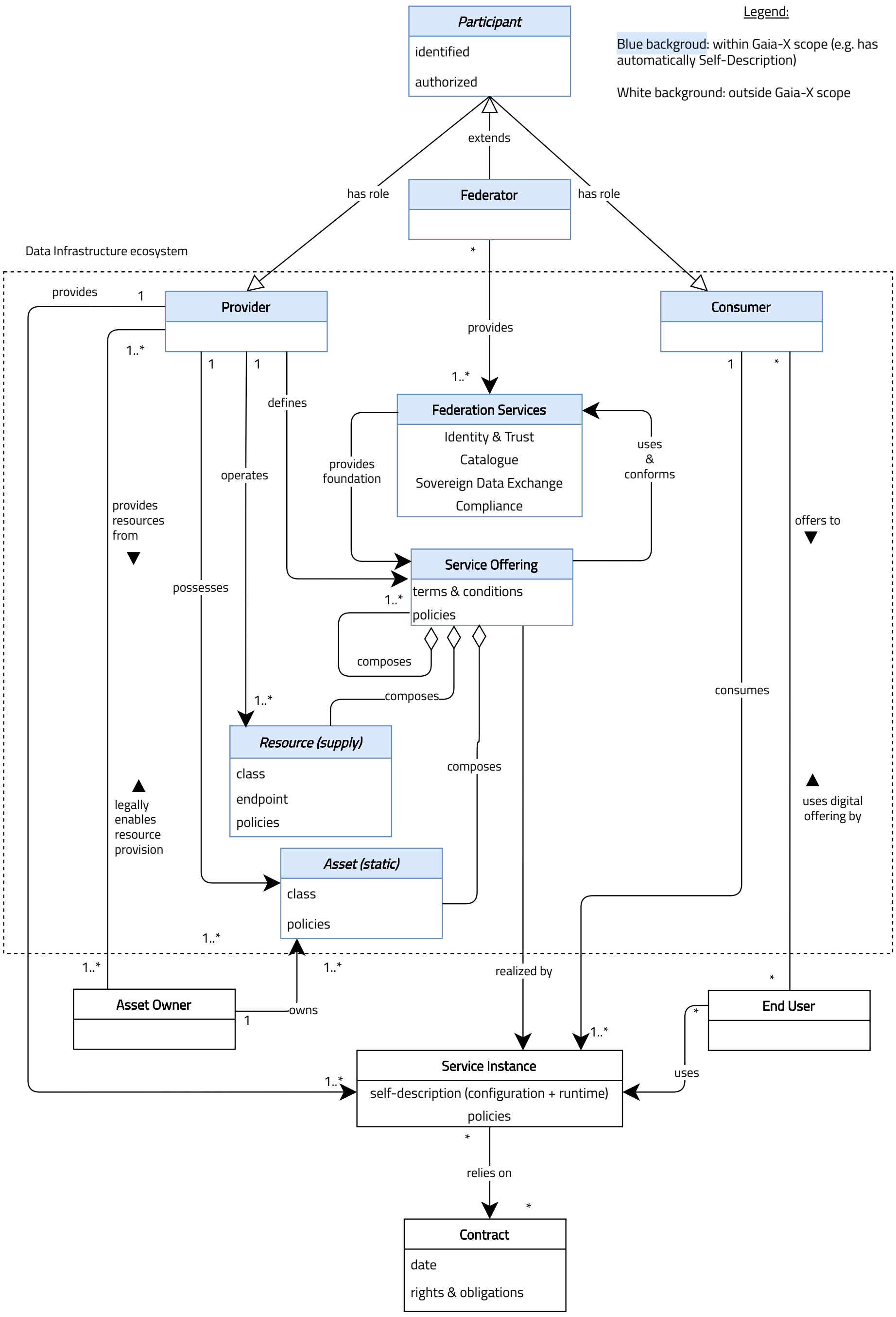
Gaia-X Conceptual Model

2 Gaia-X Conceptual Model

The Gaia-X conceptual model, shown in Figure 2, describes all concepts in the scope of Gaia-X and their relation to each other. Supplementary, more detailed models may be created in the future to specify further aspects. The general interaction pattern is further depicted in section 4.4.

The Gaia-X core concepts are represented in classes. An entity highlighted in blue shows that an element is part of Gaia-X and therefore described by a Gaia-X **Self-Description**. The upper part of the model shows different actors of Gaia-X, while the lower part shows elements of commercial trade and the relationship to actors outside Gaia-X.

Figure 2: Gaia-X conceptual model



2.1 Participants

A **Participant** is an entity, as defined in ISO/IEC 24760-1 as "item relevant for the purpose of operation of a domain (3.2.3) that has recognizably distinct existence"[7], which is onboarded and has a Gaia-X **Self-Description**. A **Participant** can take on one or multiple of the following roles: **Provider, Consumer, Federator**. Section 4 demonstrates use cases that illustrate how these roles could be filled. **Provider** and **Consumer** present the core roles that are in a business-to-business relationship while the **Federator** enables their interaction.

2.1.1 Provider

A **Provider** is a **Participant** who provides **Assets** and **Resources** in the **Gaia-X Ecosystem**. It defines the **Service Offering** including terms and conditions as well as technical **Policies**. Further, it provides the **Service Instance** that includes a **Self-Description** and technical **Policies**. Therefore, the **Provider** operates different **Resources** and possesses different **Assets**.

2.1.2 Federator

Federators are in charge of the **Federation Services** and the **Federation** which are autonomous of each other. **Federators** are Gaia-X **Participants**. There can be one or more **Federators** per type of **Federation Service**.

A **Federation** refers to a loose set of interacting actors that directly or indirectly consume, produce, or provide **Assets** and related **Resources**.

2.1.3 Consumer

A **Consumer** is a **Participant** who searches **Service Offerings** and consumes **Service Instances** in the **Gaia-X Ecosystem** to enable digital offerings for **End-Users**.

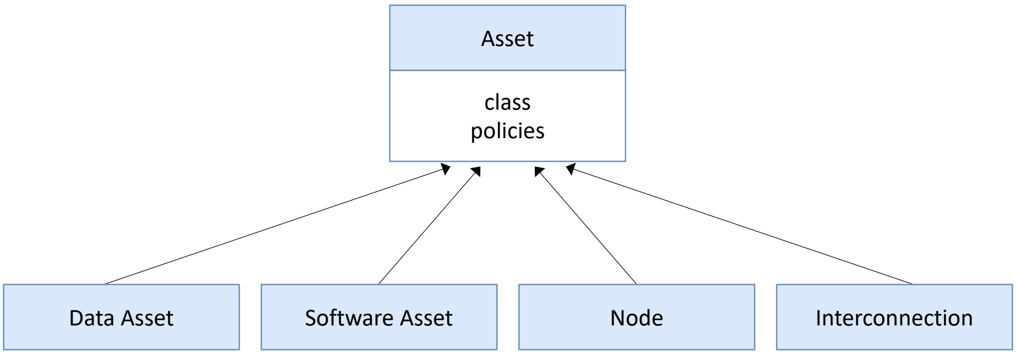
2.2 Resources and Assets

Resources and **Assets** describe in general the goods and objects of a **Gaia-X Ecosystem** and are defined as follows. **Resources** and **Assets** compose the **Service Offering**.

2.2.1 Assets

An **Asset** is an element which does not expose an **Endpoint** and is used to compose the **Service Offering**. An **Endpoint** is defined according to ISO ISO/TR 24097-3:2019(en) as a combination of a binding a network address[8]. An **Asset** can be a **Data Asset**, a **Software Asset**, a **Node** or an **Interconnection Asset**. A set of **Policies** is tied to each **Asset**. The different categories of **Assets** are visualized in Figure 3 and defined below:

Figure 3: Asset Categories



[7] ISO / IEC. IT Security and Privacy – A framework for identity management: Part 1: Terminology and concepts (24760-1:2019(en)). ISO / IEC. https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

[8] ISO/IEC. Intelligent transport systems – Using web services (machine-machine delivery) for ITS service delivery (ISO/TR 24097-3:2019(en)). https://www.iso.org/obp/ui/fr/#iso:std:iso:tr:24097:-3:ed-1:v1:en

A **Data Asset** is an **Asset** that consist of data in any form and necessary information for data sharing.

A **Node** is an **Asset** and represents a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities.

A **Software Asset** is a form of **Assets** that consist of non-physical functions.

An **Interconnection** is an **Asset** that presents the connection between two or multiple **Nodes**.

2.2.2 Resources

Resources expose an **Endpoint** and compose a **Service Offering**. They are bound to certain **Policies**.

The difference between **Resources** and **Assets** can be described as follows: **Resources** represent those elements necessary to supply **Assets**. They can be explained as internal **Service Instances** not available for order. For example, the running instance that provides a data set is a **Resource**.

2.2.3 Policies

Policies in a technical sense are defined as statements, rules or assertions that specify the correct or expected behaviour of an entity[9].

A **Policy** can be either a **Provider** Policy (alias **Usage Policies**) or a **Consumer Policy**. A **Provider** Policy constraints the **Consumer's** use of an **Asset** or **Resource**. In contrast to a **Consumer Policy**, which is a **Policy** that describes a **Consumer's** restrictions of a requested **Asset** or **Resource**[10]. In the conceptual model, they appear as attributes in all elements related to **Assets** and **Resources**.

In the legal or organizational sense, **Policy** is defined as a statement of objectives, rules, practices, or regulations governing the activities of **Participants** within Gaia-X. They build the Policy Rules, which are central element of the Gaia-X Compliance Framework and the Gaia-X Federation Services Compliance.

2.3 Federation Services

Federation Services are services required for the operational implementation of a Gaia-X **Data Ecosystem**. They are explained in greater detail in section 3.

They comprise four groups of services that are necessary to enable **Federation** of **Assets, Resources, Participants** and interactions between **Ecosystems**. The four service groups are **Identity and Trust, Federated Catalogue,** Sovereign Data Exchange and **Compliance**.

2.4 Service Offering

A **Service Offering** is defined as a set of **Assets** and **Resources,** which a **Provider** bundles into an offering and lists in a **Catalogue**. To realize service composition, a **Service Offering** can be nested with one or more other **Service Offerings**. The **Federation Services** provide the foundation for **Service Offerings** and the **Service Offering** uses and conforms to the **Federation Services**.

2.5 Additional Concepts

In addition to those concepts and their relations mentioned above, further ones exist in the conceptual model that are not directly governed by Gaia-X. These concepts do not need to undergo any procedures directly related to Gaia-X, e.g. do not create or maintain a Gaia-X **Self-Description**.

[9] Singhal, A., Winograd, T., & Scarfone, K. A. (2007). Guide to secure web services: Guide to Secure Web Services – Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD. NIST. https://csrc.nist.gov/publications/detail/sp/800-95/final https://doi.org/10.6028/NIST.SP.800-95

[10] Oldehoeft, A. E. (1992). Foundations of a security policy for use of the National Research and Educational Network. Gaithersburg, MD. NIST. https://doi.org/10.6028/NIST.IR.4734 https://doi.org/10.6028/NIST.IR.4734

First, the **Service Instance** realizes a **Service Offering** and can be used by **End-Users** while relying on a contractual basis.

Second, **Contracts** are not in scope of Gaia-X but present the legal basis for the **Services Instances** and include specified **Policies**. **Contract** means the binding legal agreement describing a **Service Instance** and includes all rights and obligations. This comes in addition to the automated digital rights management embedded in every entity's self-description.

Further relevant actors exist outside of the Gaia-X scope in terms of **End-Users** and **Asset Owners**.

Asset Owners, e.g. data owners, describe a natural or legal person, which holds the rights of an **Asset** that will be provided according to Gaia-X regulations by a **Provider** and legally enable its provision.

End-Users use digital offerings of a Gaia-X **Consumer** that are enabled by Gaia-X. The **End-User** uses the **Service Instances** containing **Self-Description** and **Policies**.

gaia-x

3

Federation Services

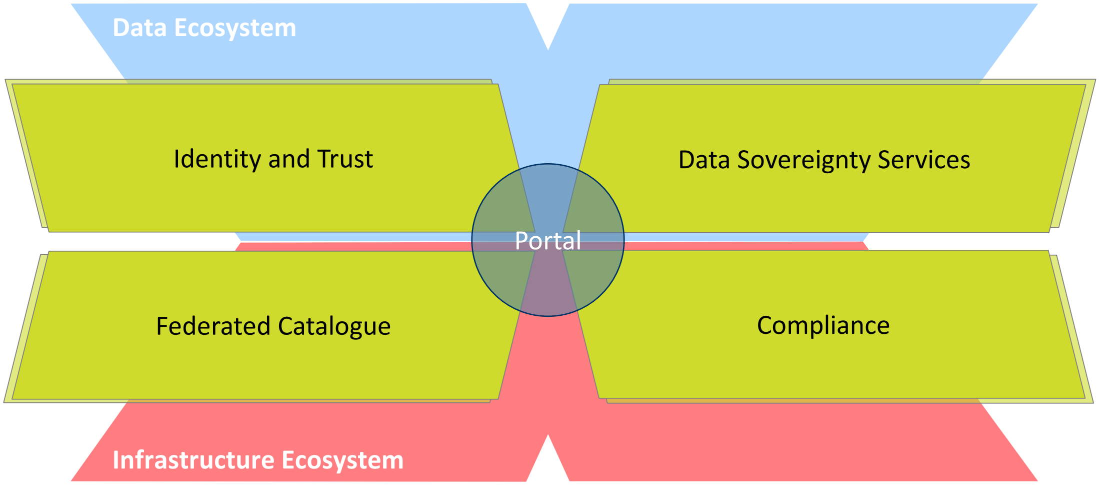
3 Federation Services

The **Federation Services** are necessary to enable a **Federation** of infrastructure and data, provided with open source reference implementation. This will open up technology where applicable, while existing **Certifications** and standards for **Accreditation** will be recognized.

Details about the operationalization of the **Federation Service** will be outlined in the upcoming **Federation Services** documents. Details about the role of **Federation Services** for **Ecosystems** are elaborated in section 5, with an overview shown in Figure 4.

- The **Federated Catalogue** (section 3.1) constitutes the central repository for Gaia-X **Self-Descriptions** to enable the discovery and selection of **Providers** and their **Service Offerings**. The **Self-Description** as expression of properties and **Claims** of **Participants** and **Assets** represents a key element for transparency and trust in Gaia-X.
- **Identity and Trust** (section 3.2) covers authentication and authorization, credential management, decentral **Identity** management as well as the verification of analogue credentials.
- **Data Sovereignty Services** (section 3.3) enable the sovereign data exchange of **Participants** by providing a **Data Agreement Service** and a **Data Logging Service** to enable the enforcement of **Policies**. Further, usage constraints for data exchange can be expressed by Provider Policies as part of the **Self-Description**.
- **Compliance** (section 3.4) includes mechanisms to ensure a **Participant's** adherence to the Policy Rules in areas such as security, privacy transparency and interoperability during onboarding and service delivery.
- **Gaia-X Portals** and API (section 3.5) will support onboarding and **Accreditation** of **Participants**, demonstrate service discovery, orchestration and provisioning of sample services.

Figure 4: Gaia-X Federation Services and Portal as covered in the Architecture Document



3.1 Federated Catalogue

Self-Descriptions intended for public usage can be published in a **Catalogue** where they can be found by potential **Consumers**. The **Providers** decide in a self-sovereign manner which information they want to make public in a **Catalogue** and which information they only want to share privately. The goal of **Catalogues** is to enable **Consumers** to find best-matching offerings and to monitor for relevant changes of the offerings.

A **Catalogue** contains two types of storage: The Self-Description Storage for the published Self-Description files and the **Self-Description Graph**. By following references between **Self-Descriptions** in the graph, advanced queries across individual **Self-Descriptions** become possible.

The system of **Federated Catalogues** comprises a top-level **Catalogue** operated by the Gaia-X, European Association for Data and Cloud, AISBL as well as **Ecosystem**-specific **Catalogues** (e.g., for the healthcare domain) and even company-internal **Catalogues** with private **Self-Descriptions** to be used only internally. **Self-Descriptions** in a **Catalogue** are either loaded directly into a **Catalogue** or exchanged from another **Catalogue** by an inter-**Catalogue** synchronization interface.

Since **Self-Descriptions** are protected by cryptographic signatures, they are immutable and cannot be changed once published. The lifecycle state of a **Self-Description** is described in additional metadata. There are four possible states for the **Self-Description** lifecycle. The default state is "active". The other states are terminal, i.e., no further state transitions follow upon them:

- Active
- End-of-Life (after a timeout date, e.g., the expiry of a cryptographic signature)
- Deprecated (by a newer **Self-Description**)
- Revoked (by the original issuer or a trusted party, e.g., because it contained wrong or fraudulent information)

The **Catalogues** provide access to the raw **Self-Descriptions** that are currently loaded including the lifecycle metadata. This allows **Consumers** to verify the **Self-Descriptions** and the cryptographic proofs contained in them in a self-sovereign manner.

The **Self-Description Graph** contains the information imported from the **Self-Descriptions** that are known to a **Catalogue** and in an "active" lifecycle state. The **Self-Description Graph** allows for complex queries across **Self-Descriptions**.

To present search results objectively and without discrimination, compliant **Catalogues** use a graph query language with no internal ranking of results: Besides the user-defined query statements with explicit filter- and sort-criteria, results are ordered randomly. The random seed for the search results can be set on a per-session basis so that the query results are repeatable within a session with a **Catalogue**.

In a private **Catalogue**, the authentication information can be used to allow a user to upload new **Self-Descriptions** and / or change the lifecycle state of existing ones. In a public **Catalogue**, the cryptographic signatures of the **Self-Descriptions** are checked if its issuer is the owner of its subject. If that is the case, the **Self-Description** is accepted by the **Catalogue**. Hence, **Self-Descriptions** can be communicated to the **Catalogue** by third parties, as the trust verification is independent from the distribution mechanism. **Self-Descriptions** can be marked by the issuer as "non-public" to prevent them from being copied public **Catalogue** by a third-party that received the **Self-Description** JSON-LD file over a private channel.

A **Visitor** is an anonymous user accessing a **Catalogue** without a known account for session. Every **Non-Visitor** user (see Principal in section 3.2) interacts with a **Catalogue** REST API in the context of a session. Another option to interact with a **Catalogue** is to use a GUI frontend (e.g. a **Gaia-X Portal** or a custom GUI implementation) that uses a **Catalogue** REST API in the background. The interaction between a **Catalogue** and its GUI frontend is based on an authenticated session for the individual user of the GUI frontend.

Self-Description

Gaia-X **Self-Descriptions** express characteristics of **Assets, Resources, Service Offerings** and **Participants** are tied to their respective **Identifier**. **Providers** are responsible for the creation of their **Asset's** or **Resource's Self-Description**. In addition to self-declared **Claims** made by **Participants** about themselves or about the **Service Offering** provided by them, a **Self-Description** may comprise **Credentials** issued and signed by trusted parties. Such **Credentials** include **Claims** about the **Provider** or **Asset / Resource**, which have been asserted by the issuer.

Self-Descriptions in combination with trustworthy verification mechanisms empower **Participants** in their decision-making process. Specifically, **Self-Descriptions** can be used for:

- Discovery and composition of **Service Offerings** in a **Catalogue**
- Tool-assisted evaluation, selection, integration and orchestration of **Service Instances** comprising **Assets** and **Resources**
- Enforcement, continuous validation and trust monitoring together with **Usage Policies**
- Negotiation of contractual terms concerning **Assets** and **Resources** of a **Service Offering** and **Participants**

Self-Descriptions are characterized by the following properties:

- Machine-readable and machine-interpretable
- Technology-agnostic
- Adhering to a generalized schema with an expressive semantics and validation rules
- Interoperable, following standards in terms of format, structure, and included expressions (semantics)
- Flexible, extensible and future-proof in that new properties can be added
- Navigable and can be referenced from anywhere in a unique, decentralised fashion
- Accompanied by statements of proof (e.g., certificates and signatures), making them trustworthy by providing cryptographically secure verifiable information

A possible exchange format for **Self-Descriptions** can be the JSON-LD format. JSON-LD uses JSON encoding to represent subject-predicate-object triples according to the W3C Resource Description Framework (RDF).

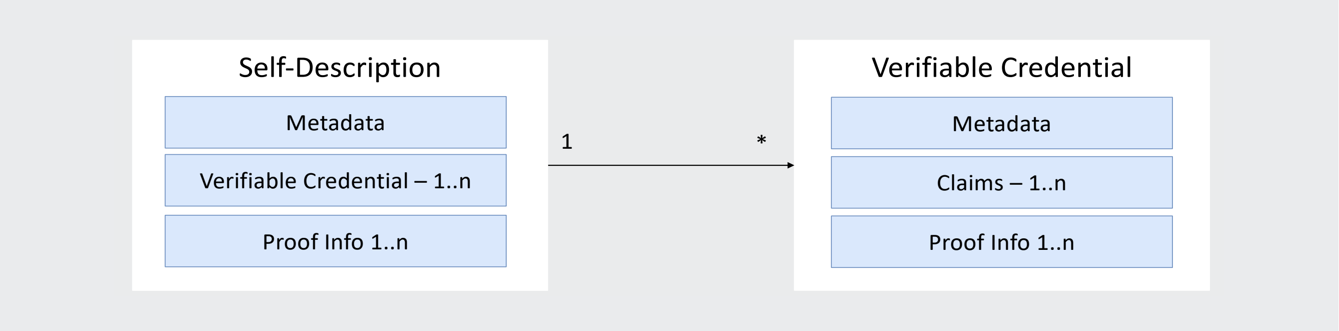
The **Self-Description** of one entity may refer to another entity by its **Identifier**. These relations form a graph with typed edges, which is called the **Self-Description Graph**. The **Catalogues** implement a query algorithm on top of the **Self-Description Graph**. Furthermore, **Certification** aspects and **Usage Policies** can be expressed and checked based on the **Self-Description Graph** that cannot be gained from individual **Self-Descriptions**. For example, a **Consumer** could use C**atalogue Services** to require that a **Service Instance** cannot depend on other **Service Instances** that are deployed on **Nodes** outside a **Consumer**-specified list of acceptable countries.

A **Self-Description** contains the **Identifier** of the **Asset, Resource** or **Participant**, metadata and one or more **Credentials** as shown in Figure 5. A **Credential** contains one or more **Claims**, comprised of subjects, properties and values. The metadata of each **Credential** includes issuing timestamps, expiry dates, issuer references and so forth. Each **Credential** can have a cryptographic signature, wherein trusted parties confirm the contained **Claims. Claims** may follow the same subject-property-object structure of the data model. The W3C Verifiable Credentials Data Model[11] is a possible technical standard to express **Credentials** and **Claims** on top of JSON-LD[12].

[11] W3C. Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web [W3C Recommendation 19 November 2019]. https://www.w3.org/TR/vc-data-model/

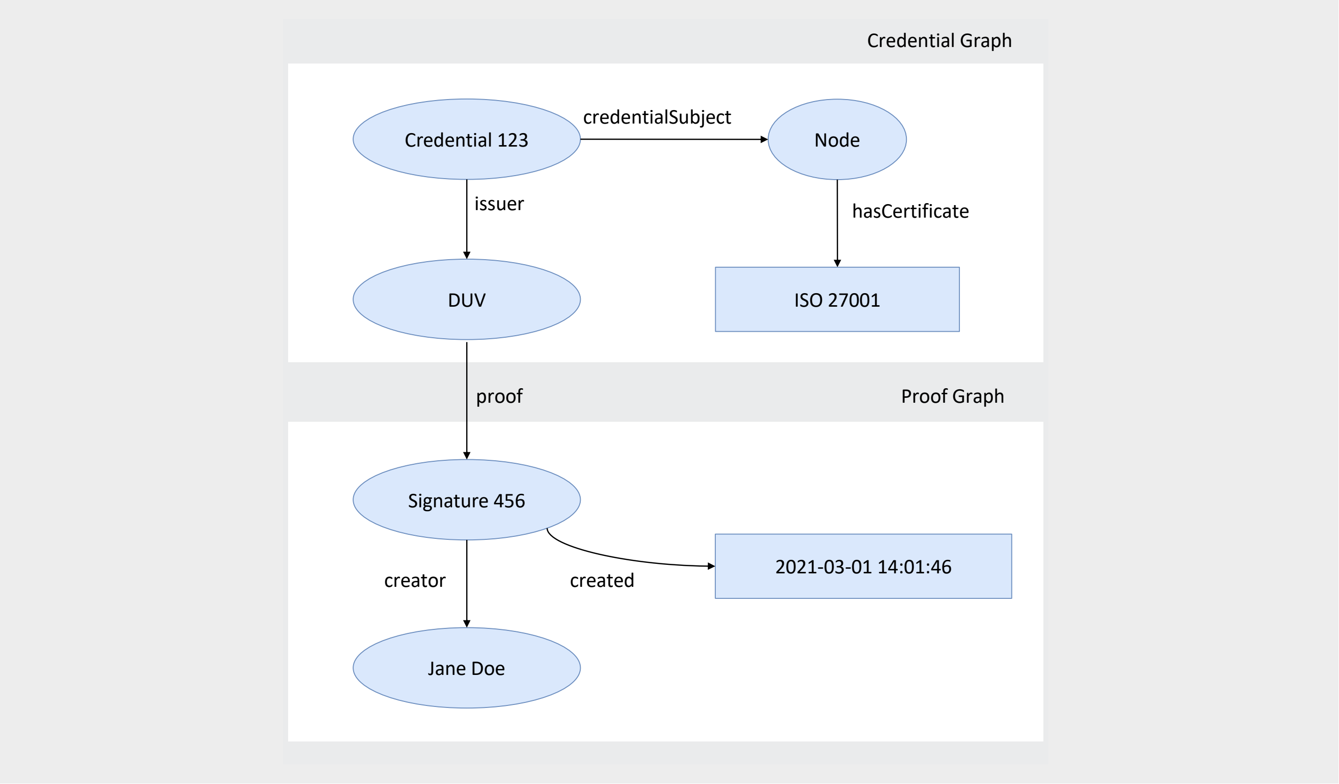
[12] W3C. JSON-LD 1.1: A JSON-based Serialization for Linked Data [W3C Recommendation 16 July 2020]. https://www.w3.org/TR/json-ld11/

Figure 5: Self-Description assembly model



The generic data model for **Claims** is powerful and can be used to express a large variety of statements. Individual **Claims** can be merged together to express a graph of information about an **Asset / Resource** (subject). For example, a **Node** complying with ISO 27001 is shown in Figure 6.

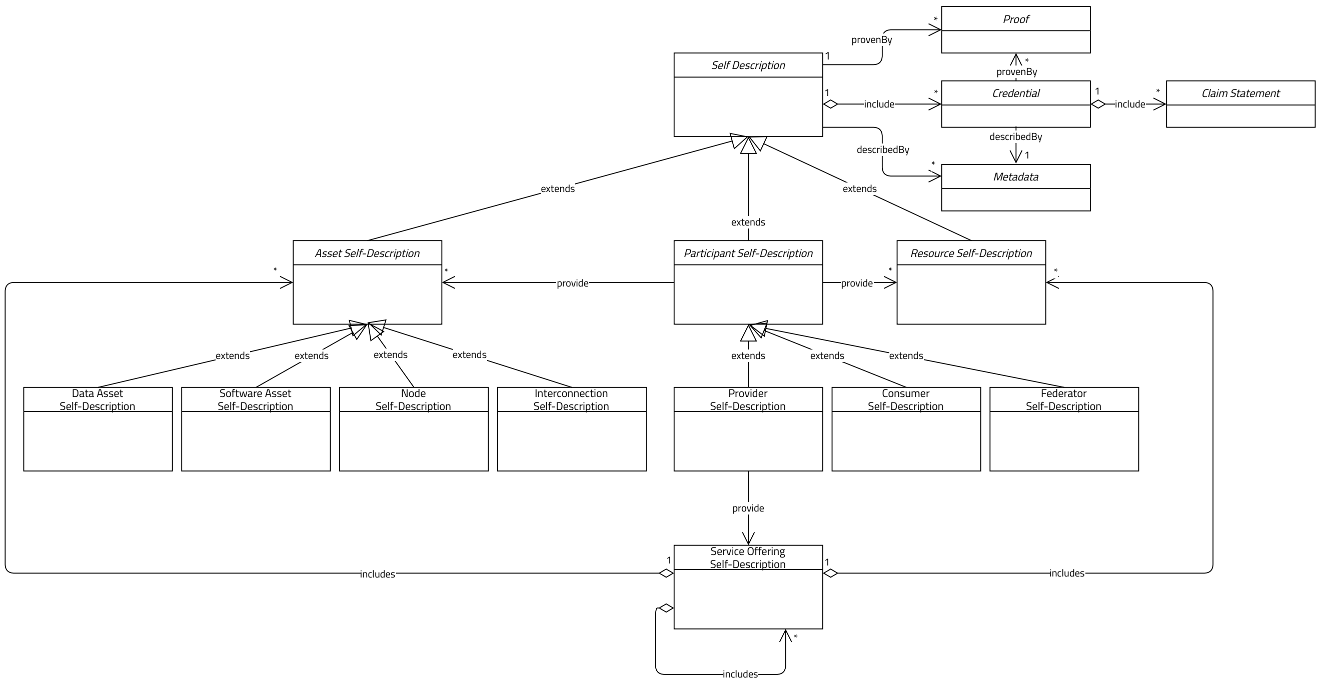
Figure 6: Linked Claim statements as a graph representation



To foster interoperability, **Self-Description** schemas with optional and mandatory properties and relations are defined. A **Self-Description** has to state which schemas are used in its metadata. Only properties and relations defined in these schemas must be used. A **Self-Description** schema corresponds to a class in RDF. The **Self-Description** schemas form an extensible class hierarchy with inheritance of properties and relations.

The **Federation Services** specification describes how core **Self-Description** schemas based on the conceptual model are created and maintained. Individual **Ecosystems** can extend the schema hierarchy for their application domain[13]. Such extensions must make an explicit reference to the organization that is responsible for the development and maintenance of the extension.

Figure 7: Schematic inheritance relations and properties for the top-level Self-Description


Proof
provenBy
*
1
Self Description
provenBy
Credential
include
Claim Statement
include
describedBy
describedBy
Metadata
extends
extends
extends
Asset Self-Description
Participant Self-Description
Resource Self-Description
provide
provide
extends
Data Asset Self-Description
Software Asset Self-Description
Node Self-Description
Interconnection Self-Description
Provider Self-Description
Consumer Self-Description
Federator Self-Description
provide
Service Offering Self-Description
includes
includes
includes

The **Self-Description** schemas can follow the Linked Data best practices[14] making the W3C Semantic Web family[15] a possible standard to be built upon to enable broad adoption and tooling.

Gaia-X aims at building upon existing schemas, preferably such that have been standardized or at least widely adopted[16] to get a common understanding of the meaning and purpose of any property and **Claim** statement. Examples of attribute categories per **Self-Description** in Gaia-X are discussed in Appendix A1.

3.2 Identity and Trust

Identities, which are used to gain access to the **Ecosystem**, rely on unique **Identifiers** and a list of attributes. Gaia-X uses existing identities and does not maintain them directly. Uniqueness is ensured by a specific **Identifier** format relying on properties of existing protocols. Trust – confidence in the **Identity** and capabilities of a **Participant, Asset** or **Resource** – is established by cryptographically verifying **Identities** using the Federated Trust Model of Gaia-X, which is a component that guarantees **Identity** proofing of the involved **Participants**

[13] This is in analogy to, e.g., how DCAT-AP specifies the application of DCAT for data portals in Europe; European Commission Semantic Interoperability Community. DCAT Application Profile for data portals in Europe. https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/dcat-application-profile-data-portals-europe

[14] Berners-Lee, T. (2009). Linked Data. W3C. https://www.w3.org/DesignIssues/LinkedData

[15] W3C. (2015). Semantic Web. https://www.w3.org/standards/semanticweb/

[16] Examples include the W3C Organization Ontology (https://www.w3.org/TR/vocab-org/), the community-maintained schema.org vocabulary (https://schema.org/), the W3C Data Catalog Vocabulary DCAT (https://www.w3.org/TR/vocab-dcat-2/), the W3C Open Digital Rights Language (https://www.w3.org/TR/odrl-model/), and the International Data Spaces Information Model (https://w3id.org/idsa/core)

to make sure that Gaia-X **Participants** are who they claim to be. In the context of **Identity and Trust**, the natural person or a digital representation, which acts on behalf of a **Participant** is referred to as **Principal**. As **Participants** need to trust other **Participants** and **Service Offerings** provided, it is important that the Gaia-X Federated Trust Model provides transparency for everyone. Therefore, proper lifecycle management is required, covering **Identity** onboarding, maintaining, and offboarding. Table 1 shows the Participant Lifecycle Process.

Table 1: Participant Lifecycle Process

Lifecycle Activity	Description
Onboarding	The governing body of a Gaia-X **Ecosystem** validates and signs the **Self-Description** provided by a **Visitor** (the future **Participant / Principal**).
Maintaining	Trust related changes to the **Self-Descriptions** are recorded in a new version and validated and signed by the governing body of a Gaia-X **Ecosystem**. This includes both information controlled by the **Participant / Principal**.
Offboarding	The offboarding process of a **Participant** is time-constrained and involves all dependent **Participants / Principals**.

An **Identity** is composed of a unique **Identifier** and an attribute or set of attributes that uniquely describe an entity (**Participant / Asset**) within a given context. Attributes will be derived from existing identities as shown in the IAM Framework[17].

A secure **Identifier** for an **Identity** will be assigned by the issuer in a cryptographically secure manner. In addition, the process of identifying the holder of an **Identity** is transparent. Furthermore, it is traceable since when the **Identifier** exists in this form, whether it is regularly checked and according to which policy this is done. It must also be possible to revoke issued **Identity** attributes[18].

Trust Framework

Gaia-X defines a trust framework on established standards and EU regulation. The Trust Framework solution supports the privacy and self-sovereign requirements and gains the chain of trust without the need of a global and traceable unique ID across the **Ecosystem**.

Trust in Gaia-X is established by technical elements, such as technical components and processes as well as by a fair and transparent governing body.

The Gaia-X AISBL is the main trust anchor. **Participants** trusting AISBL is a prerequisite for a functioning **Ecosystem**. In this sense, Gaia-X can act as a **Federator** (according to section 2). Then, Gaia-X maintains a list of

[17] For a comprehensive view of the current discussion in the broader Gaia-X community, extra documents from the open working packages can be found on the Gaia-X community platform at https://gaia.coyocloud.com/web/public-link/e01b9066-3823-42a7-b10b-9596871059ef/download.

[18] For more on Secure Identities, see Plattform Industrie 4.0: Working Group on the Security of Networked Systems. (2016). Technical Overview: Secure Identities. https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/secure-identities.pdf.

organizations it trusts to carry out tasks like onboarding, **Certifications**, and so forth. **Participants** are free to agree on additional trust providing organizations, for example in certain domains. The EU eIDAS Trusted Lists[19] can also be used as a source for trust service providers and **Conformity Assessment Bodies**.

Self-Descriptions (see section 3.1) play another crucial part in establishing Trust within Gaia-X. In addition to non-trust-related information, which can be updated by the **Participant**, they contain trust-related information such as the organization DID and / or the organization IDM OpenID Connect issuer (which connects to the organization's **Identity System**). The trust-related part is vetted according to Gaia-X **Policy** and electronically signed by a trusted organization. Possible later changes regarding the trust related information have to be approved. Gaia-X in turn maintains a **Self-Description**, which lists its policies and accepted trust providers as mentioned before.

Service Offerings may have different levels of Trust. During service composition, it is determined by the lowest trust state of the **Service Offering** it relies on. The trust state of a **Service Offering** will not affect the trust state of a **Participant**. On the other hand, a **Policy** violation of a **Participant** can result in losing the trust state of its service.

Hybrid Identity and Access Management

The Gaia-X IAM Framework supports two different approaches, the federated **Identity** approach and the decentralized **Identity** approach.

In the federated **Identity** approach, a Principal access a standardized query API, which forwards the login request to the Gaia-X Internal Access Management component (**Gaia-X AM**). The **Gaia-X AM** requests authentication from the preselected Provider **Identity System**. The **Principal** will provide the **Credentials** to the **Identity System**. The **Identity System** validates the inputs and provides attributes to **Gaia-X AM**, which grants / denies access to Gaia-X. Based on the assigned **Principal** roles, specific permissions are granted or not.

In the decentralized **Identity** approach, authentication and authorization in Self Sovereign Identity (SSI) is based on Decentralized Identifiers (DID)[20]. Public key infrastructure is used to verify controllership of a certain DID and Verifiable Credential[21] that in turn contains any kind of third party issued attributes. Those Verified Credentials can be used to make decisions to grant access to certain **Resources** (authorization). Depending on the existing system landscape, it may be necessary to set up a "trusted transformation" point to translate between new SSIs and existing **Identity Systems**. This outsources the issuing and verification of Verifiable Credentials to another component, controlled by an existing **Identity System**.

Gaia-X might need to comply with additional requirements on the type and usage of credential manager applications, e.g. mandatory minimum-security requirements such as Multi Factor Authentication. Server-to-Server Communication plays a crucial role in Gaia-X and the integration of self-sovereignty will be worked out in more detail.

Federated Trust Model

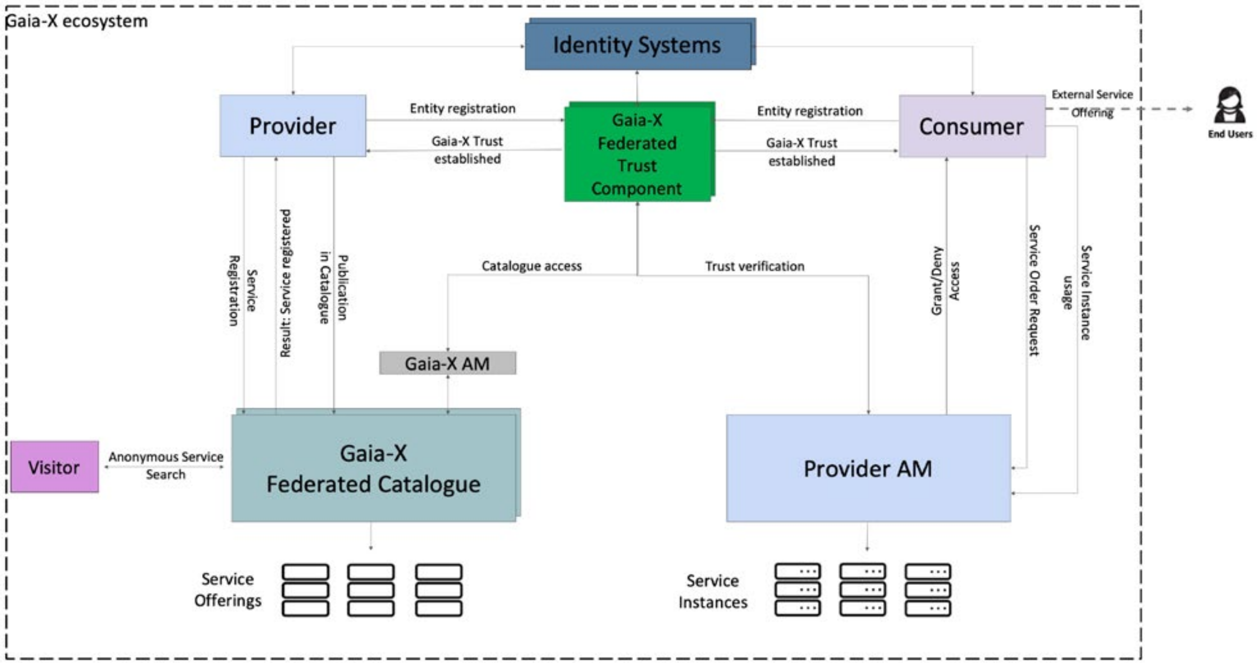
For achieving Trust between identities, the Federated Trust Model is built around the definition of standardized processes and practices, incorporating general accepted policies as well as domain specific policies derived out of private, industrial, governmental and educational sectors.

[19] European Commission. Trusted List Browser: Tool to browse the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL). https://webgate.ec.europa.eu/tl-browser/#/

[20] W3C. (2021). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/

[21] W3C. Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web [W3C Recommendation 19 November 2019]. https://www.w3.org/TR/vc-data-model/

Figure 8: Detailed Level Design of the Gaia-X Federated Trust Model



The Federated Trust Model achieves Trust between **Consumers** and **Providers**. This is realized with the components shown in Figure 8. While the **Federated Trust Component** and the **Federated Catalogue** have been defined before, the Federated Trust Model further involves the **Gaia-X AM**, which is an internal Gaia-X access management component responsible for authorizing Principals' interactions within the **Gaia-X Portals** and the **Provider Access Management** (Provider AM), which the **Provider** will use to grant access for the **Consumer** to **Service Instances**.

Within the federated approach, Identities are built up of verifiable **Claims** and shared on a need to know basis. For an operational example of the Federated Trust Model, see A2.

Access Control

The Access Management covers the internal **Gaia-X AM** and Provider AM. The Provider AM in Gaia-X validates the **Principal** on the **Consumer** side using the **Federated Trust Component**. **End-Users** are handled using existing technology at the **Consumer**. For the **Gaia-X AM**, roles will be needed for Gaia-X **Principals** which can be used for the access control. Examples for such roles could be Gaia-X Administrator, **Participant** Administrator, **Principal**. Roles will be maintained by the Gaia-X AISBL. Clear policies will be in place concerning processes and responsibilities[22].

Gaia-X itself enables fine-grained access control-based attribute evaluation. Attributes will be derived from metadata, **Self-Descriptions** and runtime context (e.g. user **Identity** and associated properties.)

Gaia-X will not implement central access control mechanisms for **Assets** or **Resources**. The responsibility stays with the **Provider**. However, Gaia-X will provide a standardized query API which enables the **Provider** and **Consumer** to query and verify the **Identity** and **Self-Description** of the respective other party.

[22] For details, see chapter 2.1 in Gaia-X IAM Community Working Group. For a comprehensive view of the current discussion in the broader Gaia-X community, extra documents from the open working packages can be found on the Gaia-X community platform at https://gaia.coyocloud.com/web/public-link/e01b9066-3823-42a7-b10b-9596871059ef/download.

3.3 Data Sovereignty Service

Data Sovereignty Services provide **Participants** the capability to be entirely self-determined regarding the exchange and sharing of their data. They can also decide to act without having the **Data Sovereignty Service** involved, if they wish to do so.

Informational self-determination for all **Participants** comprises two aspects within the **Data Ecosystem**: Transparency of data usages and control of data usages. Enabling **Data Sovereignty** when exchanging, sharing and using data relies on fundamental functions and capabilities that are provided by **Federation Services** in conjunction with other mechanisms, concepts, and standards. The **Data Sovereignty Services** build on existing concepts of usage control that extends traditional access control. Thus, usage control is concerned with requirements that pertain to future data usages (i.e., obligations), rather than data access (provisions).

Capabilities for Data Sovereignty Services

The foundation for **Data Sovereignty** is a trust-management mechanism to enable a reliable foundation for peer-to-peer data exchange and usage, but also to enable data value chains with multiple **Providers** and **Consumers** being involved. All functions and capabilities can be extended and configured based on domain-specific or use case-specific requirements in order to form reusable schemes.

The following capabilities are essential for ensuring **Data Sovereignty** in the **Data Ecosystems**:

Table 2: Capabilities for Gaia-X Data Sovereignty Services

Capability	Description
Expression of policies in a machine-readable form	To enable transparency and control of data usages, it is important to have a common policy specification language to express data usage restrictions in a formal and technology-independent manner that is agreed and understood within all Gaia-X **Participants**. Therefore, they have to be formalized and expressed in a common standard, e.g. ODRL[23].
Inclusion of Policies in Self-Description	Informational self-determination and transparency require metadata to describe **Data Assets**, including on **Provider, Consumer,** and **Usage Policies** as provided by **Self-Descriptions** and the **Federated Catalogues** (section 3.1).
Interpretation of Usage Policies	For a **Policy** to be agreed upon, it must be understood by all **Participants** in a way that enables negotiation and possible technical and organizational re-enforcement of **Policies**.
Enforcement	Monitoring data usage is a detective enforcement with subsequent (compensating) actions. In contrast, preventive enforcement[24] ensures the policy **Compliance** with technical means (e.g., cancel or modify data flow).

[23] W3C. ODRL Information Model 2.2 [W3C Recommendation 15 February 2018]. https://www.w3.org/TR/odrl-model/

[24] Currently not in scope of Gaia-X Federation Services

Functions of Data Sovereignty Services

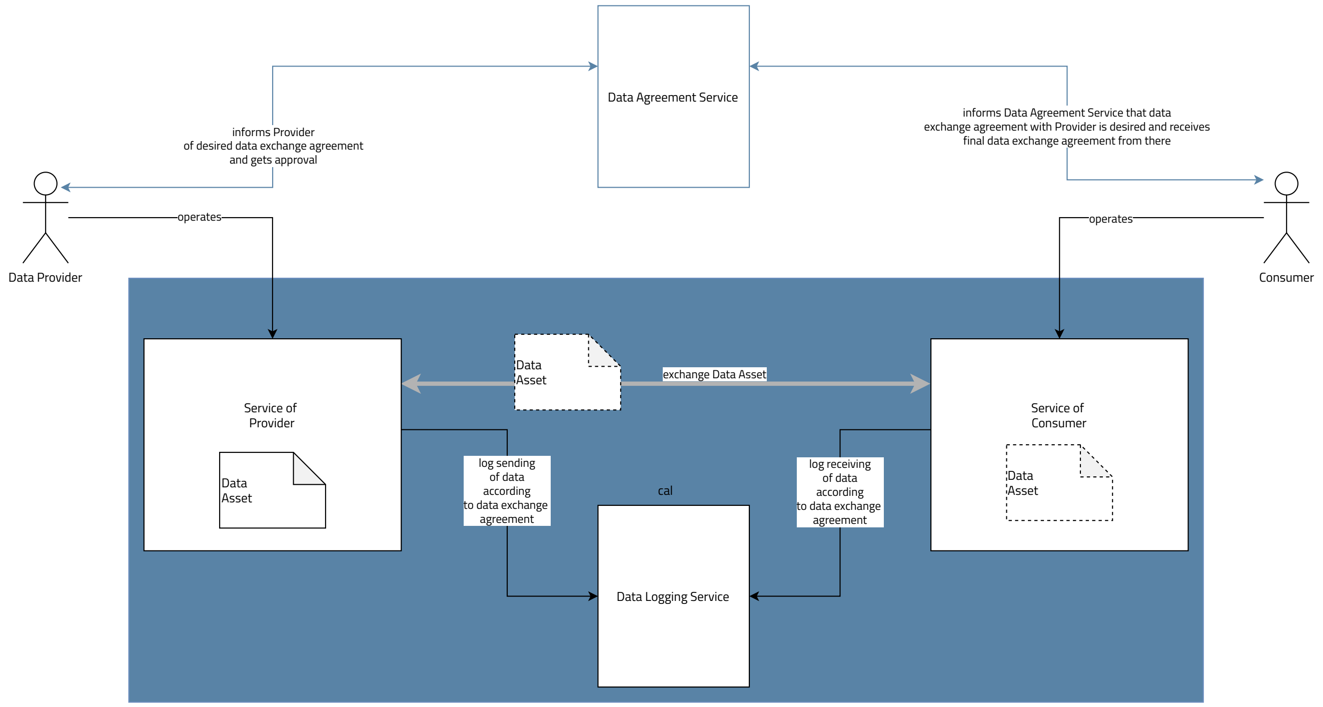
Information services provide more detailed information about the general context of the data usage transaction. All that information on the data exchange and data usage must be traceable, therefore agreed monitoring and logging capabilities are required for all data usages and transactions. Self-determination also means that **Providers** can choose to apply no **Usage Policies** at all.

The **Data Sovereignty Services** in Gaia-X implement different functions for different phases of the data exchange. Therefore, three phases of the data exchange have to be differentiated:

- before transaction
- during transaction
- after transaction

Before the data exchange transaction, the **Data Agreement Service** is triggered and both parties negotiate a data exchange agreement. This includes **Usage Policies** and the required measures to implement those. During the transaction, a **Data Logging Service** receives logging-messages that are useful to trace the transaction. This includes data provided, data received, policy enforced, and policy-violating messages. During and after the transaction the information stored can be queried by the transaction partners and a third eligible party, if required. Figure 9 shows the role of mentioned services to enable sovereign data exchange.

Figure 9: Data Sovereignty Services Big Picture



The **Data Agreement Service** enables data transactions in a secure, trusted, and auditable way. It offers interfaces for the negotiation detailing the agreed terms for planned data exchange. The service is not meant to handle the transaction of data (that is described in the negotiated data contracts).

The **Data Logging Service** provides evidence that data has been (a) submitted, (b) received and (c) that rules and obligations (**Usage Policies**) were enforced or violated. This supports the clearing of operational issues but also fraudulent transactions.

The **Provider** can track if, how, what data was provided, with the **Consumer** being notified about this. The **Consumer** can track if data was received or not, and, additionally, track and provide evidence on the enforcement or violation of **Usage Policies**.

3.4 Compliance

Gaia-X defines a **Compliance** framework that manifests e.g. in the form of a code of conduct, third party **Certifications** / attestations, or acceptance of terms and conditions. It is detailed in the Policy and Rules document. Requirements from the field of security (e.g. data encryption, protection, or interoperability) form the basis for this **Compliance** framework. The main objective of the Federation Service **Compliance** is to provide Gaia-X users with transparency on the **Compliance** of each **Service Offering**.

This **Federation Service** consists of two components: First, the **Onboarding and Accreditation Workflow** (OAW) that ensures that all **Participants, Assets, Resources** and **Service Offerings** undergo a validation process before being added to a **Catalogue**. Second, the Continuous Automated Monitoring (CAM) that enables monitoring of the **Compliance** based on **Self-Descriptions**. This is achieved by automatically interacting with the service-under-test, using standardised protocols and interfaces to retrieve technical evidence. One goal of the OAW is to document the validation process and the generation of an audit trail to guarantee adherence to generally accepted practices in **Conformity Assessment**. Besides the general onboarding workflow, a special focus is set on:

- Monitoring of the **Compliance** relevant basis
- Update of the **Service Offering** that imply re-assurance of **Compliance**
- Suspension of **Service Offerings**
- Revocation of **Service Offerings**.

3.5 Portal and API

The **Gaia-X Portals** support **Participants** to interact with central **Federation Service** functions via a user interface, which provides mechanisms to interact with core capabilities using API calls. The goal is a consistent user experience for all tasks that can be performed with a specific focus on security and **Compliance**. The **Portals** provide information on **Assets, Resources** and **Service Offerings** and interaction mechanisms for tasks related to their maintenance. The functions of the **Portals** are further described below.

A **Portal** supports the registration of organizations as new **Participants**. This process provides the steps to identify and authorize becoming a **Participant**. Additionally, organizations are assisted singing up as members of AISBL. **Participants** are be supported managing **Self-Descriptions** and organizing **Credentials**. This includes **Self-Description** editing and administration. A **Portal** further offers search and filtering of **Service Offerings** and **Participants**, based on **Federated Catalogues**. Additionally, solution packaging refers to a composition mechanism for the selection and combination of **Service Offerings** into solution packages to address specific use cases possible with a **Portal**. To orchestrate the various APIs, an API framework to create a consistent user and developer experience for API access and lifecycle is introduced. An API gateway will ensure security to all integrated services. An API portal will provide a single point of information about available API services and version management.

4

Gaia-X
Participant Use Cases

4 Gaia-X Participant Use Cases

This section illustrates how **Consumers, Federators** and **Provider** described in the conceptual model can interact with each other. Therefore, different actors are considered in the role of **Consumer** and **Provider**. The section focuses on the most typical kinds of actors and the list is not exhaustive.

4.1 Provider Use Cases

This section describes typical kinds of actors that obtain the **Provider** role in Gaia-X. This includes cloud service providers, data providers or providers of **Software Assets** as well as **Interconnection** service providers.

Cloud Service Provider

This section focuses on cloud service providers in the **Provider** role. A possible service model can be an infrastructure (IaaS), platform (PaaS) or software (SaaS) provider. The deployment model explicitly includes private cloud, public cloud, edge and hybrid cloud. As standardization is crucial for achieving interoperability and portability, Gaia-X builds on existing standards. Demanding adherence to certain standards goes along with several challenges for potential **Providers**.

Data Provider

When offering data via Gaia-X, the **Data Sovereignty Services** offer the opportunity to provide **Data Assets** with attached usage control mechanisms. This means that data provisioning and monitoring on the usage of data is given. Furthermore, the **Consumer** can also define **Policies**, which present obligations for the **Provider**. This could, as an example, mean that only data obtained in a certain jurisdiction should be transmitted. The data can be used for different applications and proceedings, including training data for artificial intelligence applications. **Data Sovereignty** technologies provide transparency for the data providers about where their data has been processed and under which conditions.

Software Asset Provider

Gaia-X offers the opportunity to provide **Software Assets** that are data-intensive and use advanced technology approaches, such as artificial intelligence and big data. They can be offered via the **Federated Catalogues** and be provided with certain policies that specify the obligations for the execution of the **Service Instance** of that **Software Asset**, e.g. only in a certain jurisdiction or for a restricted period. **Software Assets** also especially address to Start-Ups or small and medium enterprises. They obtain the opportunity of not only providing their services to a broad mass via Gaia-X under certain **Compliance** regulations and standards, but also having easy access to other complementary services being provided via Gaia-X.

Interconnection Service Provider

In addition to so-called “Best Effort” services, e.g. basic internet connectivity as part of networking between different **Providers**, Gaia-X also provides the possibility to offer more elevated **Interconnection** Services that exhibit special characteristics such as guarantees of bandwidth and latency or security-related settings. Like other **Service Offerings**, **Interconnection Service Offerings** will be listed in a **Catalogue.** Amongst others, **Interconnection** Services will compromise the existing services of internet service providers, internet exchange points, or cloud service providers such as network as a service (NaaS).

4.2 Consumer Use Cases

This section describes different Gaia-X **Consumer** scenarios, where the **Consumer** can obtain different roles. Therefore, the typical role of cloud service consumers, data consumers, **Consumers** of combined services and the **End-Users** of services are described.

Cloud Service Consumer

The consumption of cloud services via Gaia-X, referring to those who follow the Gaia-X standard and **Compliance**, increases transparency for the **Consumer.** It lowers the barrier to adapt different cloud services and reduces the risk of lock-in effects. Gaia-X offers the option for service composition, which also enables the use of cloud-native services. Furthermore, service composition can be used to build a customized service package that covers different aspects and **Providers**, without binding on one single **Provider** only. These aspects will facilitate the adoption of cloud services, especially for small and medium enterprises. They will easily obtain a transparent overview about cloud services following Gaia-X **Policy Rules** and be sure to use trustful services compliant with privacy and security standards. Further, more customized services will appear due to cloud service composition. **Consumers** will keep control over their **Digital Sovereignty** and ensure their trade secrets remain undisclosed.

Data Consumer

A **Consumer** of a **Data Asset** in Gaia-X can be certain that the consumption takes place in a compliant way where transparency about the **Provider** is given. Therefore, the **Self-Description** and **Certification** of the Data Provider creates trust and transparency. Using existing standards for sovereign data sharing enables further trust and builds on established processes. Beyond that, defining search policies enables **Consumers** to set up specific criteria a potential **Provider** needs to fulfil. Gaia-X also eases the processing and offering of resulting products or services, so that it accompanies all following steps in the data value chain. Overall, Gaia-X lowers the entry barriers for **Consumers** of data by creating trust in data offerings. Data-related standards within and across domains make data more accessible and will leverage data sharing also for small and medium enterprises.

Consumer of Combined Service

Gaia-X offers the opportunity to combine different services and create bundles. **Consumers** of these bundles can be sure that all elements are Gaia-X compliant and that there is transparency about each involved actor. **Consumers** can also create service combinations themselves, by selecting suitable building blocks from a **Catalogue**. Here, the **Catalogue** and the **Compliance** levels offer the opportunity to make different building blocks comparable and visible.

Consumer of High-Performance Computing Services

As Gaia-X is open for a broad range of various **Providers** while at the same time being bound to strict **Compliance** rules, it provides the opportunity to address the area of high-performance computing. Especially the **Federation Service** of Identity Management provides benefits for this area: high-performance computing is often used in the academic sector with independent **Identity** federations on a national and international level. These are often not suitable for industrial applications, e.g. in form of consortia. Gaia-X could support such use cases by providing standards for service definitions as well as solutions to ensure interoperable service compositions which fit across sectors. Further, Gaia-X strives for easy access and the general fostering of a collaborative **Ecosystem**, which also benefits all stakeholders of the high-performance computing use cases. The **Federated Catalogues** make the availability of high-performance computing transparent and can enable even small businesses to have low access barriers.

End-User of Data and Cloud Services

The underlying **Compliance** and policy mechanisms enable the trust of **End-Users** in Gaia-X-based end-products or -services. This increases the willingness to use a new service or to expand its application. As Gaia-X refers to the infrastructure and underlying B2B-relations between different actors, the **End-User** will not necessarily recognize that a **Service Instance** is based on Gaia-X. The **End-User** also has not to be a Gaia-X **Participant** or undergo any **Certification** processes.

4.3 Federator Use Cases

Federator of a (domain-)specific Gaia-X Ecosystem

A **Federator** focusing on a domain-specific **Ecosystem** provides the **Federation Services** according to the specific needs of this domain. The **Compliance** to Gaia-X must be fulfilled and **Federation Services** should comply or even base on the open source **Federation Service** software. The domain-specific **Ecosystem** may comprise, for example, domain-specific **Catalogues**, additional trust mechanisms or requirements for data sharing.

Federator of a Gaia-X Ecosystem

A **Ecosystem** is given if all **Federators** comply to Gaia-X and the **Federation Services** fulfil certain criteria (e.g. interoperability verified by a testbed). In this case, any entity has the option to become a **Participant** and participate in such **Ecosystem** activities if they adhere to the Policy Rules.

Federator of an Ecosystem not federated by Gaia-X AISBL

Federators have the option to facilitate an ecosystem by using the available open source **Federation Service** software but being not officially compliant to Gaia-X. An **Ecosystem** may, for example, provide only a private **Catalogue** and set up own criteria for having access to the **Ecosystem**. Despite this kind of **Ecosystem** bases on Gaia-X technology, it cannot be called an official **Gaia-X Ecosystem**.

Gaia-X AISBL in the Federator role

The Gaia-X AISBL may enable and synchronize an **Ecosystem**. As it is not a separate entity in the conceptual model, it takes on the role as **Federator** in this case and has to comply with the Policy Rules and other **Compliance** mechanisms as well as any other **Federator**.

4.4 Basic Interactions of Participants

This section describes the basic interaction of the different **Participants** as described in the conceptual model (see section 2).

Providers and **Consumers** within a **Ecosystem** are identified and well described through their valid **Self-Description**, which is initially created before or during the onboarding process. **Providers** define their **Service Offerings** consisting of **Assets** and Resources by **Self-Descriptions** and publish them in a **Catalogue**. In turn, **Consumers** search for **Service Offerings** in Gaia-X **Catalogues** that are coordinated by **Federators**. Once the **Consumer** finds a matching **Service Offering** in a Gaia-X **Catalogue**, the **Contract** negotiation between **Provider** and **Consumer** determine further conditions under which the **Service Instance** will be provided. The AISBL does not play an intermediary role during the **Contract** negotiations but ensures the trustworthiness of **Participants** and **Service Offerings**.

The following diagram presents the general workflow for a Gaia-X service provisioning and consumption process. Note that this overview represents the current standings and may be subject to changes according to the **Federation Services** specification. The specification will provide more details about the different elements that are part of the concrete processes.

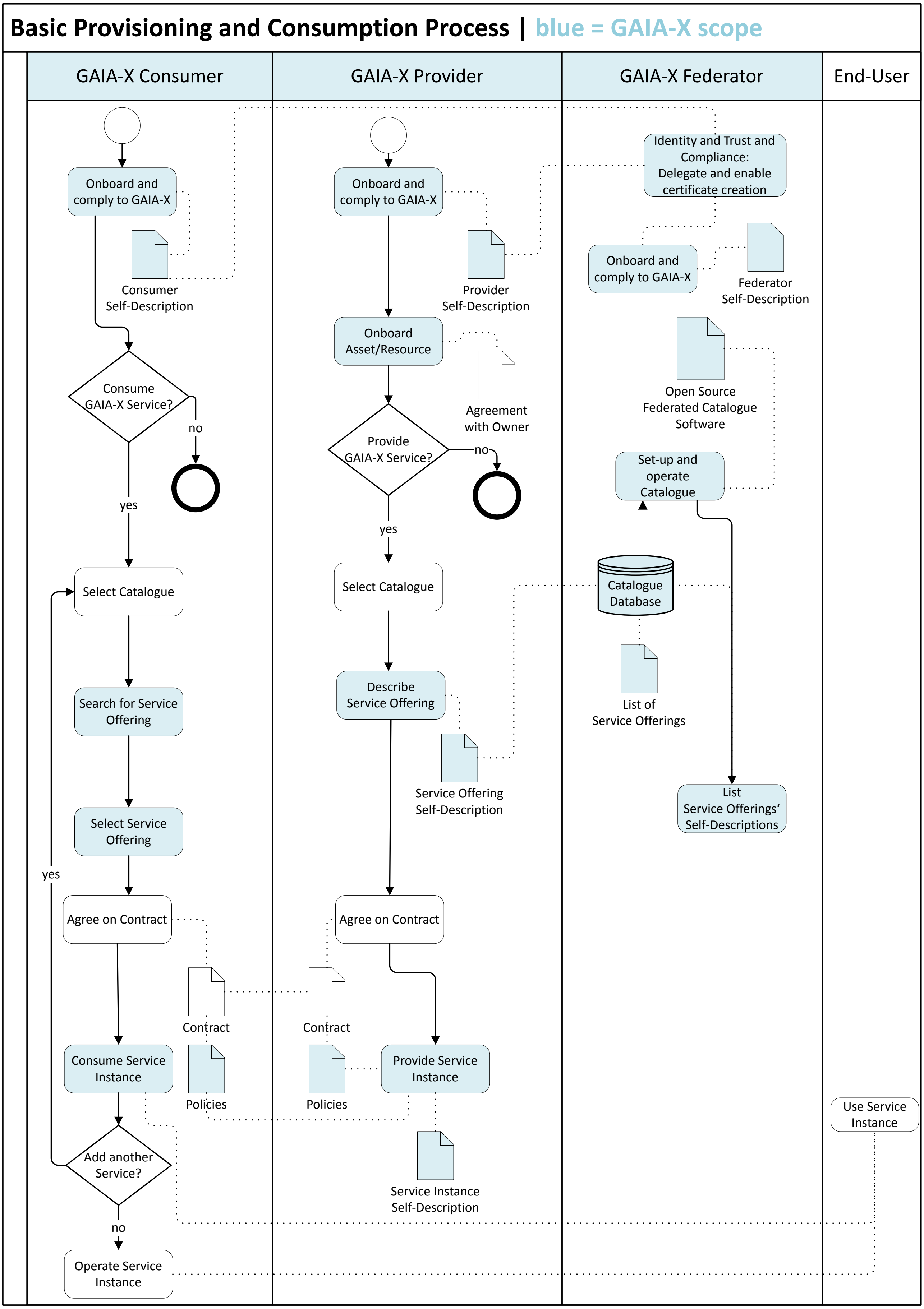
The **Federation Services** are visible in following objects: Data **Sovereignty Services** appear in the mutual agreement and execution of (Usage) Policies that are defined in a **Contract** and stick to the **Data Asset**.

Identity and Trust appears in the onboarding and ensures the unique identification of all **Participants.**

Compliance is also assured during the onboarding and appears as underlying continuous automated monitoring throughout the whole process.

The **Federated Catalogue** and the **Self-Descriptions** are the element that matches the **Consumer** with the **Provider**.

Figure 10: Basic Provisioning and Consumption Process


Basic Provisioning and Consumption Process | blue = GAIA-X scope
GAIA-X Consumer
GAIA-X Provider
GAIA-X Federator
End-User
Onboard and comply to GAIA-X
Consumer Self-Description
Consume GAIA-X Service?
no
yes
Select Catalogue
Search for Service Offering
Select Service Offering
Agree on Contract
Contract
Policies
Consume Service Instance
Add another Service?
yes
no
Operate Service Instance
Onboard and comply to GAIA-X
Provider Self-Description
Onboard Asset/Resource
Agreement with Owner
Provide GAIA-X Service?
no
yes
Select Catalogue
Describe Service Offering
Service Offering Self-Description
Agree on Contract
Contract
Policies
Provide Service Instance
Service Instance Self-Description
Identity and Trust and Compliance: Delegate and enable certificate creation
Onboard and comply to GAIA-X
Federator Self-Description
Open Source Federated Catalogue Software
Set-up and operate Catalogue
Catalogue Database
List of Service Offerings
List Service Offerings' Self-Descriptions
Use Service Instance

5

Gaia-X Ecosystems

5 Gaia-X Ecosystems

5.1 Gaia-X as Enabler for Ecosystems

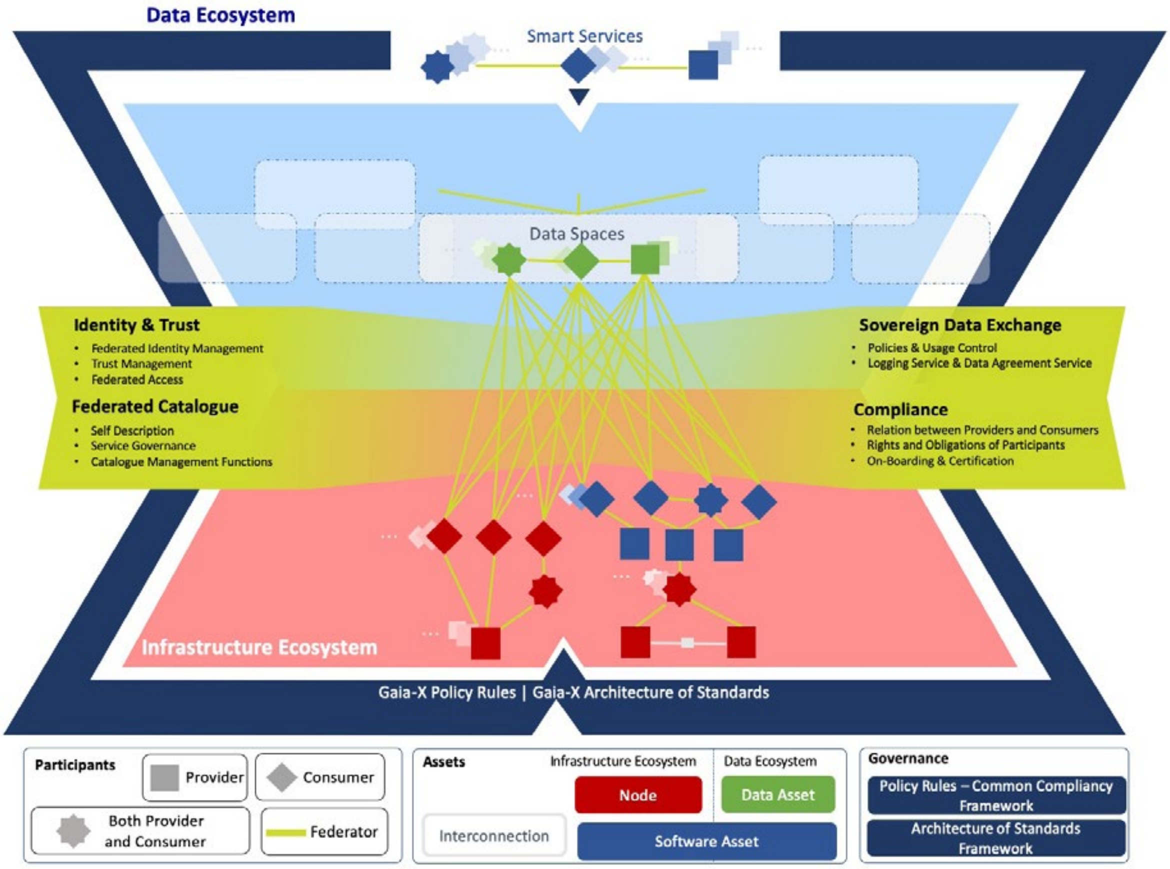
The Gaia-X **Architecture** enables **Ecosystems** and data spaces using the elements explained in the conceptual model (see section 2) in general and the **Federation Services** (section 3) in particular.

An **Ecosystem** is an organizing principle describing the interaction of different actors and their environment as an integrated whole, like in a biological **Ecosystem**. In a technical context, it refers to a set of loosely coupled actors who jointly create an economic community.

Gaia-X proposes a structuring into a data **Ecosystem** and an **Infrastructure Ecosystem**, each with a different focus on exchanged goods and services. Despite each of them has a separate focus, they cannot be viewed separately as they build upon each other.

The **Gaia-X Ecosystem** consists of the entirety of all individual **Ecosystems** that use the **Architecture** and conform to Gaia-X requirements. Several individual **Ecosystems** may exist (e.g. Catena-X) that orchestrate themselves, use the **Architecture** and may or may not use the **Federation Services** open source software.

Figure 11: Gaia-X Ecosystem Visualization

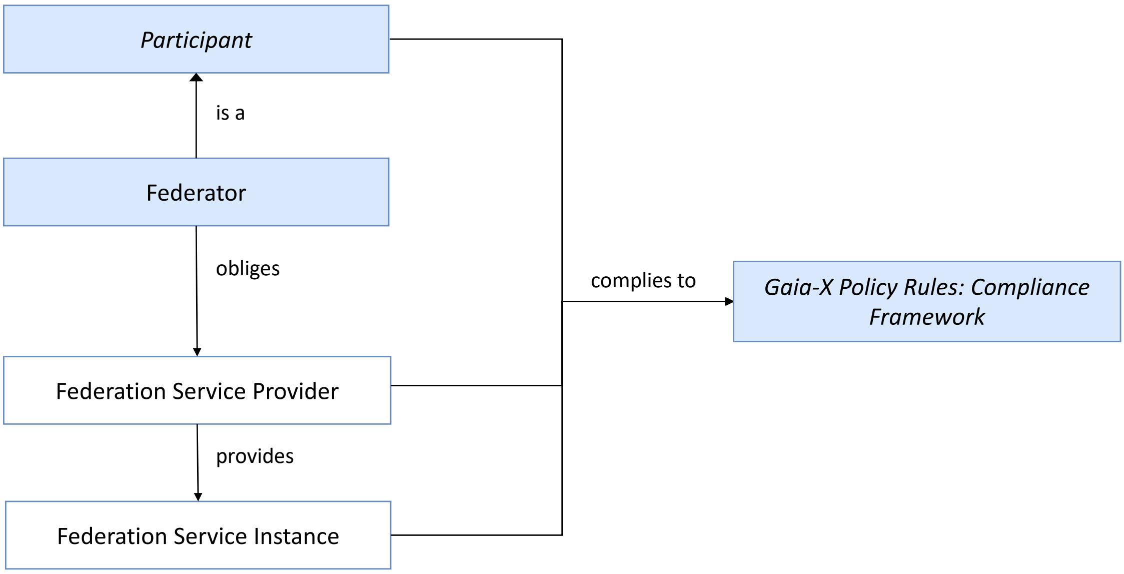

Data Ecosystem
Smart Services
Data Spaces
Identity & Trust
• Federated Identity Management
• Trust Management
• Federated Access
Federated Catalogue
• Self Description
• Service Governance
• Catalogue Management Functions
Sovereign Data Exchange
• Policies & Usage Control
• Logging Service & Data Agreement Service
Compliance
• Relation between Providers and Consumers
• Rights and Obligations of Participants
• On-Boarding & Certification
Infrastructure Ecosystem
Gaia-X Policy Rules | Gaia-X Architecture of Standards
Participants
Provider
Consumer
Both Provider and Consumer
Federator
Assets
Infrastructure Ecosystem
Data Ecosystem
Node
Data Asset
Interconnection
Software Asset
Governance
Policy Rules – Common Compliancy Framework
Architecture of Standards Framework

The basic roles of **Consumer** and **Provider** are visualized as different squares, while the **Federator** appears as connecting element. **Federation Services** are presented as connection between the different elements as well as between the different **Ecosystems**. The star-shaped element visualizes that **Consumers** can act also as **Providers** by offering composed services or processed data again via **Catalogues**. Governance comprises the Policy Rules, which are statements of objectives, rules, practices or regulations governing the activities of **Participants** within the **Ecosystem**. Additionally, the **Architecture of Standards** defines a target for Gaia-X by analysing and integrating already existing standards for data, sovereignty and infrastructure components.

5.2 The Role of Federation Services for Ecosystems

Figure 12 visualizes how the **Federation Service Instances** are related to the **Federator** described in the conceptual model (see section 2.1.2). The **Federators** enable the **Federation Services** by obliging **Federation** Service Providers, which provide the concrete **Federation Service Instances**. The sum of all **Federation Service Instances** form the **Federation Services**.

Figure 12: Federation Services Relations


Participant
is a
Federator
obliges
Federation Service Provider
provides
Federation Service Instance
complies to
Gaia-X Policy Rules: Compliance Framework

Goals of Federation Services

Federation Services aim to enable and facilitate interoperability and portability of **Assets** and **Resources** within Gaia-X-based **Ecosystems** and to provide **Data Sovereignty**. They ensure trust between **Participants,** make **Assets** and **Resources** searchable, discoverable and consumable, and provide means for **Data Sovereignty** in a distributed **Ecosystem** environment.

They do not interfere with the business models of other members in the **Gaia-X Ecosystem**, especially **Providers** and **Consumers**. **Federation Services** are centrally defined while being federated themselves, so that they are set up in a federated manner. In this way, they can be used within individual **Ecosystems** and communities and, through their federation, enable the sharing of data and services across **Ecosystems** or communities as well as the interoperability and portability of data. The set of **Ecosystems** that use the **Federation Services** form the **Ecosystem**.

Nesting and Cascading of Federation Services

Federation Services can be nested and cascaded. Cascading is needed, for example, to ensure uniqueness of identities and **Catalogue** entries across different individual **Ecosystems** / communities that use the **Federation Services**. (Comparable to DNS servers: there are local servers, but information can be pushed up to the root servers).

Therefore, a top-level **Federation Service** is necessary, which will be described in detail in the upcoming Gaia-X **Federation Services** documents.

Ecosystem Governance vs. Management Operations

To enable interoperability, portability and **Data Sovereignty** across different **Ecosystems** and communities, **Federation Services** need to adhere to common standards. These standards (e.g. related to service self-description, digital identities, logging of data sharing transactions, etc.) must be unambiguous and are therefore defined by the Gaia-X AISBL. The Gaia-X AISBL owns the **Compliance** framework and related regulations or governance aspects. Different entities may take on the role of **Federator** and **Federation** Services Provider.

Avoiding Silos

There may be **Ecosystems** that use the open source **Federation Services** but do not go through the **Compliance** and testing required by the Gaia-X AISBL. This does not affect the functionality of the **Federation Services** within the respective **Ecosystem** but would hinder their interaction.

To enable open **Ecosystems** and avoid „siloed" use of **Federation Services**, only those that are compliant, interoperable (and tested) are designated as **Ecosystems**. Therefore, the **Federation Services** act as a connecting element not only between different **Participants**, commodities, but also **Ecosystems** (see above).

The following table presents how the **Federation Services** contribute to the Architecture Requirements that are mentioned in section 1.7.

Table 3: Federation Services match the Architecture Requirements

Requirement	Relation to the Federation Services
Interoperability	- The **Federated Catalogues** ensure **Providers** to offer services along the whole technology stack. The common **Self-Description** scheme also enables interoperability. - A shared **Compliance** framework and the use of existing standards supports the combination and interaction between different **Assets & Resources**. - The **Identity and Trust** mechanisms enable unique identification in a federated, distributed setting. - The possibility to exchange data with full control and enforcement of policies as well as logging options encourages **Participants** to do so. The semantic interoperability enables that data exchange.

Requirement	Relation to the Federation Services
Portability	- The **Federated Catalogues** encourage **Providers** to offer **Assets** and Resources with transparent **Self-Descriptions** and make it possible to find the right kind of service that fits exactly and makes the interaction possible. - The open source implementations of the **Federation Services** provide a common technical basis and enables to move **Assets** and Resource in **Ecosystems** and between different ones. - Common **Compliance** levels and the re-use of existing standards supports portability of data and services.
Sovereignty	- **Identity and Trust** provide the foundation for privacy considerations as well as access and usage rights. Standards for sovereign data exchange enable logging functions and Usage Policies. The **Self-Descriptions** offer the opportunity to specify and attach **Usage Policies** for **Data Assets**.
Security and trust	- The **Architecture** and **Federation Services** provide definitions for trust mechanisms that can be enabled by different entities and enable transparency. - **Sovereign Data Exchange**, as well as **Compliance** concerns address security considerations. The identity and trust mechanisms provide the basis. The **Federated Catalogues** present **Self-Descriptions** and provide transparency over **Service Offerings**.

5.2.1 Infrastructure Ecosystem

The **Infrastructure Ecosystem** has a focus on computing, storage and **Interconnection** elements. Speaking in terms of **Assets** and **Resources**, these elements are addressed as **Nodes, Interconnection** and different **Software Assets**. They range from low-level services like bare metal computing up to high sophisticated offerings, such as high-performance computing. **Interconnection** services ensure secure and performant data exchange between the different **Providers, Consumers** and their services. Gaia-X enables combinations of services that range across multiple **Providers** of the **Ecosystem**.

5.2.2 Data Ecosystem

Gaia-X facilitates **Data Spaces** which present a virtual data integration concept, where data are made available in a decentralised manner, for example, to combine and share data of different cloud storages. **Data Spaces** form the foundation of **Data Ecosystems**. In general, **Data Ecosystems** enable **Participants** to leverage data as a strategic resource in an inter-organizational network without restrictions on a fixed defined partner or central keystone companies. For data to unfold its full potential, it must be made available in cross-company, cross-industry **Ecosystems**. Therefore, **Data Ecosystem** not only enables the whole data value chain but provides technical means to enable **Data Sovereignty**. Such sovereign data sharing addresses different layers and enables a broad range of business models that would not be possible otherwise. Trust and control mechanisms foster the general amount of data sharing and proliferate the **Ecosystem** growth.

5.2.3 Federation, Distribution, Decentralization and Sharing

The principles of **Federation**, distribution, decentralization and sharing are emphasized in the **Federation Services** as they provide several benefits for the **Ecosystem**:

Table 4: Summary of Federation Services as enabler

Principle	Need for Gaia-X	Implemented in Gaia-X Architecture
Decentralization	Decentralization will ensure Gaia-X is not controlled by the few and strengthens the participation of everyone. It also adds key technological properties like redundancy, and therefore resilience against unavailability and exploitability. Different implementations of this architecture create a diverse **Ecosystem** that can reflect the respective requirements of its Participants. (example: IP address assignment)	The role of **Federators** may be taken by diverse actors. The open source **Federation Services** can be used and changed according to own requirements as long as they are compliant and tested.
Distribution	Distribution fosters the usage of different **Assets** and **Resources** by different **Providers** spread over geographical locations. (Example: Domain Name System)	The **Self-Description** allows to describe every **Asset, Resource** and **Service Offering** in a standardized way and enables to list them in a **Catalogue** and assign a unique **Identifier**. Therefore, it enables to handle the de-facto distribution of commodities.
Federation	**Federation** technically enables connections and a web of trust between different parts of the **Ecosystem**. It addresses the following challenges: - Decentralized processing locations - Multiple actors and stakeholders - Multiple technology stacks - Special policy requirements or regulated markets (Example: Autonomous Systems)	Each system can interact with each other, e.g. the **Catalogues** could exchange information and the **Identity** remains unique. Further, different **Conformity Assessment Bodies** may exist.
Sharing	Sharing of the relevant services and components and contributes to the **Ecosystem** development. Sharing of **Assets** and **Resources** across the **Gaia-X Ecosystem** enables spillovers and opens up various economic growth opportunities.	The **Federated Catalogues** enable the matching between **Provider** and **Consumer**. **Sovereign Data Exchange** lowers hurdles for data exchange and **Ecosystem** creation.

By utilizing common specifications and standards, harmonized rules and policies Gaia-X is aligned with specifications like NIST Cloud Federation Reference Architecture[25]:

- Security and collaboration context are not owned by a single entity
- **Participants** in the Gaia-X AISBL jointly agree upon the common goals and governance of the Gaia-X AISBL
- **Participants** can selectively make some of their **Assets** and **Resources** discoverable and accessible by other **Participants** in **Compliance** with Gaia-X
- **Providers** can restrict their discovery and disclose certain information but might lose the Gaia-X **Compliance** level

5.3 Interoperability and Portability for Infrastructure and Data

For the success of a federated **Ecosystem** it is of importance that data, services and the underlying technology can interact seamlessly with each other. Therefore, portability and interoperability are two key requirements for the success of Gaia-X as they are the cornerstones for a working platform and ensure a functional federated, multi-provider environment.

Interoperability is defined as the ability of several systems or services to exchange information and to use the exchanged information mutually. Portability refers to the enablement of data transfer and processing to increase the usefulness of data as a strategic resource. For services, portability implies that they can be migrated from one provider to another, while the migration should be possible without significant changes and adaptations and have a similar QoS.

Areas of Interoperability and Portability

The **Gaia-X Ecosystem** includes a huge variety of **Participants** and **Service Offerings**. Therefore, interoperability needs to be ensured on different levels (Infrastructure services, platform as a service, software as a service, data, and others).

Regarding interoperability of data, core elements to be identified in this endeavour are API specifications and best practices for semantic data descriptions. The use of semantic interoperability is seen as a foundation to eventually create a clear mapping between domain-specific approaches based on a community process and open source efforts.

5.4 Infrastructure and Interconnection

To best accommodate the wide variety of **Service Offerings**, the Gaia-X Architecture is based on the notion of a sovereign and flexible **Interconnection** of networks and **Data Ecosystems**, where data may be flexibly exchanged between different **Participants**. Therefore, **Interconnection** presents a dedicated category of **Assets** as described in section 2.

There is a strong need for **Interconnection** of the different **Nodes** in Gaia-X. It supports the federation of the **Infrastructure Ecosystem**, which in turn builds the basis for the **Data Ecosystem**. Due to the different needs of the **Consumers** and **Providers** as well as due to the highly heterogeneous architectures, different requirements arise for those **Interconnections**.

The Support of Interconnection and Networking Services

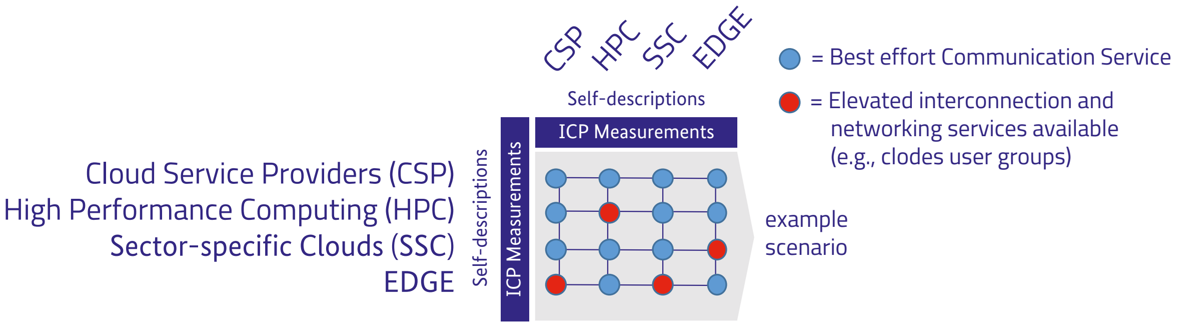
A high-level overview, which outlines the needs of the use cases in Gaia-X with respect to **Interconnection** and networking services is shown in Figure 13[26].

[25] Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST Cloud Federation Reference Architecture: Special Publication (NIST SP) - 500-332. NIST Pubs. https://doi.org/10.6028/NIST.SP.500-332

[26] For a comprehensive view of the current discussion in the broader Gaia-X community, extra documents from the open working packages can be found on the Gaia-X community platform at https://gaia.coyocloud.com/web/public-link/e01b9066-3823-42a7-b10b-9596871059ef/download.

Such a perspective enables a differentiated service capability between “Best Effort” services, e.g., basic Internet connectivity, and more elevated services, which can be provided by dedicated **Interconnection** and networking services. Consequently, and as explained in section 4.1, the **Federated Catalogues** must be extended with adequate networking and **Interconnection** services, considering, for instance, functional and non-functional QoS requirements; portability requirements, etc.

Figure 13: Gaia-X network requirements to use case mapping.


CSP
HPC
SSC
EDGE
Self-descriptions
ICP Measurements
Cloud Service Providers (CSP)
High Performance Computing (HPC)
Sector-specific Clouds (SSC)
EDGE
Self-descriptions
ICP Measurements
example scenario
● = Best effort Communication Service
● = Elevated interconnection and networking services available (e.g., clodes user groups)

Currently, Gaia-X addresses the architectural needs for networking and **Interconnection** via three building blocks: (i) a self-description model, which considers connectivity attributes such as type of networking interface (NIC); supported data rates; latency; (ii) inter-cloud provider (ICP) measurements, describing connectivity between **Nodes / Providers**; (iii) **Interconnection** and networking services based on Internet, QoS attributes and metrics.

Given these three building blocks, the focus is mainly on the **Self-Description** of Gaia-X **Nodes**, where **Interconnection** and networking are addressed via the definition of attributes. The **Self-Descriptions** for the Gaia-X infrastructure currently consider QoS functional parameters relevant for real-time data services, e.g., latency, data rates, bandwidth. Non-functional requirements for supported services need to be defined as well. Therefore, **Self-Description** of **Interconnection** and networking services should not be limited to QoS but also address quality of experience (QoE)-related attributes and consider non-functional requirements, such as security and reliability. A distinct and rich description of these functional and non-functional requirements enables differentiating between the different **Service Offerings** and helps to select the appropriate **Interconnection** and networking service from the **Federated Catalogues**.

Network Service Composition

Networking and **Interconnection** services can be composed via heterogeneous offerings from multiple **Providers** and technologies. To achieve flexibility but also sovereignty and trust, network service composition shall be supported. It is also relevant to consider the capability to describe **Interconnection** and networking services in a flexible way. Such a composition must take existing approaches into consideration and must be as rich as, e.g., composing a slice for verticals, via private and public Clouds[27].

A network service composition framework embeds both functional and non-functional requirements and has the capability to integrate metadata (e.g., in the form of intents) to consider abstract descriptions of the networking service components with their related

[27] For a comprehensive view of the current discussion in the broader Gaia-X community, extra documents from the open working packages can be found on the Gaia-X community platform at https:/gaia.coyocloud.com/web/public-link/e01b9066-3823-42a7-b10b-9596871059ef/download.

requirements. Interface definition languages need to be adopted to enable the composition of functional elements to support network service composition. Furthermore, taking the non-functional aspects for networking services into consideration, the chosen interface definition languages have to be coupled with data modelling languages. This supports the consideration and integration of non-functional elements when composing network services.

In addition to non-constraining interface definition languages and data modelling languages, an overall networking service description framework needs to be used. Examples of available service description frameworks that are relevant to consider in Gaia-X are, for instance, the OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA)[28]. With respect to network service management and orchestration, potential candidates cover but are not limited to the ONF Software Defined Network (SDN) architecture and the ETSI Standards for Network Function Virtualization (ETSI NFV)[29].

A crucial aspect to achieve an adequate network service composition is to integrate support for the intertwining of networking services and application level services. Thus, both semantic and syntactic interoperability need to be ensured. Specifically, an adequate and semantic support for the available and multiple communication protocols is required. This relates to the OSI Layer 2 and 3 communication aspects, but it has also to accommodate additional protocols. Each use case has its own set of building blocks. Therefore, the **Interconnection** services should cover diverse scenarios ranging from a single point-to-point connection to complex multipoint architectures. For example, the open IX-API[30] as well as solutions from the area of Software Defined Networking can be used to flexibly interconnect and configure these architectures, and consider host-reachability and content-oriented developments.

One further important aspect is that **Interconnection** services need to be composed according to customers' requirements and applications being served. Semantic and syntactic interoperability, as stated previously, need therefore to be addressed also by ensuring that the described networking and **Interconnection** services can be adequately associated with **Self-Descriptions**, offered as Gaia-X services, so that they can be looked up in the **Federated Catalogues** and can be used in composing more complex services by Gaia-X users[31].

[28] OASIS (2013). Topology and Orchestration Specification for Cloud Applications Version 1.0. http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html

[29] ETSI. Network Functions Virtualisation (NFV). https://www.etsi.org/technologies/nfv

[30] IX-API. IX-API. https://ix-api.net/

[31] For a comprehensive view of the current discussion in the broader Gaia-X community, extra documents from the open working packages can be found on the Gaia-X community platform at https://gaia.coyocloud.com/web/public-link/e01b9066-3823-42a7-b10b-9596871059ef/download.

Glossary

Name	Definition	Alias / Synonym
Accreditation	Accreditation is the third-party attestation related to a Conformity Assessment Body conveying formal demonstration of its competence to carry out specific Conformity Assessment tasks.	
Architecture of Standards (AoS)	The Architecture of Standards document defines a target for Gaia-X by analysing and integrating already existing standards for data, sovereignty and infrastructure components as well as which standards are supported.	
Architecture Principle	Architecture Principles define the underlying guidelines for the use and deployment of all IT resources and assets across the initiative. They reflect a level of consensus among the various elements of the initiative and form the basis for making future IT decisions.	
Asset	Element used to compose the Service Offering, which does not expose an endpoint.	
Asset Owner	A natural or legal person who is in legal possession of the Asset and can define Policies for the Asset.	
Catalogue	A Catalogue is an instance of the Federation Service Federated Catalogue and present a list of Service Offerings available. Catalogues are the main building blocks for the publication and discovery of a Participant's or Service Offering's Self-Descriptions.	
Certification	The provision by an independent body of written assurance (a certificate) that the Participants, Assets, Resources in question meet specific requirements.	
Claim	An assertion made about a subject within Gaia-X.	
Compliance	Compliance refers to the accordance to Gaia-X Rules.	
Conformity Assessment	Conformity assessment is the demonstration that specified requirements relating to a product, process, service, person, system or body are fulfilled.	
Conformity Assessment Body	Body that performs Conformity Assessment services.	
Consumer	A Consumer is a Participant who consumes Service Instances in the Gaia-X ecosystem to enable digital offerings for End-Users.	
Consumer Policy	A Consumer Policy is a Policy that describes a Consumer's restriction of their requested Assets and Resources.	Search Policy

Name	Definition	Alias / Synonym
Contract	Contract means the binding legal agreement describing a Service Instance and includes all rights and obligations.	
Credential	A set of one or more Claims made and asserted by an issuer.	
Data Asset	Data Asset is a subclass of Asset and consist of data in any form and necessary information for data sharing.	
Data Agreement Service	The Data Agreement Service is a Federation Service of the category Data Sovereignty and considers negotiation of agreements for data exchange.	
Data Ecosystem	A Data Ecosystem is a loose set of interacting actors that directly or indirectly consume, produce, or provide data and other related resources.	
Data Sovereignty	Data Sovereignty can be defined as a natural person's or corporate entity's capability of being entirely self-determined with regard to its data.	
Data Space	A Data Space is a virtual data integration concept defined as a set of participants and a set of relationships among them, where participants provide their data resources and computing services. Data Spaces have following design principles: a) data resides in its sources; b) only semantic integration of data and no common data schema; c) nesting and overlaps are possible; d) spontaneous networking of data, data visiting and coexistence of data are enabled. Within one Data Ecosystem, several Data Spaces can emerge.	
Data Logging Service	The Data Logging Service is a Federation Service of the category Data Sovereignty Service and provides log messages to trace relevant information about the data exchange transaction.	
Data Sovereignty Service	Data Sovereignty Service is a Federation Service.	
Digital Sovereignty	Digital Sovereignty is the power to make decisions about how digital processes, infrastructures and the movement of data are structured, built and managed.	
Ecosystem	An Ecosystem enables value creation by autonomous, loosely coupled actors via both cooperation and competition.	see also Federation
Endpoint	Combination of a binding and a network address.	
End-User	A natural person or process not being Principal, using digital offering from a Consumer. End-Users own an Identity within the Consumer context.	
Federated Catalogue	Federated Catalogue is a Federation Service.	

Name	Definition	Alias / Synonym
Federated Trust Component	A Federation Service component, which ensures trust and trustworthiness between Gaia-X and the interacting Identity System of the Participant. This component guarantees Identity proofing of the involved Participants to make sure that Gaia-X Participants are who they claim to be.	Federated Trust Model
Federation	A Federation refers to a loose set of interacting actors that directly or indirectly consume, produce, or provide Assets and related Resources.	See also: Ecosystem
Federation Services	Federation Services are services required for the operational implementation of a Gaia-X Data Ecosystem.	
Federator	Federators are in charge of the Federation Services and the Federation which are autonomous of each other. Federators are Gaia-X Participants. There can be one or more Federators per type of Federation Service.	
Gaia-X AM	Gaia-X internal Access Management component.	
Gaia-X Ecosystem	The Gaia-X Ecosystem consists of the entirety of all individual ecosystems that use the Gaia-X Architecture and conform to Gaia-X requirements. Several individual ecosystems may exist that orchestrate themselves, use the Gaia-X Architecture and may or may not use the Gaia-X Federation Services open source software.	
Gaia-X Identifier	One unique attribute used to identify an entity within the Gaia-X context and following Gaia-X format.	
Gaia-X Portal	The Gaia-X Portal is a Federation Service to support Participants in interacting with central Federation Service functions via a graphical user interface.	
Identifier	One or more attributes used to identify an entity within a context.	
Identity	An Identity is a representation of an entity (Participant / Asset / Resource) in the form of one or more attributes that allow the entity to be sufficiently distinguished within context. An Identity may have several Identifiers.	
Identity System	An Identity System authenticates / provides additional attributes to the Identity of the Gaia-X Principal and forwards this identity to the requestor. A Gaia-X accredited Identity System follows a hybrid approach and consists of both centralized components, like company identity management systems, and decentralized components like Decentralized Identifiers (DIDs).	

Name	Definition	Alias / Synonym
Identity and Trust	Identity and Trust is a Federation Service.	
Infrastructure Ecosystem	An Infrastructure Ecosystem is a loose set of actors who provide or consume storage, computing and network capacities.	
Interconnection	Interconnection is a subclass of Assets. An Interconnection is a connection between two or multiple Nodes. These Nodes are usually deployed in different infrastructure domains and owned by different stakeholders, such as Consumers and / or Providers. The Interconnection between the Nodes can be seen as a path which exhibits special characteristics, such as latency and bandwidth guarantees, that go beyond the characteristics of a path over the public Internet.	
Node	A Node is a subclass of Assets. A Node represents a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities. A Node can contain other Nodes as sub-nodes so that a hierarchy of Nodes is established.	
Onboarding and Accreditation Workflow (OAW)	The Onboarding and Accreditation workflow is a Federation Service of the category Compliance and is about the initial onboarding and accreditation of Gaia-X Participants.	
Participant	A Participant is an entity as defined in ISO / IEC 24760-1 which is identified, onboarded and has a Gaia-X Self-Description. A Participant can take on one or multiple of the following roles: Provider, Consumer, Federator.	
Policy (legal)	A statement of objectives, rules, practices or regulations governing the activities of people within a certain context. They are placed in the Federation Service of Compliance.	see Policies in Federation Service Compliance
Policy (technical)	Statements, rules or assertions that specify the correct or expected behaviour of an entity. In the conceptual model, they appear as attributes in all elements related to Assets and Resources.	
Principal	A Principal is either a natural person or a digital representation which acts on behalf of a Gaia-X Participant.	
Provider	A Participant who provides Assets and Resources in the Gaia-X ecosystem.	
Provider Access Management (Provider AM)	The Service Ordering Process will involve the Consumer and the Provider. This component is internal to the Provider. The Service Provider will create the Service Instance and will grant access for the Consumer by this component.	Service Provider AM
Resource	Internal, not available for order, Service Instance used to compose the Service Offering, which exposes endpoints.	

Name	Definition	Alias / Synonym
Self-Description	A Self-Description expresses characteristics of an Asset, Resource, Service Offering or Participant and describes properties and Claims while being tied to the Identifier.	
Self-Description Graph	The Self-Description Graph contains the information imported from the Self-Descriptions that are known to the Catalogue and in an "active" lifecycle state.	
Service Instance	Realisation by the Provider of the Service Offering.	
Service Offering	A Service Offering is a set of Assets and Resources, which a Provider bundles into an offering. A Service Offering can be nested with one or more Service Offerings.	
Software Asset	Software Assets are a form of Assets that consist of non-physical functions, like source-code. A running instance of a Software Asset has a PID[32] and is considered to be a Resource.	
Usage Control	Usage Control is a technical mechanism to enforce usage restrictions in form of Usage Policies after access has been granted and is concerned with requirements that pertain to future usages (obligations), rather than (e.g. data) access (provisions).	
Usage Policy	A Usage Policy is a Policy in a technical sense, by which a Provider constraints the Consumer's use of the Assets and Resources offered.	Provider Policy
Visitor	Anonymous, non-registered entity (natural person, bot, ...) browsing a Federated Catalogue.	

[32] The Open Group (2018). The Open Group Base Specifications Issue 7. https://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap03.html#tag_03_300

References

- Berners-Lee, T. (2009). Linked Data. W3C. https://www.w3.org/DesignIssues/LinkedData
- Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST Cloud Federation Reference Architecture: Special Publication (NIST SP) - 500-332. NIST Pubs. https://doi.org/10.6028/NIST.SP.500-332
- ETSI. Network Functions Virtualisation (NFV). https://www.etsi.org/technologies/nfv
- European Commission. Trusted List Browser: Tool to browse the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL). https://webgate.ec.europa.eu/tl-browser/#/
- European Commission. (2020). Towards a next generation cloud for Europe. https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe
- European Commission Semantic Interoperability Community. DCAT Application Profile for data portals in Europe. https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/dcat-application-profile-data-portals-europe
- Federal Ministry for Economic Affairs and Energy. (2019). Project Gaia-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-Gaia-X.htm
- Federal Ministry for Economic Affairs and Energy. (2020). Gaia-X: Technical Architecture: Release - June, 2020. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/Gaia-X-technical-architecture.html
- Gaia-X AISBL. Architecture Decision Record (ADR) Process: GitLab Wiki. https://gitlab.com/Gaia-X/Gaia-X-technical-committee/Gaia-X-core-document-technical-concept-architecture/-/wikis/home
- ISO / IEC. Intelligent transport systems - Using web services (machine-machine delivery) for ITS service delivery (ISO / TR 24097-3:2019(en)). https://www.iso.org/obp/ui/fr/#iso:std:iso:tr:24097:-3:ed-1:v1:en
- ISO / IEC. IT Security and Privacy – A framework for identity management: Part 1: Terminology and concepts (24760-1:2019(en)). ISO / IEC. https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en
- IX-API. IX-API. https://ix-api.net/
- OASIS (2013). Topology and Orchestration Specification for Cloud Applications Version 1.0. http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html
- Oldehoeft, A. E. (1992). Foundations of a security policy for use of the National Research and Educational Network. Gaithersburg, MD. NIST. https://doi.org/10.6028/NIST.IR.4734 https://doi.org/10.6028/NIST.IR.4734
- Open Source Initiative. Licenses & Standards. https://opensource.org/licenses
- Open Source Initiative. The Open Source Definition (Annotated). https://opensource.org/osd-annotated
- Plattform Industrie 4.0: Working Group on the Security of Networked Systems. (2016). Technical Overview: Secure Identities. https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/secure-identities.pdf Singhal, A., Winograd, T., & Scarfone, K. A. (2007). Guide to secure web services: Guide to Secure Web Services - Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD. NIST. https://csrc.nist.gov/publications/detail/sp/800-95/final https://doi.org/10.6028/NIST.SP.800-95
- W3C. JSON-LD 1.1: A JSON-based Serialization for Linked Data [W3C Recommendation 16 July 2020]. https://www.w3.org/TR/json-ld11/
- W3C. ODRL Information Model 2.2 [W3C Recommendation 15 February 2018]. https://www.w3.org/TR/odrl-model/
- W3C. Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web [W3C Recommendation 19 November 2019]. https://www.w3.org/TR/vc-data-model/
- W3C. (2015). Semantic Web. https://www.w3.org/standards/semanticweb/
- W3C. (2021). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/

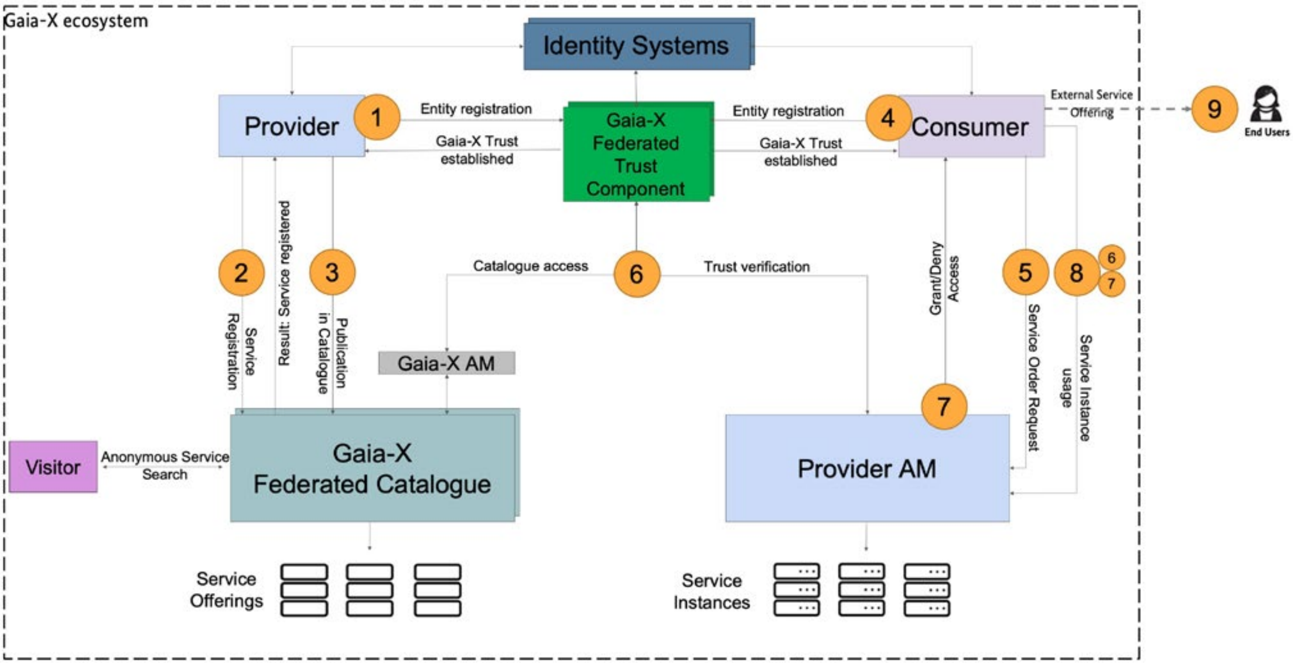
Appendix

A1

Examples of Attribute Categories per **Self-Description** in Gaia-X are discussed in Appendix A.

- **Providers:** Every **Provider** of **Service Offerings** has to be registered as **Provider** and thus requires a **Self-Description**. The categories comprise identity, contact information, **Certification**.
- **Nodes: Self-Descriptions** of **Nodes** describe relevant functional and non-functional attributes of **Nodes** as described in Section "Basic Architecture Elements". The Attribute Categories comprise availability, connectivity, hardware, monitoring, physical security and sustainability.
- **Software Assets: Self-Descriptions** of **Software Assets** describe **Software Assets** as defined in Section 2 (Conceptual Model). Attribute Categories for **Software Assets** are still under discussion and are not yet finalized.
- **Consumers (optional): Self-Descriptions** of **Consumers** are optional, but may be required for accessing critical **Data Assets** and / or specific domains. Attribute categories for **Consumers** are still under discussion and are not yet finalized.

A2



Operational example Federated Trust Model

0. A Visitor accesses the Gaia-X Federated Trust, browses the Gaia-X **Federated Catalogue** and starts a Service search query. A list with possible services matching the service search criteria will be displayed to the Visitor.

1. The **Provider** entity registers in Gaia-X. One of the mandatory fields is the input of the **Identity System**. An **Identity System** must confirm the **Identity** of the **Provider**.

2. Existing **Identifiers** will be enabled for Gaia-X usage. Result: The **Provider** is verified and registered in Gaia-X. The **Provider** is able to register a Service in the Gaia-X **Federated Catalogue**, it is generated during Service **Self-Description** creation. The registered Service will be published to the Gaia-X **Federated Catalogue** and is publicly available.

3. A **Consumer** registers in Gaia-X. One of the mandatory fields is the input of the **Identity System**. An **Identity System** must confirm the **Identity** of the **Consumer** and can be verified itself by Gaia-X. Existing **Identifiers** will be enabled for Gaia-X usage. Result: The **Consumer** is verified and registered in Gaia-X.

4. The registered **Consumer** contacts the Service **Provider** to order a specific Service.

5. The **Provider** AM checks the trustworthiness of the **Consumer**. The Gaia-X **Federated Trust Component** is used to check the **Identity** via the **Identity System**. The Gaia-X **Federated Trust Component** is used to verify the Service Access (e.g. required certifications of the **Consumer** to access health data).

   a. Deny / Grant Access

   b. Deny: The **Provider** AM will provide the result to the **Consumer**.

6. Grant: The **Provider** AM will trigger the service orchestration engine to create the **Service Instance** for the **Consumer** (= Service Instantiation process). The Service **Provider** will forward the **Service Instance** Details to the **Consumer**.

7. The **Consumer** is now able to use the ordered **Service Instance**. The **Provider** AM will check / verify for each access the **Identity** of the **Consumer** using the **Federated Trust Component** to guarantee that the **Consumer** attribute matches the required ones (see step 6 / 7).

8. The **Consumer** can offer – outside of the **Gaia-X Ecosystem** – Services to their **End-Users** (not part of Gaia-X). These external offerings can rely on Gaia-X **Service instances** or can be enriched by data out of Gaia-X Services.