Gaia-X Architecture Document

21.06 Release

Gaia-X European Association for Data and Cloud AISBL

Table of contents

1. Gaia-X Architecture Document

1.1 Publisher

Gaia-X European Association for Data and Cloud AISBL
Avenue des Arts 6-9
1210 Brussels
www.gaia-x.eu

1.2 Authors

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

1.3 Contact

E-mail: architecture-document@gaia-x.eu

1.4 Copyright notice

2. Overview

2.1 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-anchored 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 anong them. It describes how Gaia-X facilitates interconnection, interoperability and integration among all participants in the European digital economy, relative 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: Architecture, Release 21.03 – April 2021.[3].

2.2 Objectives

This document describes the top-level Gaia-X Architecture model. It focuses on conceptual modelling and key considerations of an operating model and is agnostic regarding technology and vendor. In doing so, it aims to represent 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 advancements in the technological state of the art.

2.3 Scope

The Gaia-X Architecture document describes the concepts required to establish the Gaia-X Data and Infrastructure Ecosystem. It integrates the Providers, Consumers, and Services essential 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 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.

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.

2.4 Audience and Use

The Gaia-X Architecture document is directed towards all Gaia-X interests and stakeholder groups, such as Gaia-X Association 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 among them and as a reference for elaboration and specification of the Gaia-X Architecture.

2.5 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. Additional Compliance-relevant information will be outlined in the documents on "Policy Rules" as well as "Architecture of Standards". The Federation Services specification, which is also the basis for the upcoming open source implementation, adds details about the Federation Services functionalities as well as the upcoming test workbench.

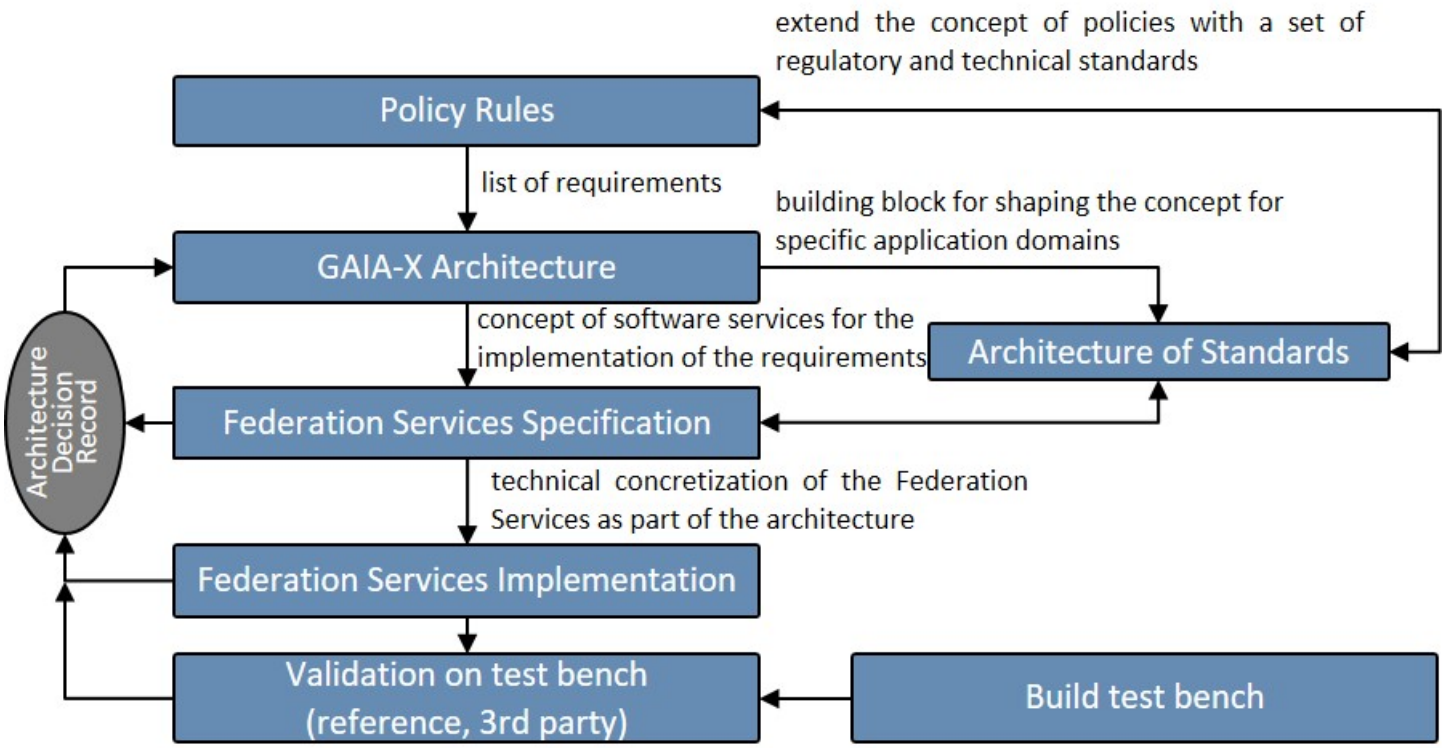


Fig: Relation to other Documents

2.6 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].

2.7 Architecture Requirements

The architecture is used 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 in mutually beneficial ways.
- **Portability of data and services:** Data is described in a standardized 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 follows the EU's data protection provisions and emphasizes a general 'compliance-by-design' and 'continuous-auditability' approach.
- **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.

2.8 Architecture Design Principles

The following design principles[5] underlie the architecture:

Name - Statement - Rationale - Implications

- **Federation:** Federated systems describe autonomous entities, tied together by a specified set of standards, frameworks, and legal rules. The principle balances the need for a minimal set of requirements to enable interoperability and information sharing between and among the different entities while giving them maximum autonomy. The principle defines the orchestrating role of Gaia-X governance elements and implies interoperability within and across Gaia-X Ecosystems.
- **Decentralization:** Decentralization describes how lower-level entities operate locally without centralized control in a self-organized manner. (The federation principle enables this self-organization by providing capabilities for connectivity within a network of autonomously acting Gaia-X Participants.) The principle of decentralization implies individual responsibility for contributions and no control over the components, which fosters scalability.
- **Openness**: The open architecture makes adding, updating, and changing of components easy and allows insights into all parts of the architecture without any proprietary claims. In this way, Gaia-X is open to future innovation and standards and aware of evolving technologies. The documentation and specifications of Gaia-X architectures and technologies are openly available and provide transparency as technology choices will be made to encourage the distribution of collaboratively created artifacts under OSD[6] compliant open source licenses[7].

---

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. https://gaia-x.eu/sites/default/files/2021-05/Gaia-X_Architecture_Document_2103.pdf. ↩
4. Gaia-X European Assocation for Data and Cloud 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. TOGAF 9.2. Components of Architecture Principles. https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap20.html#:~:text=Architecture%20Principles%20define%20the%20underlying,for%20making%20future%20
6. Open Source Initiative. The Open Source Definition (Annotated). https://opensource.org/osd-annotated ↩
7. Open Source Initiative. Licenses & Standards. https://opensource.org/licenses ↩

3. Gaia-X Conceptual Model

The Gaia-X conceptual model, shown in the figure below, describes all concepts in the scope of Gaia-X and relations among them. Supplementary, more detailed models may be created in the future to specify further aspects. Minimum versions of important core concepts in the form of mandatory attributes for Self-Descriptions are presented in Appendix A3. The general interaction pattern is further depicted in section The general interaction pattern is further depicted in section Basic Interactions of Participants.

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.

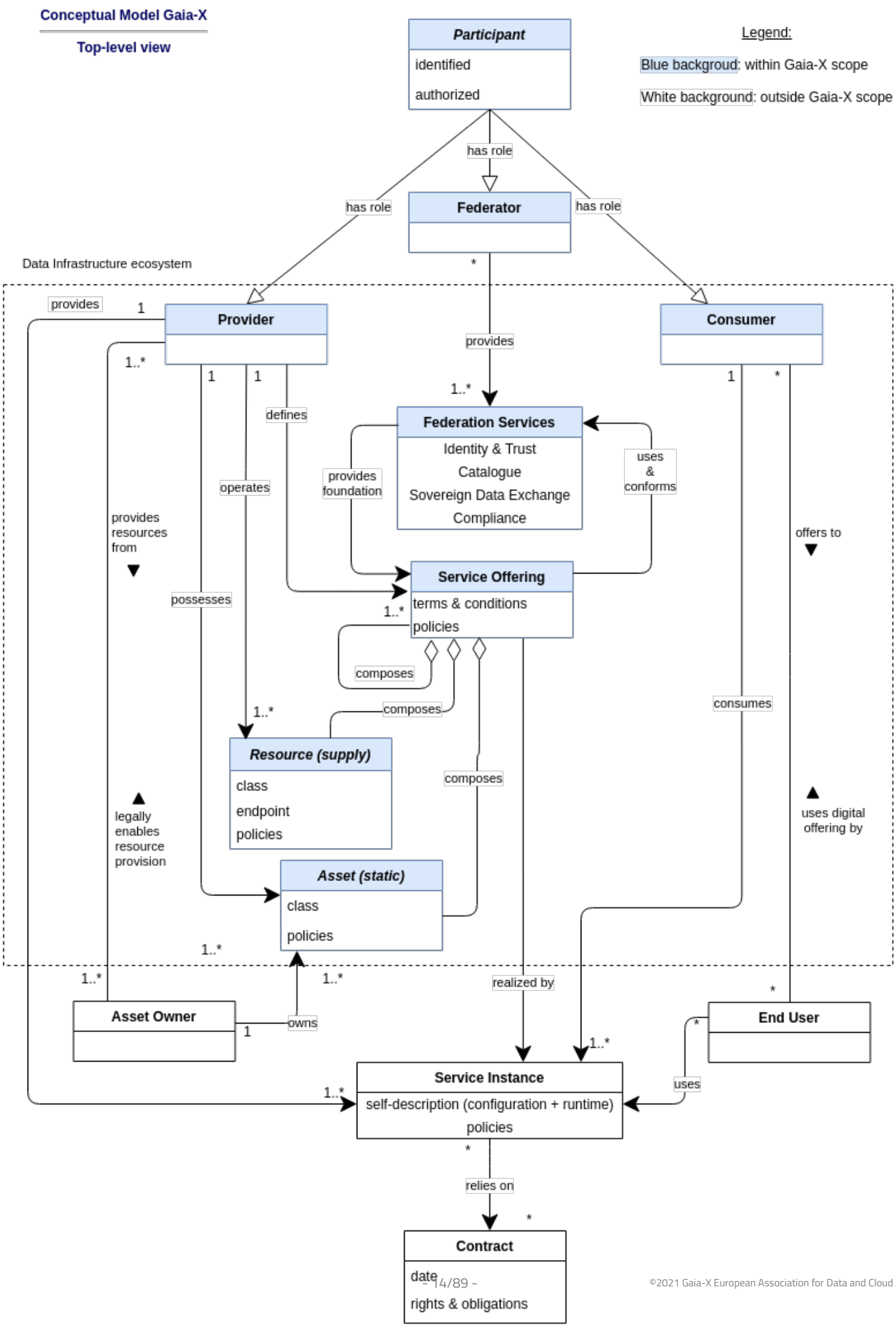


Fig: Gaia-X conceptual model

3.1 Participants

A Participant is an entity, as defined in ISO/IEC 24760-1 as "item relevant for the purpose of operation of a domain that has recognizably distinct existence"[1], which is onboarded and has a Gaia-X Self-Description. A Participant can take on one or more of the following roles: Provider, Consumer, Federator. Section Federation Services 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.

3.1.1 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. Furthermore, it provides the Service Instance that includes a Self-Description and associated Policies. Therefore, the Provider operates different Resources and possesses different Assets.

3.1.2 Federator

Federators are in charge of the Federation Services and the Federation which are independent 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.

3.1.3 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.

3.2 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 Offerings.

An Asset can be a Data Asset, a Software Asset, a Node or an Interconnection Asset. A set of Policies described in a Self-Description is bound to each Asset. The different categories of Assets are visualized in Figure 3 and defined below:

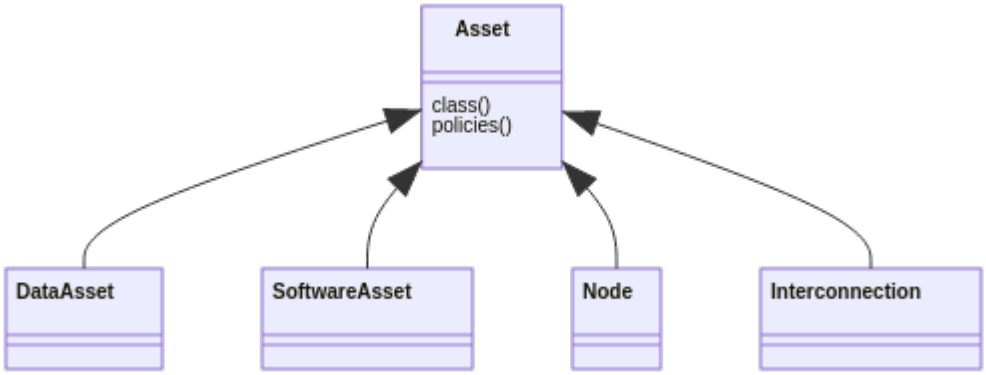


Fig: Asset Categories

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 as an Asset presents the connection between two or more 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, bandwidth and security guarantees, that go beyond the characteristics of a path over the public Internet.

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.

3.2.1 Policies

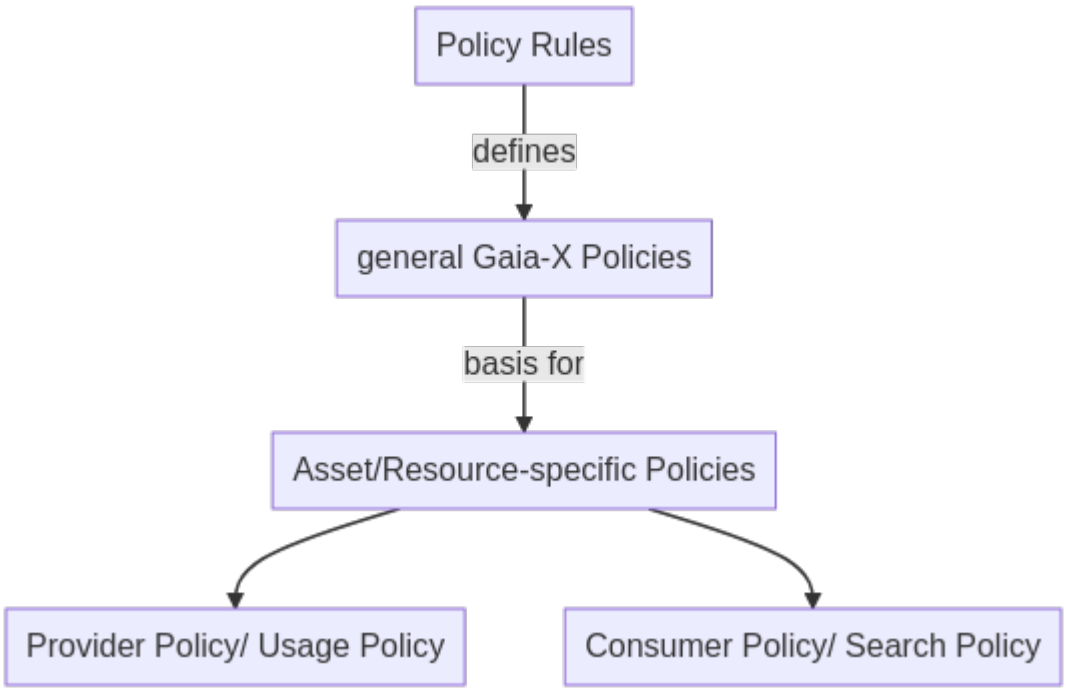
Policy is defined as a statement of objectives, rules, practices, or regulations governing the activities of Participants within Gaia-X. From a technical perspective Policies are statements, rules or assertions that specify the correct or expected behaviour of an entity[23].

The Policy Rules Document explains the general Policies defined by the Gaia-X association for all Providers and Service Offerings. They cover, for example, privacy or cybersecurity policies and are expressed in the conceptual model indirectly via Gaia-X Federation Service Compliance and as attributes of the Assets, Resources, Service Offerings, and Service Instances.

These general Policies form the basis for detailed Policies for a particular Service Offering, which can be defined additionally and contain particular restrictions and obligations defined by the respective Provider or Consumer. They occur either as a Provider Policy (alias Usage Policies) or as a Consumer Policy (alias Search Policy):

- A Provider Policy/Usage Policy constraints the Consumer's use of an Asset or Resource. *For example, a Usage Policy for data can constrain the use of the data by allowing to use it only for x times or for y days.*
- A Consumer Policy describes a Consumer's restrictions of a requested Asset or Resource. *For example, a Consumer gives the restriction that a Provider of a certain service has to fulfil demands such as being located in a particular jurisdiction or fulfil a certain service level.*

In the conceptual model, they appear as attributes in all elements related to Assets and Resources. The specific Policies have to be in line with the general Policies in the Policy Rules Document.



3.3 Federation Services

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

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.

3.4 Service Offering

A Service Offering is defined as a set of Assets and Resources which a Provider aggregates and publishes as a single entry in a Catalogue. Service Offerings may themselves be aggregated realizing service composition. The instantiation of a Service Offering is the deliverable of a Provider to a Consumer. The Federation Services provide the foundation for Service Offerings and the Service Offering uses and conforms to the Federation Services.

3.5 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.

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 such as 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. As Assets are bundled into a Service Offering and nested Asset compositions can be possible, there is no separate resource owner either. Assets and resources can only be realized together in a Service Offering and Service Instance by a Provider, which presents no need to model a separate legal holder of ownership rights.

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.

3.6 Examples

3.6.1 Personal Finance Management example

This example describes the various Gaia-X concepts using the Open Banking scenario of a Personal Finance Management service (PFM) in SaaS mode.

Let's suppose that the service is proposed by a company called `MyPFM` to an end user `Jane` who have bank accounts in two banks: $Bank_1$ and $Bank_2$.
`MyPFM` is using services provided by $Bank_1$ and $Bank_2$ to get the banking transactions of `Jane` and then aggregates these bank statements to create Jane's financial dashboard.

`Jane` is the **End-User**.

$Bank_1$ and $Bank_2$ are **Providers** defining the **Service Offerings** delivering the banking transactions and operating the corresponding **Service Instances**. They are also **Asset Owners** for the bank statements, which are **Assets** composing the **Service Offerings** (`Jane` is the data subject as per GDPR[4]).
The associated **Asset Policies** are in fact predefined by the PSD2[5] directive from the European Parliament.

`MyPFM` is the **Consumer** which consumes the **Service Instances** provided by $Bank_1$ and $Bank_2$ in order to create a financial dashboard and to offer it to `Jane`.
`MyPFM` is also likely consuming **Service Instances** from a PaaS **Provider** in order to run its own code, such as dashboard creation.

---

1. 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 ↩
2. 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 ↩
3. 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 ↩
4. Rights of the data subject https://gdpr-info.eu/chapter-3/ ↩
5. Payment services (PSD 2) https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en ↩

4. Gaia-X Operating Model - Concept

Gaia-X in its unique endeavor must have an operating model enabling a wide adoption from small and medium-sized enterprises up to large organisations, including highly regulated markets, to be sustainable and scalable.

To achieve the above statements, a non-exhaustive list of Critical Success Factors (CSFs) includes:

1. The solution must provide clear and unambiguous added values to the Participants.
2. The solution must have a transparent governance model with identified accountability and liability.
3. The solution must be easy to use by its Participants.
4. The solution must be financially sustainable for the Participants and the Gaia-X Association.

4.1 Decentralized Autonomous Organization

Decentralized Autonomous Organization[1], DAO, is a type of governing model where:

- There is no central leadership.
- Decisions are made by the community's members.
- The regulation is done by a set of automatically enforceable rules on a distributed ledger whose goal is to incentive its community's members to achieve a shared common mission.
- The organization has its own rules, including for managing its own funds.

4.2 Gaia-X Association roles

Based on the objective and constraints to achieve those objectives, Gaia-X Association is creating a Gaia-X DAO.

The Gaia-X Association, Gaia-X European Association for Data and Cloud AISBL, has several defined roles, to:

1. Provide a decentralized network with smart contract functionality, via a Gaia-X distributed ledger.
2. Provide a Gaia-X token enabling transactions on the decentralized network.
3. Provide the minimal set of rules to implement interoperability among Participants and Ecosystems. Those rules include how to validate Self-Descriptions, how to issue Labels, how to discover and register on the Gaia-X network another community's Ecosystems and Participants. The rules will be enforced via smart contracts and oracles[2].
4. Provide and operate a decentralized and easily searchable catalogue[3].
5. Provide and maintain a list of Self-description URIs violating Gaia-X membership rules. This list must be used by all Gaia-X Catalogue providers to filter out inappropriate content.

4.3 Decentralized Consensus algorithms

In the ongoing work a consensus algorithm will have to be defined, some considerations to be taken into account:

There is a wide range of existing consensus algorithms[4]. Among the top, we have `Proof of Work` used for example by Bitcoin. It's very energy consuming. We have `Proof of Stake` used by Tezos which requires a minimal set of stakes, i.e. tokens, to become a validator.

One possible consensus algorithm for consideration could be `Proof of Authority`, with the different distributed ledger nodes operated by a number of providers accredited following the rules set by the Gaia-X Association AISBL. Also emerging algorithms such as `Proof of Participation`[5] could be considered.

4.4 Interoperability rules

Gaia-X participants which agree to a specific set of additional rules or scope may constitute an Ecosystem with its own governance (e.g. Catena-X).

Individual Ecosystems can register themselves in the Gaia-X Ecosystem under the condition that they use the Gaia-X Architecture and conform to Gaia-X requirements.

4.4.1 Interoperability criteria

Criteria	Mandatory	Rules
Base	Yes	▪ Must use Gaia-X Self-description format and ontology ▪ Must provide public access to its raw Self-Description files ▪ Must use Verifiable credentials
Infra	No	Must use Gaia-X compliant composition format
Data	No	Must use Gaia-X compliant data description format
Identity	No	Must use Gaia-X compliant Identity methods
Access	No	Must use Gaia-X compliant digital rights and access descriptions
Usage	No	Must use Gaia-X compliant usage policy description[6]

Using this mechanism, a `Provider` from one Ecosystem can have their `Service Offering` made available to other Ecosystems. Other Ecosystems may include those `Service Offerings` in their catalogues depending on their internal rules and the interoperability level.

Not all interoperability levels are mandatory to be awarded as a Gaia-X Ecosystem. The mandatory levels are defined by the Gaia-X DAO.

4.5 Decentralized Catalogue

The Gaia-X Association will provide a decentralized Catalogue which will enable fast and transparent access to Providers and Service Offerings, including Infrastructure, Data and Algorithms offers.

Any Ecosystem can extend this Catalogue by registering their own Self-Description storage URI in the Gaia-X distributed ledger. This creates a `Catalogue of Catalogues` or more precisely a `ledger of Self-description directories`.

Any Ecosystem can create their specific Catalogue out of the decentralized published Self-Descriptions.

4.5.1 Data curation

By offering transparent access to structured and verifiable Service-Descriptions, plus visibility on Service Instance consumption, the Participants can extrapolate about the data quality.

Other metadata, such as using Great Expectations can be enforced at the Data interoperability layer to promote a Data quality score.

---

1. Example of the setup of a DAO https://blockchainhub.net/dao-decentralized-autonomous-organization/ ↩
2. Various oracles can be implemented, include decentralized ones with https://chain.link/ ↩
3. Example of decentralized data and algorithms marketplace https://oceanprotocol.com/ ↩
4. Study of Blockchain Based Decentralized Consensus Algorithms - DOI 10.1109/TENCON.2019.8929439 ↩
5. https://zoobc.how/?qa=92/what-is-proof-of-participation-in-simple-words ↩
6. Could be enforced by Digital Rights Management and https://www.openpolicyagent.org/ or similar. ↩

5. Federation Services

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 *Federation Services* will be outlined in the upcoming Federation Services documents. Details about the role of *Federation Services* for *Ecosystems* are elaborated in section Gaia-X Ecosystems, with an overview shown in the figure below.

- The *Federated Catalogue* constitutes an index repository of 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* covers authentication and authorization, credentials management, decentralized Identity management as well as the verification of analogue credentials.
- *Data Sovereignty Services* enable the sovereign data exchange of Participants by providing a Data Agreement Service and a Data Logging Service to enable the enforcement of Policies. Furthermore, usage constraints for data exchange can be expressed by Provider Policies as part of the Self-Description.
- *Compliance* 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 APIs* will support onboarding and Accreditation of Participants, demonstrate service discovery, orchestration and provisioning of sample services.

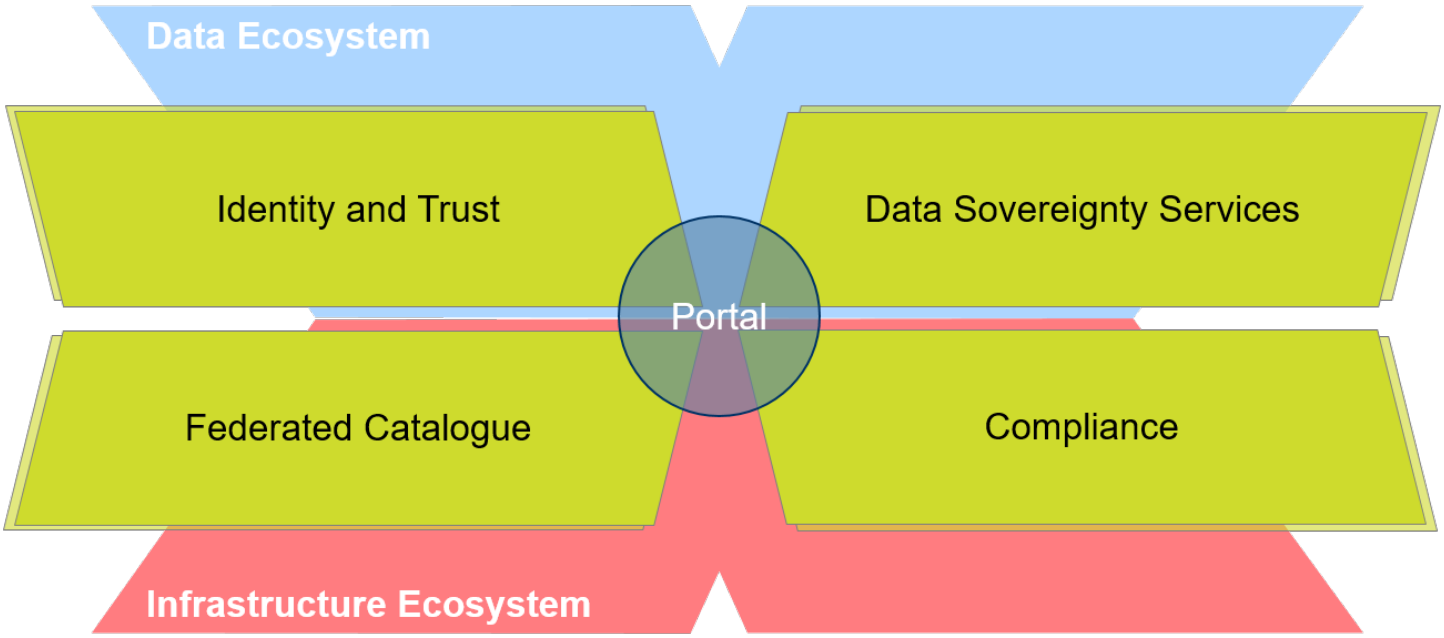


Fig: Gaia-X Federation Services and Portal as covered in the Architecture Document

5.1 Federated Catalogue

Self-Descriptions intended for public usage can be published in a Catalogue where they can be found by potential Consumers. The goal of Catalogues is to enable Consumers to find best-matching offerings and to monitor for relevant changes of the offerings. 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.

A Catalogue stores Self-Descriptions both standalone and aggregated in a graph datastructure. The Self-Description Storage contains the raw published Self-Description files in the JSON-LD format together with additional lifecycle metadata. The Self-Description Graph imports the Self-Descriptions from the Self-Description Storage into an aggregate data structure. The individual Self-Descriptions can reference each other. The Self-Description Graph is the basis for advanced query mechanisms that take the references between Self-Descriptions into consideration.

The system of Federated Catalogues comprises an initial stateless Self-Description browser provided by the Gaia-X, European Association for Data and Cloud, AISBL. In addition, Ecosystem-specific Catalogues (e.g., for the healthcare domain) and even company-internal Catalogues (with private Self-Descriptions to be used only internally) can be linked to the system of federated Catalogues. The Catalogue federation is used to exchange relevant Self-Descriptions and updates thereof. It is not used to execute queries in a distributed fashion.

Cross-referencing is enabled by unique Identifiers as described in Identity and Trust. While uniqueness means that Identifiers do not refer to more than one entity, there can be several Identifiers referring to the same entity. A Catalogue should not use multiple Identifiers for the same entity.

The system of Federated Catalogues comprises a top-level Catalogue operated by 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 function.

Since Self-Descriptions are protected by cryptographic signatures, they are immutable and cannot be changed once published. This implies that after any changes to a Self-Description, the Participant as the Self-Description issuer has to sign the Self-Description again and release it as a new version. 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-service 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 query engine with no internal ranking of results. Users can define filters and sort-criteria in their queries. But if some results have no unique ordering according to the defined sort-criteria, they are randomized. The random seed for the search result ordering is 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. Therefore, Self-Descriptions can be communicated to the Catalogue by third parties, as the trust verification is independent of the distribution mechanism. Self-Descriptions can be marked by the issuer as "non-public" to prevent them from being copied to a public Catalogue by a third party that received the Self-Description over a private channel.

A Visitor is an anonymous user accessing a Catalogue without a known account. 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.

5.1.1 Self-Description

Gaia-X Self-Descriptions express characteristics of Assets, Service Offerings and Participants that are linked to their respective Identifiers. Providers are responsible for the creation of Self-Descriptions of their Assets or Resources. 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 processes. Specifically, Self-Descriptions can be used for:

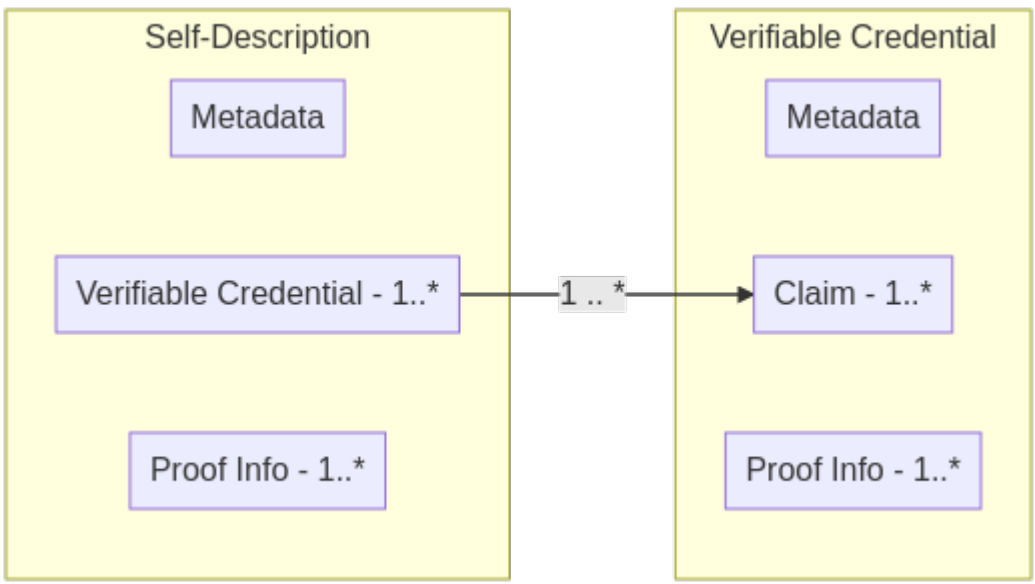
- Discovery and composition of Service Offerings in a Catalogue
- Tool-assisted evaluation, selection, integration and orchestration of Service Instances comprising Assets and Resources
- Enforcement, continuous validation and trust monitoring together with Usage Policies
- Negotiation of contractual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

Gaia-X Self-Descriptions are characterized by the following properties:

- Machine-readable and machine-interpretable
- Technology-agnostic
- Adhering to a generalized schema with 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 easily added
- Navigable and can be referenced from anywhere in a unique, decentralized fashion
- Accompanied by statements of proof (e.g., certificates and signatures), making them trustworthy by providing cryptographically secure verifiable information

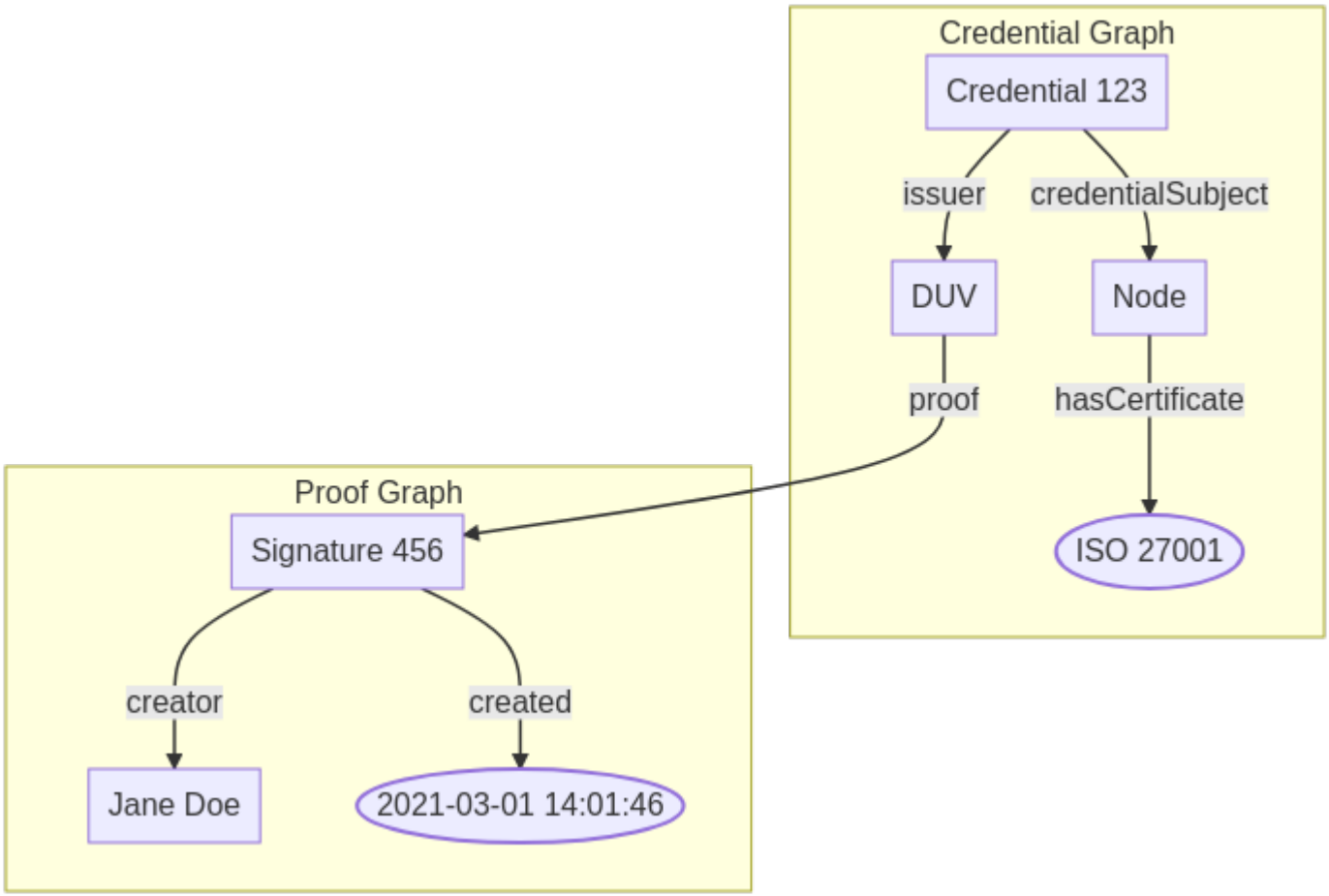
The exchange format for Self-Descriptions is JSON-LD. JSON-LD uses JSON encoding to represent subject-predicate-object triples according to the W3C Resource Description Framework (RDF).

A Self-Description contains the Identifier of the Asset, Resource or Participant, metadata and one or more Credentials as shown in the figure below. 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[1] is the technical standard to express Credentials and Claims on top of JSON-LD[2].



Graph: 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 to express a graph of information about an Asset/Resource (subject). For example, a Node complying with ISO 27001 is shown in the figure below.



Graph: Linked Claim statements as a graph representation

The Self-Description of one entity may refer to another entity by its Identifier. Identifiers in Gaia-X are URIs and follow the specification of RFC 3986. While uniqueness means that Identifiers do not refer to more than one entity, there can be several Identifiers referring to the same entity. A Catalogue should not use multiple Identifiers for the same entity. Depending on the prefix of the URI, different technical systems are defined to ensure uniqueness of Identifiers. For example, the use of a domain-name as part of the Identifier, where only the owner of the domain-name shall create Identifiers for it.

The relations between Self-Descriptions 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 Catalogue 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.

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. Individual Gaia-X Ecosystems can extend the schema hierarchy for their application domain.[3] Such extensions must make an explicit reference to the organization that is responsible for the development and maintenance of the extension.

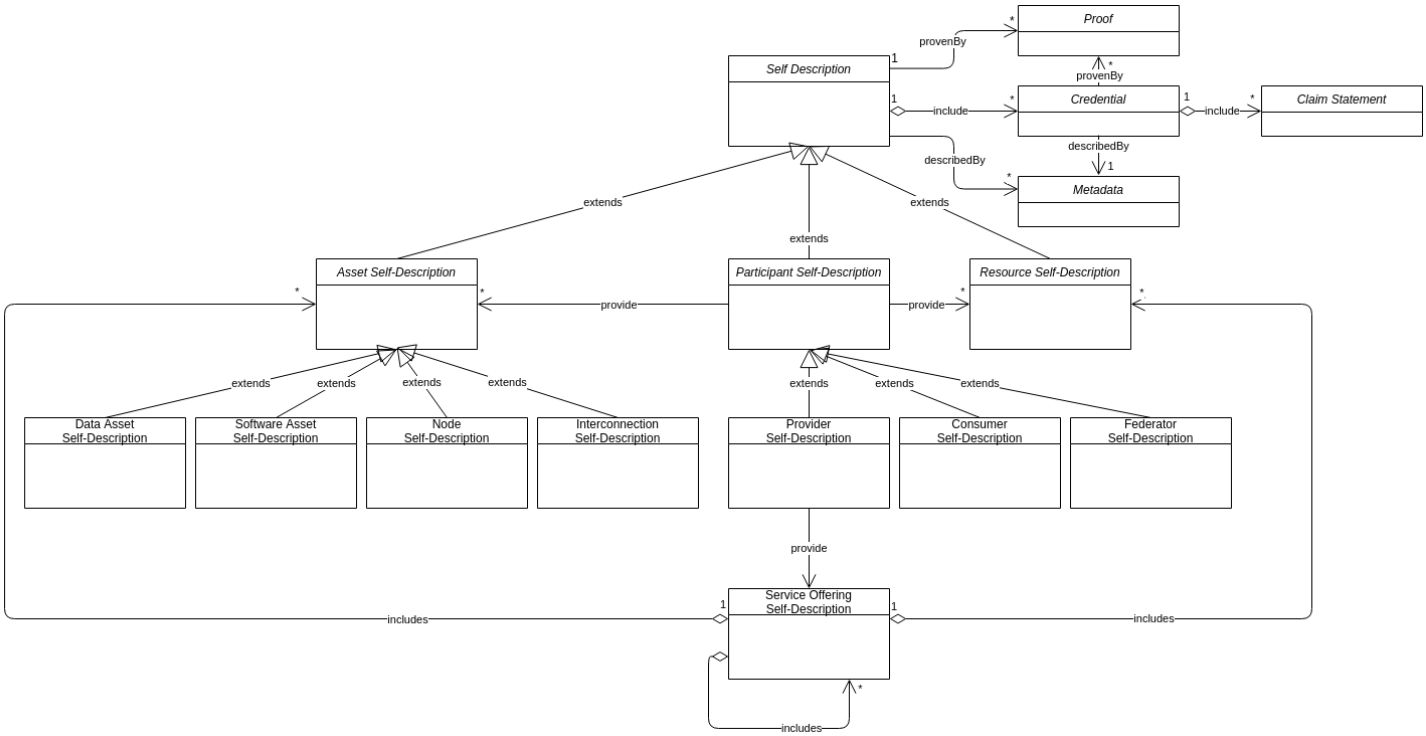


Fig: Schematic inheritance relations and properties for the top-level Self-Description

The Self-Description Schemas can follow the Linked Data best practices[4] making the W3C Semantic Web family[5] a possible standard to be built upon to enable broad adoption and tooling.

Gaia-X aims at building upon existing schemas, preferably those that have been standardized or at least widely adopted[6] to get a common understanding of the meaning and purpose of any property and Claim statements. Examples of attribute categories per Self-Description in Gaia-X are discussed in the Appendix A1,

.

5.2 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. The Identifiers are comparable in the raw form and should not contain more information than necessary (including Personal Identifiable Information). 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 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, acting 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 off-boarding. The table below shows the Participant Lifecycle Process.

Lifecycle Activity	Description
Onboarding	The governing body of a Gaia-X Ecosystem, represented by the Ecosystem's Federators, 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.
Off-boarding	The off-boarding process of a Participant is time-constrained and involves all dependent Participants/Principals.

Table: Participant Lifecycle Process

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. The lifetime of an Identifier is permanent. It may be used as a reference to an entity well beyond the lifetime of the entity it identifies or of any naming authority involved in the assignment of its name. Reuse of an Identifier for a different entity is forbidden. Attributes will be derived from existing identities as shown in the IAM Framework[7].

A secure Identifier for an Identity will be assigned by the issuer in a cryptographically secure manner. This implies that Gaia-X Participants can self-issue Identifiers. It is solely the responsibility of a Participant to determine the conditions under which the Identifier will be issued. Identifiers shall be derived from the native identifiers of an Identity System without any separate attribute needed. The Identifier shall provide a clear reference to the Identity System technology used. Additionally, the process of identifying an Identity Holder is transparent. It must also be possible to revoke issued Identity attributes[8].

5.2.1 Trust Framework

Gaia-X defines a technical trust framework based on open standards and which considers EU regulations, which is applicable for all Participants. The Trust Framework solution supports the privacy and self-determined requirements and gains the chain of trust without the need for 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.

In one Trust/Sovereignty model, Gaia-X European Association for Data and Cloud AISBL is the main trust anchor. Participants trusting Gaia-X Association AISBL is a prerequisite for a widest-reaching Ecosystem. In this sense, Gaia-X can act as a Federator (according to section Gaia-X Conceptual Model). Then, Gaia-X maintains a list of 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 List of eIDAS Trusted Lists[9] can also be used as a source for trust service providers and Conformity Assessment Bodies.

In another supported Trust/Sovereignty model, specific Ecosystems may opt or be required to set up their own trust anchors and Federators. Intra-ecosystem interoperability is achieved by leveraging common Gaia-X technology while having members join each specific Federation under its own rules. In such model, interoperability across Ecosystems requires Participants to simultaneously be members of several Gaia-X-compatible Ecosystems / Federations.

Self-Descriptions (see section Federated Catalogue) 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 upon which it relies. 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.

5.2.2 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 accesses 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 or denies access to Gaia-X. Based on the assigned Principal roles, specific permissions are granted or denied.

In the decentralized identity approach, authentication and authorization in Self Sovereign Identity (SSI) is based on decentralized identifiers (DID)[10]. Public key infrastructure is used to verify controllership of a certain DIDs and Verifiable Credentials[11] which in turn contain any kind of third-party issued attributes. These 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 credentials management applications such as 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 must 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 generally accepted policies as well as domain specific policies derived from private, industrial, governmental and educational sectors.

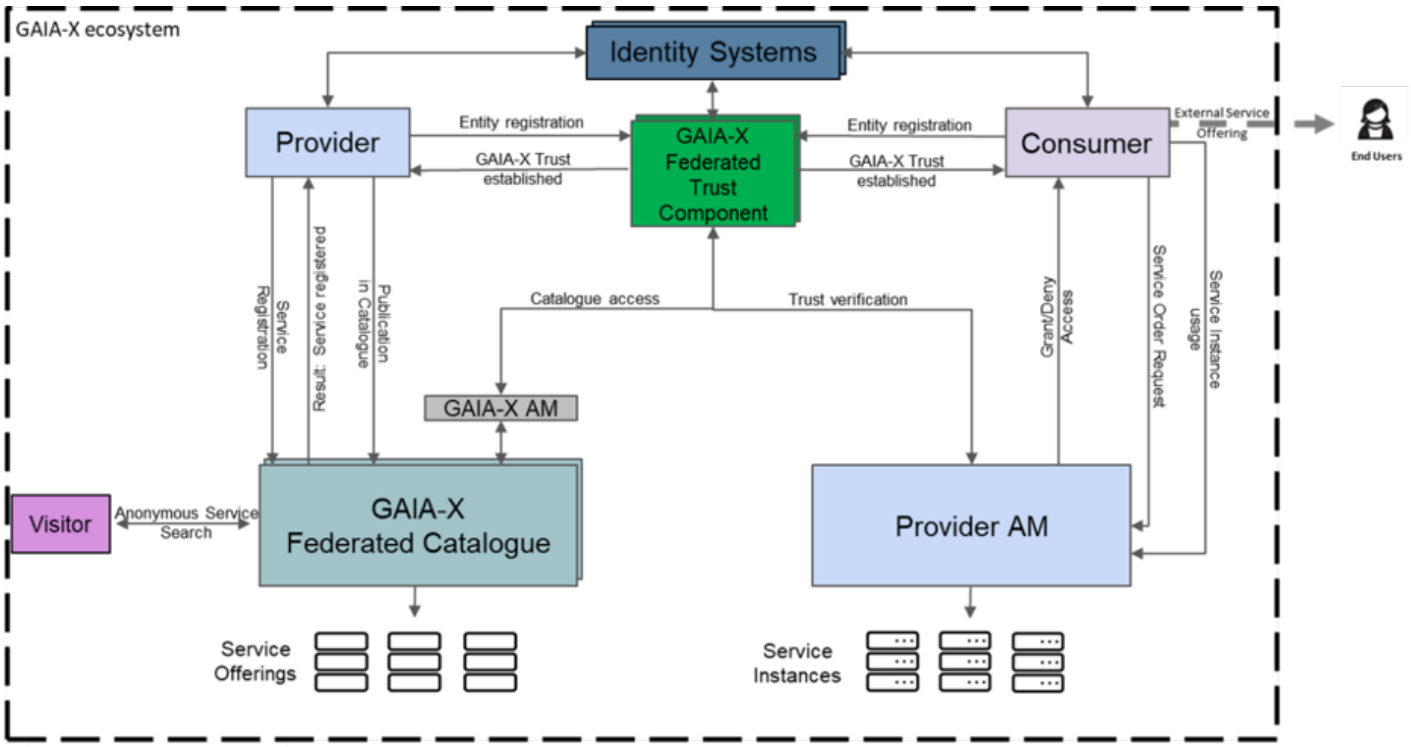


Fig: Detailed Level Design of the Gaia-X Federated Trust Model

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, please see A2.

5.2.3 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 by 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 association AISBL. Clear policies will be in place concerning processes and responsibilities[12].

Gaia-X itself enables fine-grained access control-based attribute evaluation. Attributes will be derived from the metadata, Self-Descriptions and runtime contexts (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.

5.3 Data Sovereignty Services

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: (1) Transparency, and (2) Control of data usage. 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 extend traditional access control. Thus, usage control is concerned with requirements that pertain to future data usage patterns (i.e., obligations), rather than data access (provisions).

5.3.1 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 to form reusable schemes.

The following are essential capabilities for Data Sovereignty in the Gaia-X Data Ecosystems:

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 by all Gaia-X Participants. Therefore, they have to be formalized and expressed in a common standard such as ODRL[13].
Inclusion of Policies in Self-Description	Informational self-determination and transparency require metadata to describe Data Assets including Provider, Consumer, and Usage Policies as provided by Self-Descriptions and the Federated Catalogues.
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 enforcement of Policies.
Enforcement	Monitoring of data usage is a detective enforcement of data usage with subsequent (compensating) actions. In contrast, preventive enforcement[14] ensures the policy Compliance with technical means (e.g., cancel or modify data flows).

Table: Capabilities for Gaia-X Data Sovereignty Services

5.3.2 Functions of Data Sovereignty Services

Information services provide more detailed information about the general context of the data usage transactions. All information on the data exchange and data usage transactions must be traceable; therefore, agreed monitoring and logging capabilities are required for all data usage 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 exchanges. Therefore, three phases of data exchanges 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 transactions, a Data Logging Service receives logging-messages that are useful to trace each 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. The figure below shows the role of mentioned services to enable sovereign data exchange.

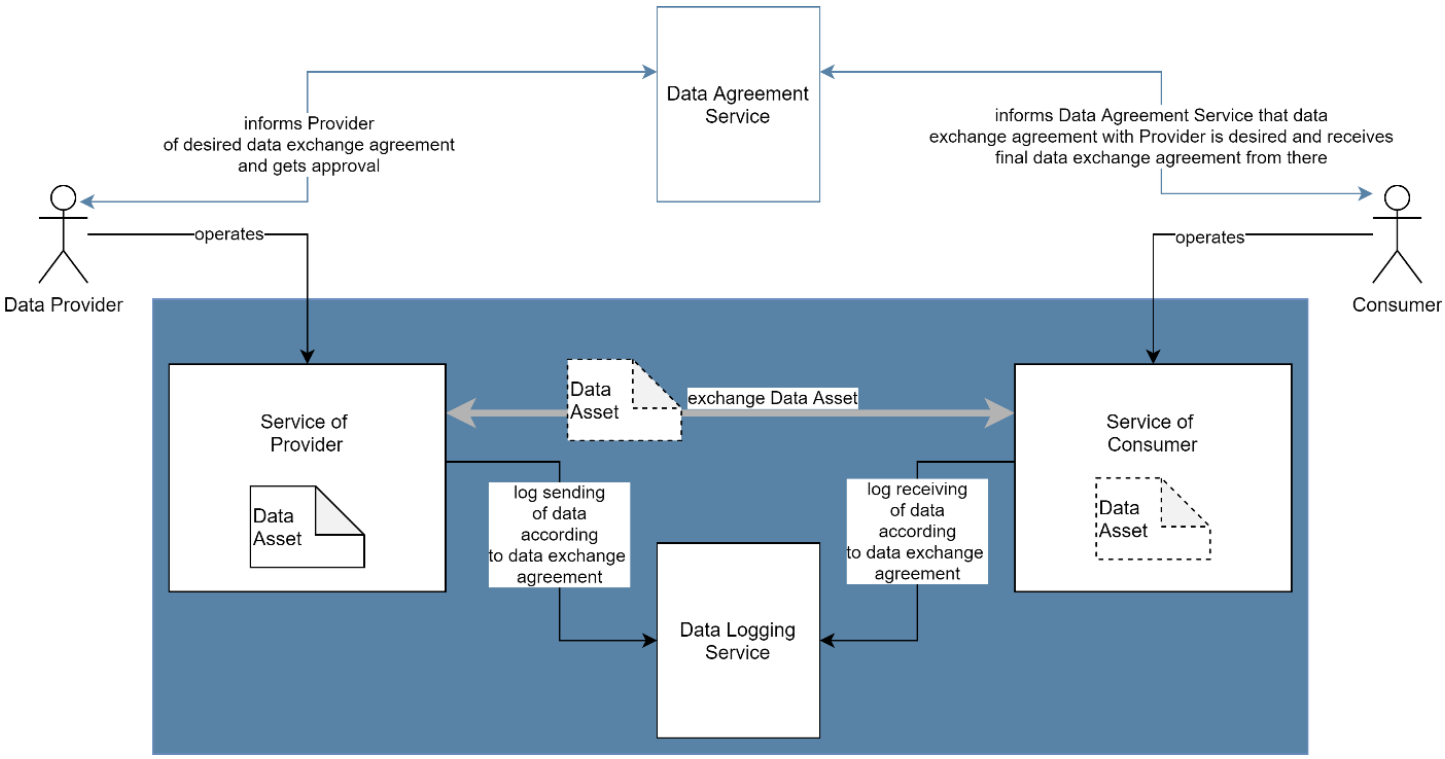


Fig: Data Sovereignty Services Big Picture

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) transmitted, (b) received and (c) that rules and obligations (Usage Policies) were successfully enforced or were violated. This supports the clearing of operational issues but also identifies fraudulent transactions.

The Provider can track if, how, and 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.

5.4 Compliance

Gaia-X defines a Compliance framework that manifests itself in the form of a code of conduct, third party Certifications / attestations, or acceptance of Terms and Conditions. It is detailed in the Policy 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 Federation Services Compliance is to provide Gaia-X users with transparency on the Compliance of each specific Service Offering.

Federation Services consist 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 Assessments. Beside the general onboarding workflow, special functions must include:

- Monitoring of the relevant bases for Compliance
- Monitoring of updates to Service Offerings that should trigger revisions / recertifications for Compliance
- Suspension of Service Offerings
- Revocation of Service Offerings

5.5 Gaia-X Portals and APIs

The Gaia-X Portals support Participants to interact with Federation Services 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. Each Ecosystem can deploy its own Portals to support interaction with Federation Services. 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 in signing up as members of Gaia-X association AISBL. Participants are supported in 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 for all integrated services. An API portal will provide a single point of information about available API services and version management.

---

1. 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/ ↩
2. W3C. JSON-LD 1.1: A JSON-based Serialization for Linked Data [W3C Recommendation 16 July 2020]. https://www.w3.org/TR/json-ld11/ ↩
3. 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 ↩
4. Berners-Lee, T. (2009). Linked Data. W3C. https://www.w3.org/DesignIssues/LinkedData ↩
5. W3C. (2015). Semantic Web. https://www.w3.org/standards/semanticweb/ ↩
6. 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) ↩
7. 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. ↩
8. For more details 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. ↩
9. 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/#/ ↩
10. W3C. (2021). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/ ↩
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. For details, please 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. ↩
13. W3C. ODRL Information Model 2.2 [W3C Recommendation 15 February 2018]. https://www.w3.org/TR/odrl-model/ ↩
14. Currently not in scope of Gaia-X Federation Services ↩

6. Gaia-X Participant Use Cases

The goal of this section is to illustrate how the Consumers, Federators and Providers described in the conceptual model can appear. Therefore, different actors are considered in the role of Consumer and Provider. This section focuses on the most typical kinds of actors and the list is not exhaustive.

6.1 Provider Use Cases

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

6.1.1 Cloud Service Provider

This section focuses on cloud service providers in the Provider role. A possible service model can be Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) providers. The deployment model explicitly includes private clouds, public clouds, edge and hybrid clouds. As standardization is crucial to achieve interoperability and portability, Gaia-X builds on existing standards.

6.1.2 Data Provider

When offering data via Gaia-X, Data Sovereignty Services offer the capacity to provide Data Assets with attached usage control mechanisms. This means that data service provisioning and data usage monitoring are enabled. Furthermore, the Consumer can also define Policies, which present obligations for the Provider. This could, as an example, mean that only data obtained within 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.

6.1.3 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 to provide their services to a broad mass of Gaia-X stakeholders following certain Compliance regulations and standards, but also provide easy access to other complementary services being provided via Gaia-X.

6.1.4 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. Among 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).

6.2 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.

6.2.1 Cloud Service Consumer

The consumption of cloud services via Gaia-X, referring to those who follow Gaia-X standards 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 to a single Provider. 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. Furthermore, other customized services may appear, based upon cloud service composition. Consumers will keep control over their Digital Sovereignty and ensure that their trade secrets remain undisclosed.

6.2.2 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 which 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.

6.2.3 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.

6.2.4 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. Specifically, Federation Services with Identity Management provide tangible benefits in this area: high-performance computing is often used in the academic sector with independent Identity federations on national and/or international levels. Gaia-X could support such use cases by providing standards for service definitions as well as solutions to ensure interoperable service compositions which span sectors. Furthermore, Gaia-X strives to facilitate 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 lower barriers to entry.

6.2.5 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 does not have to be a Gaia-X Participant or undergo any Certification processes.

6.3 Federator Use Cases

6.3.1 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 with, or be based upon, open source Federation Services software. The domain-specific Ecosystem may include, for example, domain-specific Catalogues, additional trust mechanisms or requirements for data sharing.

6.3.2 Federator of a Gaia-X Ecosystem

A Gaia-X Ecosystem is approved if all Federators comply to Gaia-X Policy Rules, and 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.

6.3.3 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 Services software but may not be officially compliant with Gaia-X Policy Rules. An Ecosystem may, for example, provide only a private Catalogue and set up its own criteria for having access to the Ecosystem. Despite this kind of Ecosystem based on Gaia-X Policy Rules and Services, it cannot be called an official Gaia-X Ecosystem.

6.3.4 Gaia-X Association AISBL in the Federator role

The Gaia-X Association 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 must comply with the Policy Rules and other Compliance mechanisms, just as any other Federator is required to do.

6.4 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 Gaia-X association AISBL does not play an intermediary role during the Contract negotiations but ensures the trustworthiness of all relevant Participants and Service Offerings.

The following diagram presents the general workflow for Gaia-X service provisioning and consumption processes. Please note that this overview represents the current situation 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 the following objects:

Data Sovereignty Services appear in the mutual agreement and execution of (Usage) Policies that are defined in a Contract and concern the Data Asset.

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

Compliance is also assured during the onboarding and is subject to the underlying continuous automated monitoring throughout the lifecycle.

The Federated Catalogue and the Self-Descriptions details the elements that match Consumers with Providers.

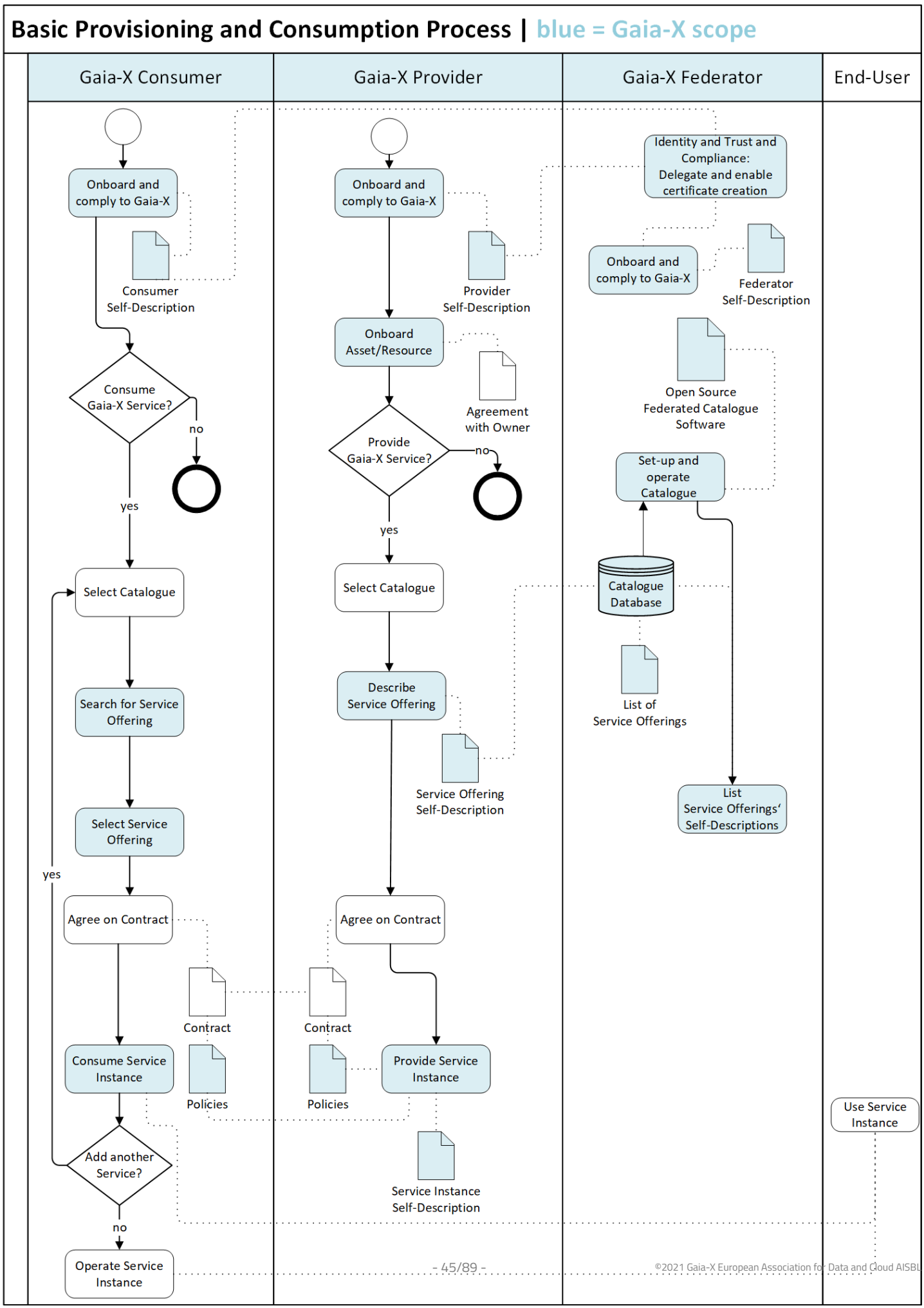


Fig: 10 Basic Provisioning and Consumption Process

7. Gaia-X Ecosystems

7.1 Gaia-X as Enabler for Ecosystems

The Gaia-X Architecture enables Ecosystems and data spaces using the elements explained in the Gaia-X Conceptual Model in general and the Federation Services 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 and its associated benefits.

Gaia-X proposes to structure a Data Ecosystem and an Infrastructure Ecosystem, each with a different focus on exchanged goods and services. Despite each of them having a separate focus, they cannot be viewed separately as they build upon each other, i.e. they are complementary.

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.

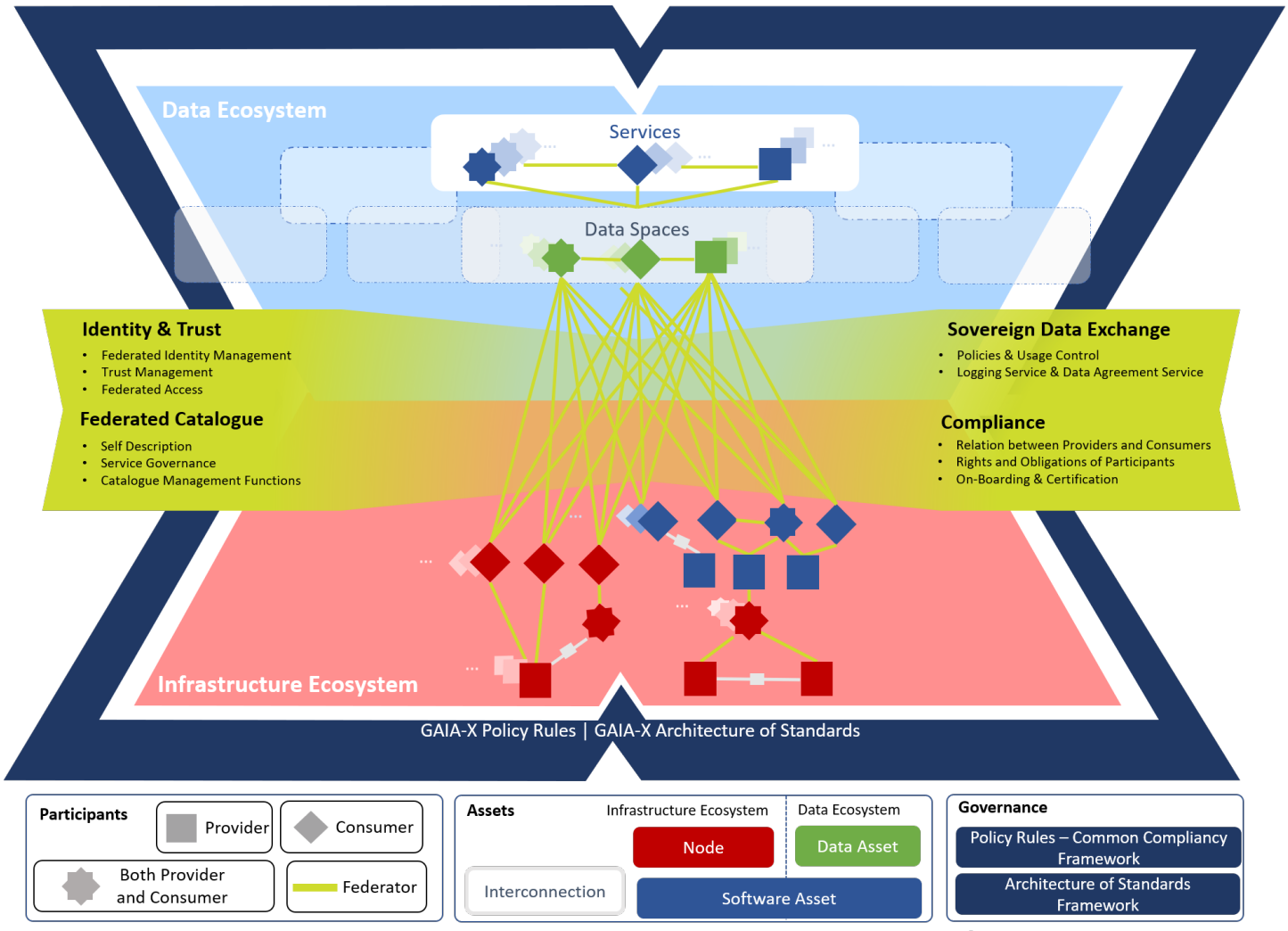


Fig: Gaia-X Ecosystem Visualization

The basic roles of Consumer and Provider are visualized as different squares, while the Federator appears as a connecting layer, offering diverse core Federation Services. Federation Services provide connections between and among the different elements as well as between or among the different Ecosystems. The star-shaped element visualizes that Consumers can act also as Providers by offering composed services or processed data via Catalogues. Governance includes 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.

7.2 The Role of Federation Services for Ecosystems

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

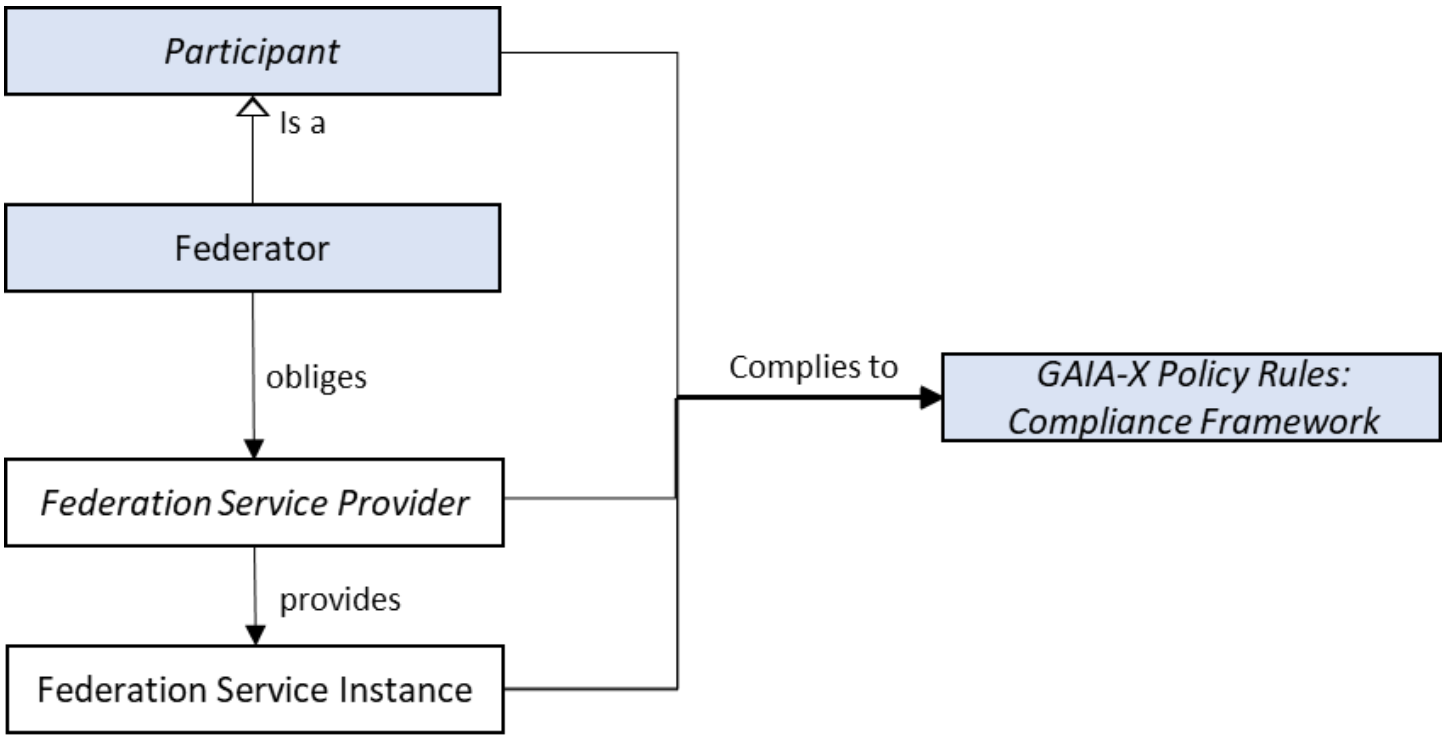


Fig: Federation Services Relations

7.2.1 Goals of Federation Services

Federation Services aim to enable and facilitate interoperability and portability of Assets and Resources within and across Gaia-X-based Ecosystems and to provide Data Sovereignty. They ensure trust between or among 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 enable the interoperability and portability of data. The set of Ecosystems that use the Federation Services form the Ecosystem.

7.2.2 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 Federation Services. (Comparable to DNS servers: there are local servers, but information can be pushed up to the root servers).

Therefore, a decentralised synchronization mechanism is necessary.

7.2.3 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 Association AISBL. The Gaia-X Association 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 Association AISBL. This does not affect the functionality of the Federation Services within specific Ecosystems 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 Architecture Requirements.

Requirement	Relation to the Federation Services
Interoperability	▪ The Federated Catalogues ensure that Providers offer services through 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. Semantic interoperability enables that data exchange.
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 is “fit for purpose” and makes the interaction possible. ▪ The open source implementations of the Federation Services provide a common technical basis and enables movement of Assets and Resources in ecosystems and across different ecosystems. ▪ 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.

Requirement	Relation to the Federation Services
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.

Table: Federation Services match the Architecture Requirements

7.2.4 Infrastructure Ecosystem

The Infrastructure Ecosystem has a focus on computing, storage and Interconnection elements. In terms of Assets and Resources, these elements are designated as Nodes, Interconnections and different Software Assets. They range from low-level services like bare metal computing up to highly 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.

7.2.5 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 stored in different cloud storage backends. 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 of a fixed defined partner or central keystone companies. For data to realize its full potential, it must be made available in cross-company, cross-industry Ecosystems. Therefore, Data Ecosystems not only enable significant data value chain improvements, but provide the technical means to enable Data Sovereignty. Such sovereign data sharing addresses different layers and enables a broad range of business models that would otherwise be impossible. Trust and control mechanisms encourage the acceleration of data sharing and proliferate the growth of Ecosystems.

7.2.6 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:

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 the many. 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 and strengths 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 specific new 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)	Self-Description ensures that all Assets, Resources and Service Offerings are defined standardized ways, which enables them to be listed in a searchable Catalogue, each with a unique Identifier. Therefore, it facilitates the reuse and distribution of these components.

Principle	Need for Gaia-X	Implemented in Gaia-X Architecture
Federation	Federation technically enables connections and a web of trust between and among different parties in the Ecosystem(s). 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. Furthermore, different Conformity Assessment Bodies may exist.
Sharing	Sharing of the relevant services and components contributes to the Ecosystem development. Sharing and reuse of Assets and Resources across the Gaia-X Ecosystem enables positive spillovers, leading to new and often unforeseen economic growth opportunities.	The Federated Catalogues enable the matching between Providers and Consumers. Sovereign Data Exchange lowers hurdles for data exchange and Ecosystem creation.

Table: Summary of Federation Services as enabler

By utilizing common specifications and standards, harmonized rules and policies, Gaia-X is well aligned with specifications like NIST Cloud Federation Reference Architecture[1]:

- Security and collaboration context are not owned by a single entity
- Participants in the Gaia-X Association AISBL jointly agree upon the common goals and governance of the Gaia-X Association 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 could risk losing their Gaia-X compliance level

7.3 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 fully 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 an equivalent QoS (Quality of Service)

7.3.1 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 as a Service [IaaS], Platform as a Service [PaaS], Software as a Service [Saas], data assets, 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 data 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.

7.4 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 are flexibly exchanged between and among many different Participants. Therefore, Interconnection Services represent a dedicated category of Assets as described in section Gaia-X Conceptual Model.

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

7.4.1 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 the figure below[2]. Such a perspective enables a differentiated service capability between "Best Effort" services, e.g., basic Internet connectivity, and higher-level services, which can be provided by dedicated Interconnection and networking services. Consequently, and as explained in section Provider Use Cases, the Federated Catalogues must be extended with adequate networking and Interconnection services, considering, for instance, functional and non-functional QoS (Quality of Service) requirements; portability requirements, etc.

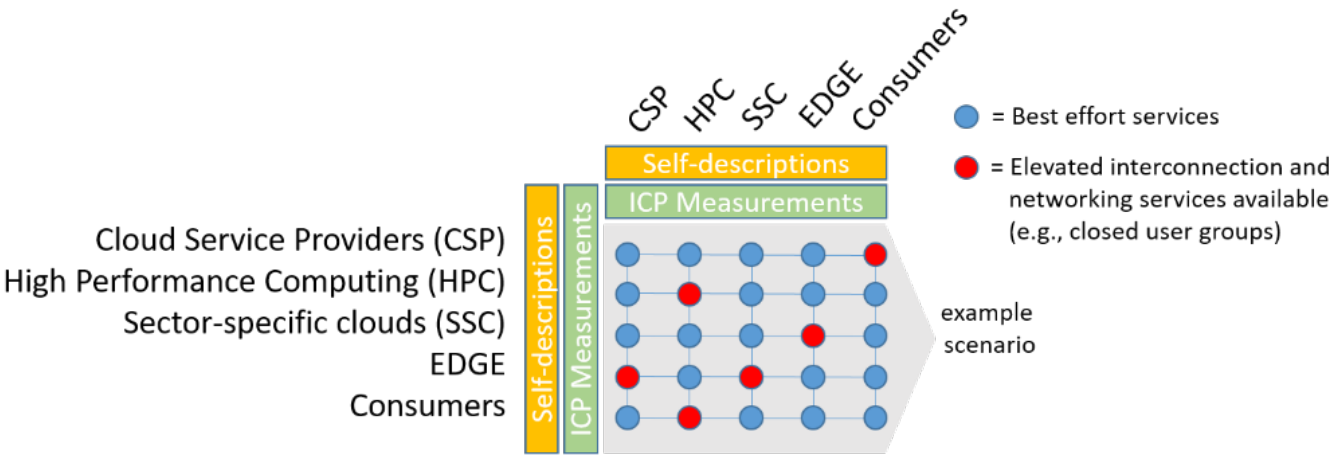


Fig: Gaia-X network requirements to use case mapping.

Currently, Gaia-X addresses the architectural needs for networking and Interconnection via three building blocks: (i) a Self-Description model, which describes Interconnection Assets and attributes necessary to describe networking services; (ii) inter-node measurements, describing connectivity between or among Gaia-X Participants; (iii) interconnection and networking services based on Internet and their assessment via QoS (Quality of Service) indicators.

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 (Quality of Service) functional parameters relevant for real-time data services, e.g., latency, data rates, bandwidth. Non-functional requirements for supported services must also be defined. Therefore, Self-Description of Interconnection and networking services should not be limited to QoS (Quality of Service) 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 Services Catalogues.

7.4.2 Network Service Composition

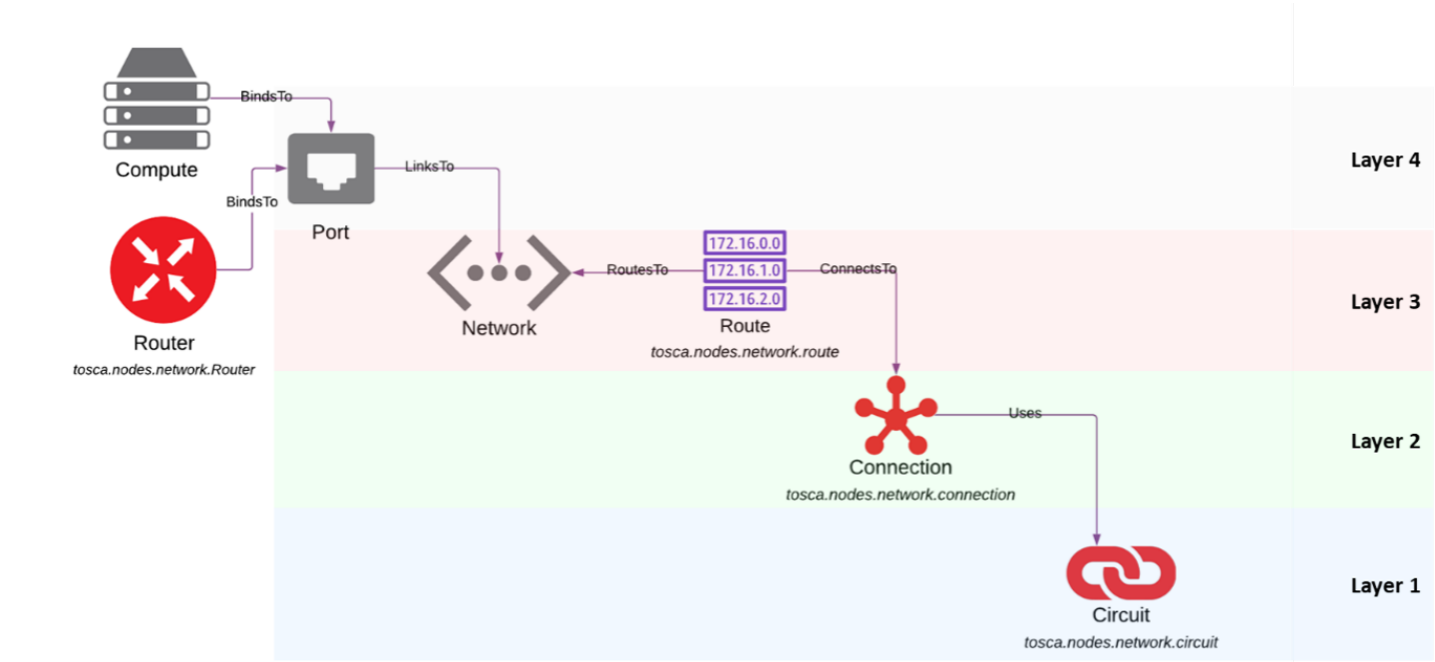
Networking and Interconnection services can be composed via heterogeneous offerings from multiple Providers and technologies. To achieve flexibility but also sovereignty and trust, network service composition shall be supported. It is also relevant to consider the capability to describe Interconnection 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[3].

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 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 by Gaia-X are, for instance, the OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA)[4]. 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)[5].

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.

A Gaia-X compliant Network Service Composition Framework should cover all communication aspects in both public and private networks as well as across all OSI Layers from OSI Layer 4 to OSI Layer 1. In order to achieve that, relevant services need to be defined.



A Network Service is a specific Gaia-X compatible Service Offering running on one or many Nodes. This type of Service provides Network Functions such as:

- Switching
- Routing
- Security Functions
- Load Balancing
- etc.
- Combinations of the above

Such a Network Service is provided by a Provider and shall be described by a Self-Description and available via Federated Catalogue for Consumers to deploy and use. To interconnect these or other Gaia-X Services, communication paths can flow via one or multiple Network Services. In any case, communication between Gaia-X Services (including communication between Network Services) would need to be established over one of the following interconnection assets:

Networks

Networks are logical communication Assets which can directly bind to Nodes via a link to a Nodes Port. A Network will link together at least two or more Ports of one or more Nodes. It is defined by the Network Protocol used, as defined in ISO/IEC standard 7498-1: for Layer 3 of the ISO/OSI Model and will use Network Addressing for the Nodes as appropriate for the Network Protocol. An example of Network Definitions can be found in the TOSCA Framework.

In order to provide Interconnection even across administrative domains, the definition of specific Interconnection Assets are needed.

Routes

A Route Asset is an Asset which defines the Reachability of one or more Networks and can be subscribed individually by users. A Route Asset will operate on Layer 3 of the ISO/OSI Model and provide connectivity to other networks using other Network Services or Interconnection Assets. These services or assets can be explicitly defined or be provided by the Route Service itself.

Connections

Connection Services operate on Layer 2 of the ISO/OSI Model and will provide a direct communication path between Networks. They can use other Network Services or Interconnection Assets. These services or assets can be explicitly defined or be provided by the Connection Asset itself.

Circuits

Circuit Assets are direct connections between two Networks or Ports and provide a direct communication path between single Networks or Nodes. They are defined by specific endpoints and cannot use other Interconnection Assets to realize the connection. They operate on Layer 1 or Layer 2 of the ISO/OSI Model.

Self-Description Attributes

To allow Customers to consume any of the above-mentioned Network Services, each of them needs to be available as a Service Offering from the Federated Catalogues and needs a self-description. To enable Network Service Composition in an automated way, any Network Service Offering and Interconnection Asset needs to describe itself from a functional and customer quality requirement view. For Interconnection Assets such as Routes, Connections or Circuits this can include network based quality parameters such as bandwidth, latency, jitter, availability. To be able to compose Network services, Interconnection Assets need attributes that describe their dependency on other Network Services or Interconnection Assets, so that Customers can query the Catalogue for the dependencies and order these according to the further requirements. In this sense, a Route Asset can provide no quality attributes itself, but depend on a specific subset of Connection or Circuit Assets that provide specific quality attributes. The Customer can query those Assets from the Catalogues. This query specifies for example detailed quality requirements, which select a specific dependency to provide the Route Asset on. A Gaia-X compliant orchestration service will then orchestrate the Network Services according to the selected services.

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[6] 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 searched in the Federated Catalogues and can be used in composing more complex services by Gaia-X users[7].

In order to ensure certain requirements of latency, bandwidth and security Gaia-X has to be able to propose more than the classic Internet with the Best-Effort principle does. The solution that we see is the Gaia-X Interconnection platform - a common or standardized API via which the interconnected WANs can exchange and make their services available. IX-API could be a possible solution to implement such a platform. This service will be provided and operated by a Gaia-X Provider (e.g., Interconnection Provider).

The resources and data from the Provider and User use cases are located in different physical locations, namely in data centers that could be spread all over Europe. If we would interconnect them directly that would result in the redundant number of connections, which would be expensive, insufficient and neither dynamic nor performant. In the example shown below, if we want to interconnect 8 data centers we would require 28 connections (picture on the left). However, with the introduction of the Interconnection platform we would need only eight connections (picture on the right). This not only means that multi-cloud setups will become easier and faster, but also that dynamic service provisioning will be possible. It will ensure the competitiveness of Gaia-X against the existing hyperscalers, as the elevated networking and interconnection services will be met.

For those customers who do not want that their traffic passing via the platform, it will also be possible to create a Closed User Group (multipoint VPN) or private point-to-point connections (for example).

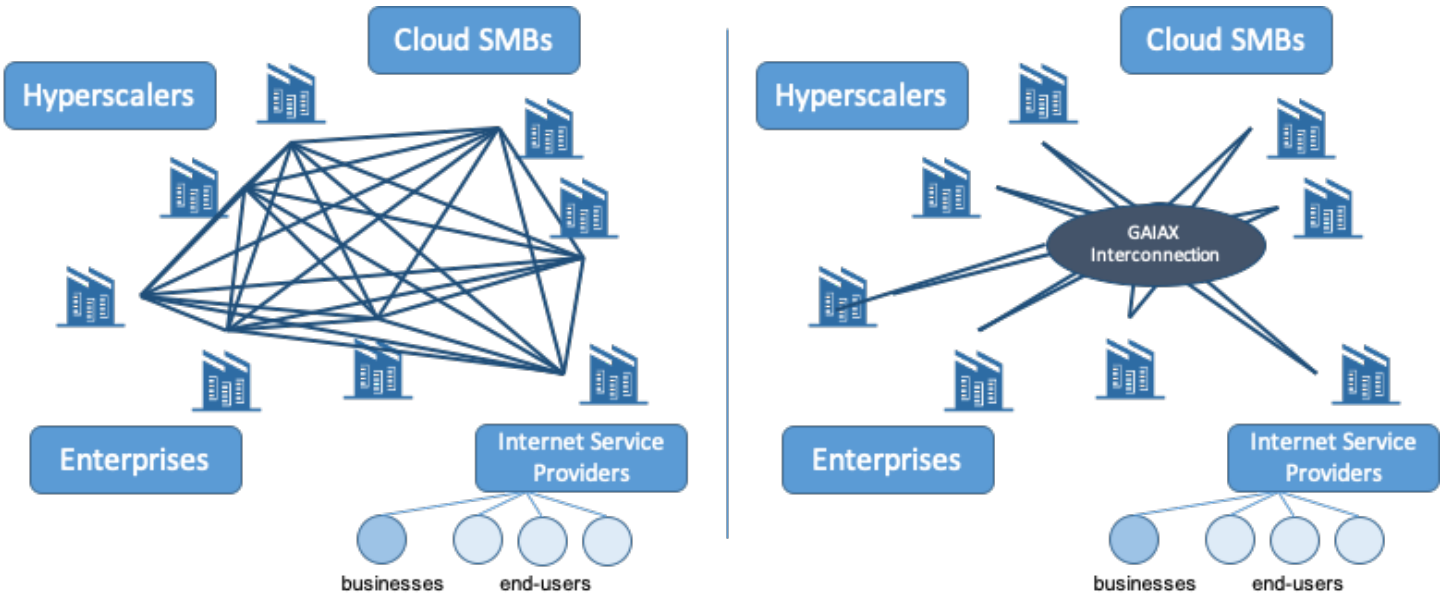


Fig: Visualization of connections via Interconnection Platform: left - without platform, right - with platform

1. 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 ↩
2. 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. 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. ↩
4. 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 ↩
5. ETSI. Network Functions Virtualisation (NFV). https://www.etsi.org/technologies/nfv ↩
6. IX-API. IX-API. https://ix-api.net/ ↩
7. 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. ↩

8. Glossary

8.1 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.

8.1.1 references

- ISO/IEC 17000:2004(en)

8.2 Architecture of Standards

The Architecture of Standards (AoS) document defines a target for Gaia-X by analysing and integrating already existing standards for data, sovereignty and infrastructure components and specifying which standards are supported.

8.2.1 alias

- AoS

8.2.2 references

- This definition was consolidated from Gaia-X documents

8.3 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.

8.3.1 references

- Adapted from Togaf V 9.2, 20.2

8.4 Asset

Element used to compose the Service Offering, which does not expose an endpoint.

8.4.1 reference

- https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-3:ed-1:v1:en:term:3.1

8.5 Asset Owner

A natural or legal person who is in legal possession of the Asset and is responsible to set policy rules on the Asset.

8.6 Catalogue

A Catalogue is an instance of the Federation Service Federated Catalogue and presents a list of available Service Offerings.

Catalogues are the main building blocks for the publication and discovery by a Participant's of Service Offering's Self-Descriptions.

8.6.1 alias

- Gaia-X Catalogue

8.7 Certification

The provision by an independent body of written assurance that the Participants, Assets, Resources in question meet specific requirements.

8.7.1 references

- Adapted from ISO: https://www.iso.org/certification.html

8.8 Claim

An assertion made about a subject within Gaia-X.

8.8.1 references

https://www.w3.org/TR/vc-use-cases/#terminology

8.9 Compatibility

8.9.1 definition

Compatibility is defined according to ISO/IEC 25010:2011 as the degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment

8.9.2 references

- ISO/IEC 25010:2011

8.10 Compliance

Compliance refers to the accordance with Gaia-X Rules.

8.11 Compliance (Federation Service)

Compliance is a Gaia-X Federation Service.

It provides mechanisms to ensure that Participants and Service Offerings in a Gaia-X Ecosystem comply with the Compliance framework defined by Gaia-X, e.g., in the Policy Rules.

8.12 Conformity Assessment

Conformity assessment is the demonstration that specified requirements relating to a product, process, service, person, system or body are fulfilled.

8.12.1 references

- https://www.iso.org/foreword-supplementary-information.html

8.13 Conformity Assessment Body

Body that performs Conformity Assessment services.

8.13.1 references

- DIN EN ISO/IEC 17000

8.14 Consumer

A Consumer is a Participant who consumes a Service Instance in the Gaia-X ecosystem to enable digital offerings for End-Users.

Note: A Gaia-X Consumer will act as a Cloud Service Customer (CSC) of the relevant Provider, but will probably also be offering cloud and/or edge services and thus acting as a Cloud Service Provider (CSP) in their own right to the customers and partners of their own business. The latter are considered End-Users from a Gaia-X perspective.

8.15 Consumer Policy

A Consumer Policy is a Policy in a technical sense that describes a Consumer's restriction of their requested Assets and Resources.

8.15.1 alias

- Search Policy

8.16 Continuous Automated Monitoring

Process that automatically gathers and assesses information about the compliance of Gaia-X services, with regard to the Gaia-X Policy Rules and Architecture of Standards.

8.16.1 alias

- CAM

8.17 Contract

Contract represents the binding legal agreement describing a Service Instance and includes all rights and obligations.

8.18 Credential

A set of one or more Claims made and asserted by an issuer.

8.18.1 references

https://www.w3.org/TR/vc-use-cases/#terminology

8.19 Data Logging Service

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.

8.19.1 alias

- DLS

8.19.2 references

- Federation Services Specification GXFS

8.20 Data Sovereignty Service

Data Sovereignty Service is a Gaia-X Federation Service.
It enables the sovereign exchange and use of data in a Gaia-X Ecosystem using digital Policies to enforce control of data flow(s) and provide transparency of data usages.

8.21 Data Agreement Service

Data Agreement Service is a Federation Service of the category Data Sovereignty Service and considers negotiation of agreements for data exchange.

8.21.1 alias

- DAS

8.21.2 references

- Federation Services Specification GXFS

8.22 Data Asset

Data Asset is a subclass of Asset and consists of data (also including derived data) in any form and includes the necessary information for data sharing.

8.23 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.

8.23.1 references

Oliveira, M. I. S., Lima, G. D. F. B., & Lóscio, B. F. (2019). Investigations into Data Ecosystems: a systematic mapping study. Knowledge and Information Systems, S.16

8.24 Data Privacy

Data Privacy is defined according to ISO/TS 19299:2015, 3.32 as rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

8.24.1 references

- ISO/TS 19299:2015, 3.32

8.25 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.

8.25.1 references

- IDS RAM 3.0

8.26 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 the following design principles:

1. data resides in its sources;
2. only semantic integration of data and no common data schema;
3. nesting and overlaps are possible;
4. spontaneous networking of data, data visiting and coexistence of data are enabled.

Within one Data Ecosystem, several Data Spaces can emerge.

8.26.1 references

Franklin, M., Halevy, A., & Maier, D. (2005). From databases to dataspaces: a new abstraction for information management. ACM Sigmod Record, 34(4), 27-33.

8.27 Digital Rights Management

Digital Rights Management (DRM) is the use of technical means to ensure that the authorised recipient of licensed content is limited to those rights that have been granted under license.

While the term DRM is usually associated with the protection of high-value media such as movies and television delivered to consumers, the subtype Information Rights Management is sometimes used to ensure correct usage of enterprise data.

DRM of all kinds usually involves the delivery of content in an encrypted form that requires both authorised/certified client software and a valid license to access.

The receiver is then able to access the content through the unlocked client which can enforce any required restrictions.

8.28 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.

8.28.1 references

- Gaia-X, TAD 2020 p.3

8.29 Ecosystem

An Ecosystem enables value creation by autonomous, loosely coupled actors via both cooperation and competition.

8.29.1 alias

- Federation

8.29.2 references

adapted from Moore, J.F. 1998. The Rise of a New Corporate Form. Washington Quarterly. Vol. 21(1), pp. 167-181.

8.30 End-User

A natural person or process not being a Principal, using a digital offering from a Consumer. An End-User has an identity within the Consumer context.

8.30.1 references

- https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en:sec:3.2.11

8.31 Endpoint

Combination of a binding and a network address.

8.31.1 reference

- https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:23188:ed-1:v1:en:term:3.1.7

8.32 Federated Catalogue

Federated Catalogue is a Gaia-X Federation Service. It enables the discovery and selection of Providers and Service Offerings in a Gaia-X Ecosystem.

8.33 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 proof of the involved Participants to make sure that Gaia-X Participants are who they claim to be.

8.33.1 alias

Federated Trust Model

8.34 Federation

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

8.34.1 alias

Ecosystem

8.35 Federation Services

Federation Services are services required for the operational implementation of a Gaia-X Data Ecosystem.

8.35.1 references

- Architecture Document 2103

8.36 Federator

Federators are in charge of the Federation Services and the Federation which are independent of each other.

Federators are Gaia-X Participants.

There can be one or more Federators per type of Federation Service.

8.37 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.

8.37.1 references

Federation Services Specification GXFS

8.38 Gaia-X AM

Gaia-X internal Access Management component.

8.39 Gaia-X Ecosystem

The Gaia-X Ecosystem consists of all individual ecosystems that use the Gaia-X Architecture and conform to Gaia-X requirements.

Several individual ecosystems may exist (e.g., Catena-X), that orchestrate themselves, use the Gaia-X Architecture and may or may not use the Gaia-X Federation Services open-source software.

8.40 Gaia-X Identifier

One unique attribute used to identify an entity within the Gaia-X context and following the Gaia-X format.

8.41 Identifier

One or more attributes used to identify an entity within a context.

8.41.1 references

- ITU-T Recommendation X1252, Baseline identity management terms and definitions

8.42 Identity and Trust

Identity and Trust is a Gaia-X Federation Service.

It ensures Participants in a Gaia-X Ecosystem are who they claim to be and enables identity and access management for Providers and Consumers.

8.43 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.

8.43.1 references

- ITU-T Recommendation X1252, Baseline identity management terms and definitions

8.44 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).

8.45 Information Rights Management

Information Rights Management (IRM) is a sub-type of Digital Rights Management (DRM) used (as one option) for the protection of enterprise data and to ensure usage only by authorised parties and only according to agreed license terms.

In Gaia-X this could include technology to restrict access to users within the EU or another jurisdiction after the data has been delivered.

Due to cost and complexity, IRM is most likely to be used only on the most valuable or sensitive shared data, or where liability could arise from misuse by the recipient.

8.46 Infrastructure Ecosystem

An Infrastructure Ecosystem is a loose set of actors who provide or consume storage, computing and network capacities.

8.47 Interconnection

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 customers 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.

8.48 Interoperability

Interoperability is defined according to ISO/IEC 17788:2014 as the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

8.48.1 references

- ISO/IEC 17788:2014

8.49 Node

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.

8.49.1 references

- Archimate 3.1 (2019)

8.50 Onboarding and Accreditation Workflow

The onboarding and accreditation workflow is a Federation Service of the category Compliance and concerns the initial onboarding and accreditation of Gaia-X Participants.

8.50.1 alias

- OAW

8.50.2 references

- Federation Services Specification GXFS

8.51 Participant

A Participant is an entity 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.

8.52 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.

8.52.1 references

- NISTIR 4734 02/01/92: NISTIR 4734
- see Policies in Federation Service Compliance

8.53 Policy (technical)

Statements, rules or assertions that specify the correct or expected behavior of an entity.

In the conceptual model, they appear as attributes in all elements related to Assets and Resources.

8.53.1 references

- NIST SP 800-95 Open Grid Services Architecture Glossary of Terms (25 January 2005)
- NISTIR 7621 Rev. 1 NIST SP 800-95 https://csrc.nist.gov/glossary/term/Policy

8.54 Portability

Portability describes the ability to move data or applications between two different services at a low cost and with minimal disruption.

8.54.1 references

- adapted from ISO/IEC 19941:2017(en)

8.55 Principal

A Principal is either a natural person or a digital representation which acts on behalf of a Gaia-X Participant.

8.56 Provider

A Participant who provides Assets, Resources and Service Offerings in the Gaia-X ecosystem.

Note: The service(s) offered by a Provider are cloud and/or Edge services. Thus, the Provider will typically be acting as a Cloud Service Provider (CSP) to their Consumers.

8.57 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 to the Consumer for this component.

8.57.1 references

- AM Framework Document and Technical Architecture Paper R. June 2020

8.58 Resource

A Resource is an internal building block, not available for order, used to compose Service Offerings. Unlike an Asset, it exposes endpoints.

Prominent attributes of a Resource are the location - physical address, Autonomous System Number, network segment - and the jurisdiction affiliations.

8.59 Self-Description Graph

The Self-Description Graph contains the information imported from the Self-Descriptions that are known to the Catalogue and have an “active” lifecycle state.

8.59.1 references

- Federated Catalogue WP

8.60 Self-Description

A Self-Description expresses characteristics of an Asset, Resource, Service Offering or Participant and describes properties and Claims and are linked to the Identifier.

8.60.1 alias

- Gaia-X Self-Description

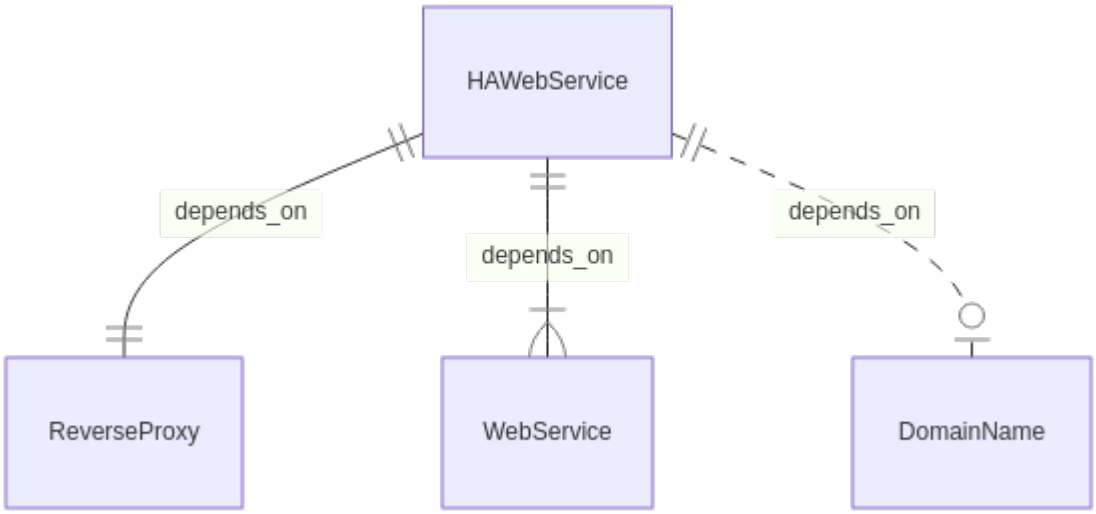
8.61 Service Composition

Service Composition is the ability for a Service Offering to describe and require presence of functional dependencies.

A functional dependency is exposing behaviors in reaction to external actions, matching its requirements and characteristics.

In the Gaia-X conceptual model, a Service Offering‘s functional dependencies can be Resources, Assets or other Service Offerings.

Exemple: A high-availability web server which needs a reverse proxy and two web servers.



8.62 Service Instance

A Service Instance is the instantiation of a Service Offering at runtime, strictly bound to a version of a Self-Description. The Service Instance has a unique Identity and can be composed of one or more atomic building blocks which must be identifiable as they are associated with a Service Subscription.

8.63 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 other Service Offerings.

8.64 Service Subscription

A Service Subscription is an agreement (contract) between a Consumer and a Provider, to allow and regulate the usage of one or more Service Instances. It is related to a specific version of a Service Offering from which it derives the attributes of the Service Instances to be provisioned. The Service Subscription has a distinct lifecycle from the Service Offering and additional attributes and logic.

8.65 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 and is considered to be a Resource.

8.65.1 references

- PID: https://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap03.html#tag_03_300

8.66 Usage Control

Usage Control is a technical mechanism to enforce usage restrictions in the form of Usage Policies after access has been granted. It is concerned with requirements that pertain to future usages (obligations), rather than (e.g., data) access (provisions).

8.67 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.

8.67.1 alias

- Provider Policy

8.67.2 references

- according to IDSA: Usage Control in the IDS, IDS RAM 3.0

8.68 Visitor

Anonymous, non-registered entity (natural person, bot, ...) browsing a Gaia-X Catalogue.

9. Changelog

9.1 2021 June release

- Adding a new Operating model section introducing the first principle for Gaia-X governance.
- Adding preview of Self-Description mandatory attributes in the Appendix.
- Improvement of the Policy rules.
- Improvement of the `Asset` and `Resource` definitions.
- Complete release automation from Gitlab.
- Source available under the 21.06 tag.

9.2 2021 March release

- First release of the Architecture document by the Gaia-X Association AISBL
- Complete rework of the Gaia-X Conceptual Model with new entities' definition.
- Adding a Glossary section
- Source available under the 21.03-markdown tag.

9.3 2020 June release

- First release of the Technical Architecture document by the BMWi

10. 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 association 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/

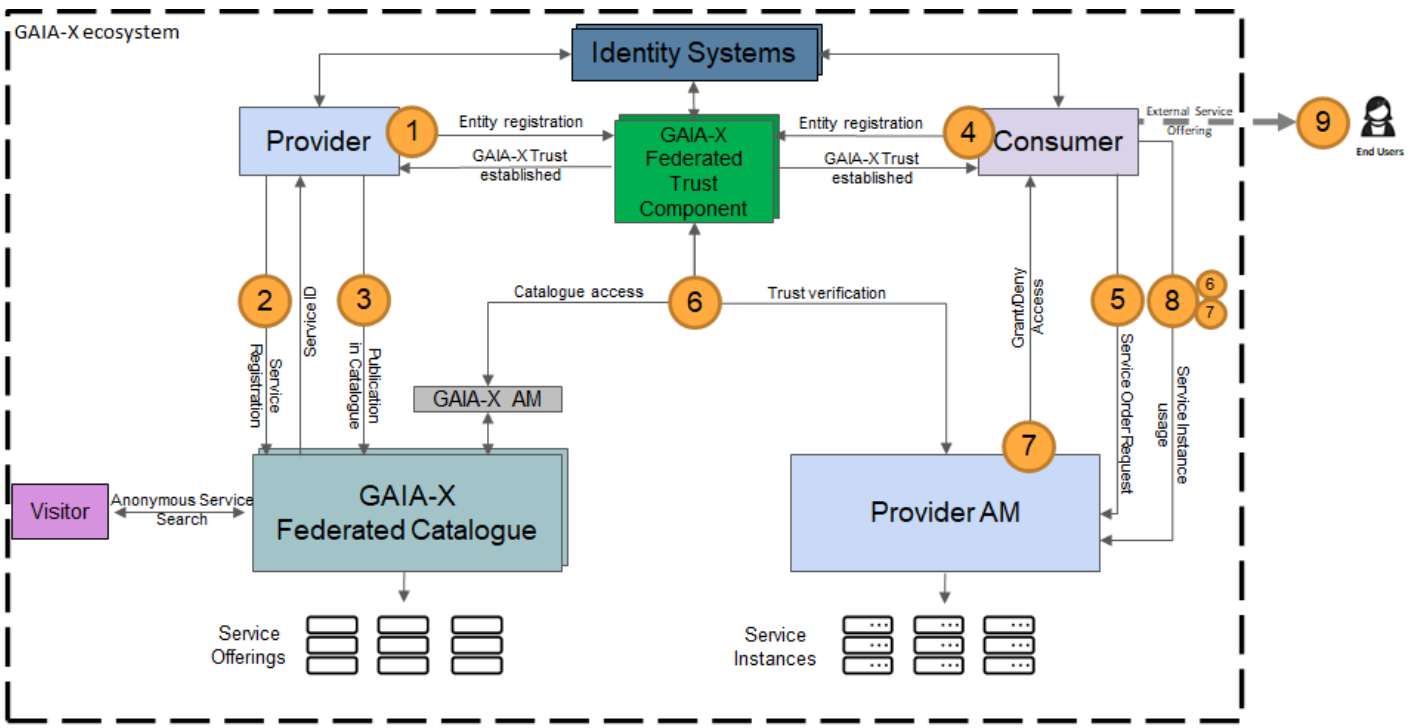
11. Appendix

11.1 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 the 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.

11.2 A2



Operational example Federated Trust Model

1. 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.
2. The Provider entity registers in Gaia-X. One of the mandatory fields is the input to the Identity System. An Identity System must confirm the Identity of the Provider.
3. 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.
4. A Consumer registers in Gaia-X. One of the mandatory fields is the input to 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.
5. The registered Consumer contacts the Service Provider to order a specific Service.
6. 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.
7. 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.
8. The Consumer is now able to use the requested 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 attributes matches the required ones (see step 6/7).
9. 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 from Gaia-X Services.

11.3 A3

This appendix presents minimal core versions of central Gaia-X concepts. That includes mandatory attributes, datatypes, and cardinalities for the core concepts of Participant, Provider, Consumer, Service Offering, Asset, Data Asset, Software Asset, Node, and Interconnection:

11.3.1 Participant

Attribute	Possible Datatype(s)	Cardinality
legal name	xsd:string	1..1
legal address	vcard:Address	1..1
web address	xsd:anyURI	1..*
contact	vcard:Agent, foaf:Person, schema:Person, ids:Person	1..*
parent_entity	gax-participant:Participant	0..1

Provider / Consumer

Same as Participant. These roles are assigned implicitly once they provide/consume at least one Asset or Service Offering.

11.3.2 Service Offering

Attribute	Possible Datatype(s)	Cardinality
name	xsd:string	1..1
description	dct:description	1..1
provided_by	gax-participant:Provider	1..*

Asset

Attribute	Possible Datatype(s)	Cardinality
name	xsd:string	1..1
description	dct:description	1..1
owned_by	foaf:Person	1..*

Data Asset / Software Asset

Data Asset and Software Asset are subclasses of Asset that do not require additional mandatory attributes.

Resource

The mandatory attributes are:

Attribute	Possible Datatype(s)	Cardinality
location	dct:location	1..1
jurisdiction	dct:location	1..1
provided_by	gax-participant:Participant	1..*

Interconnection

Interconnection is a subclass of Asset. In addition to the mandatory attributes of the Asset class, an Interconnection has the following mandatory attributes:

Attribute	Possible Datatype(s)	Cardinality
connected_node	gax-node:Node	2..*