Gaia-X Architecture Document

21.12 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 among 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 version for the Gaia-X Architecture document replaces previous version of the document.

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.

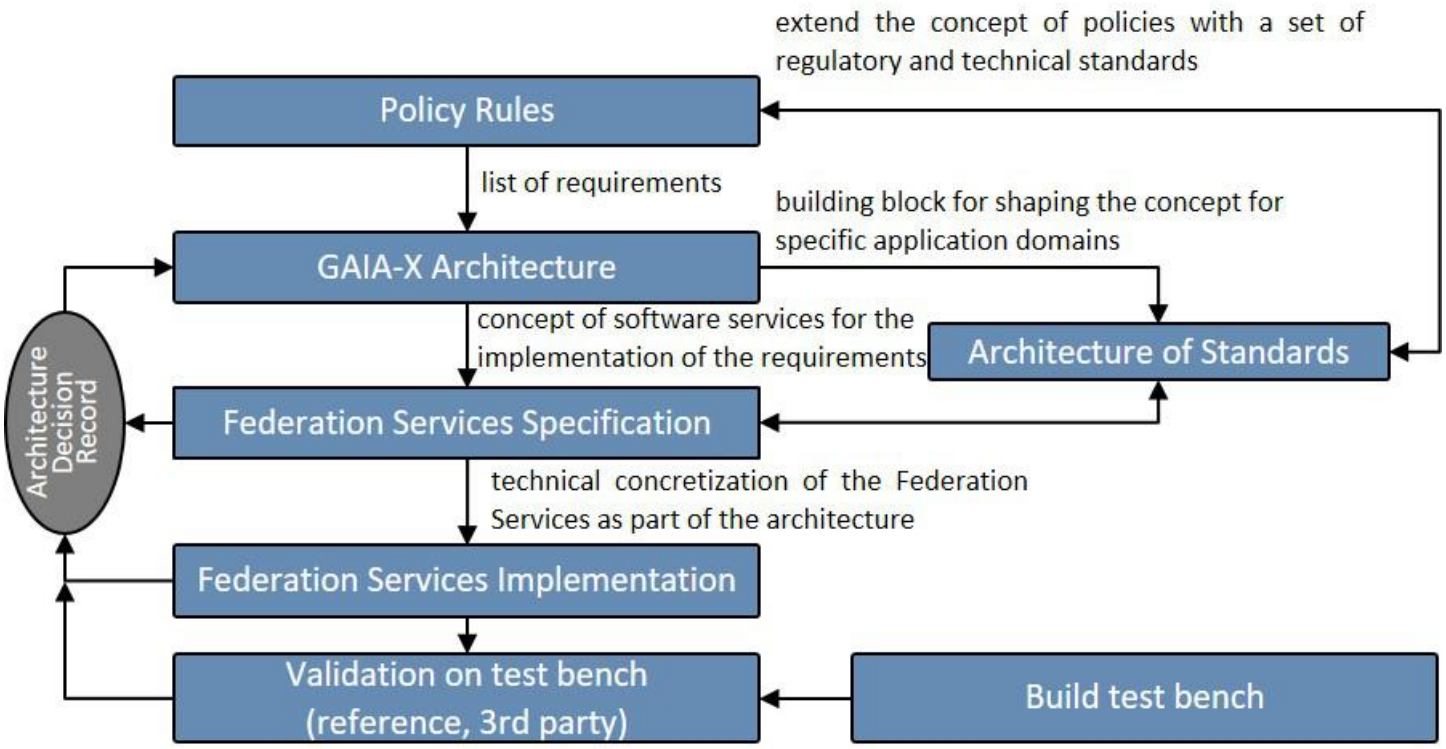


Fig: Relation to other Documents

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[3].

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[4] 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[5] compliant open source licenses[6].

---

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. 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 ↩
4. 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
5. Open Source Initiative. The Open Source Definition (Annotated). https://opensource.org/osd-annotated ↩
6. 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 described in the 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.

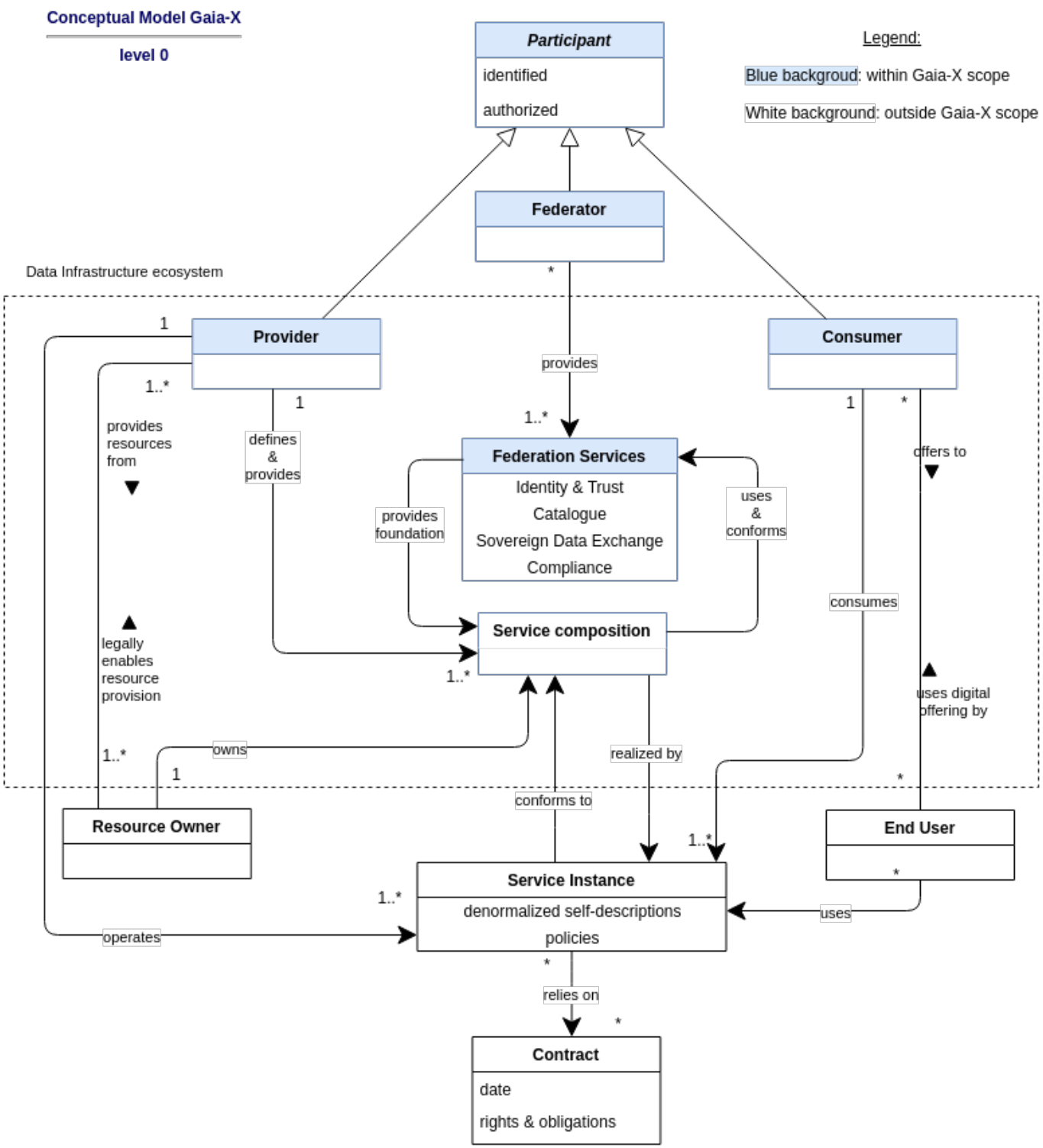


Fig: Gaia-X conceptual model

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 Resources in the Gaia-X Ecosystem. The Provider 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.

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 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 Service Composition

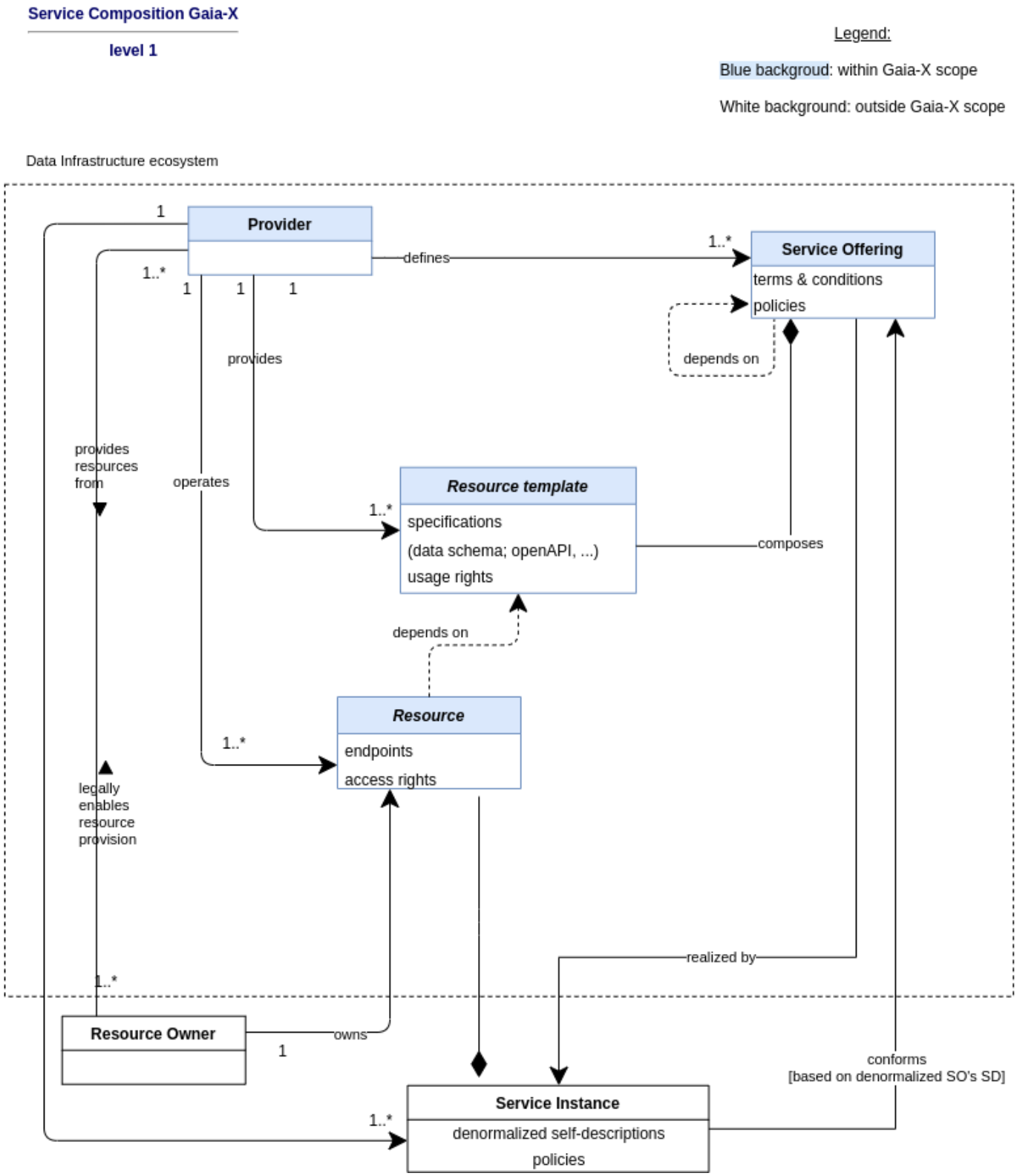
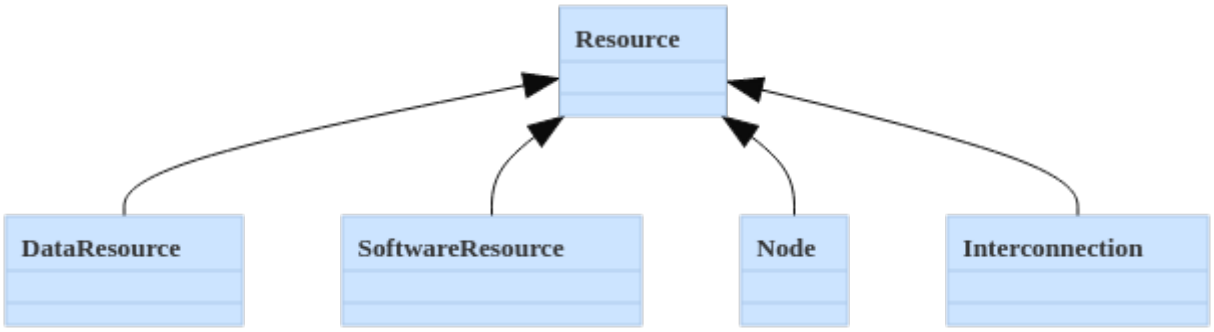


Fig: Gaia-X conceptual model

3.3 Resources and Resource Templates

Resources describe in general the goods and objects of a Gaia-X Ecosystem. A Resource can be a Data Resource, a Software Resource, a Node or an Interconnection. Each resource is characterized by endpoints and access rights and belongs to a Resource owner. The different categories of Resources are visualized in Figure 3 and defined below:



Graph: Resource Categories

A Data Resource consists of data in any form and necessary information for data sharing.

A Node is a Resource that represents a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities.

A Software Resource is a Resource consisting of non-physical functions.

An Interconnection is a Resource presenting 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.

Resource templates are the entities provided by a Provider to make the Resource available for order. They depend on the respective Resources and are characterized by a specification, e.g., of data schema, and by usage rights. Resource templates are therefore used to compose Service Offerings.

3.3.1 Policies

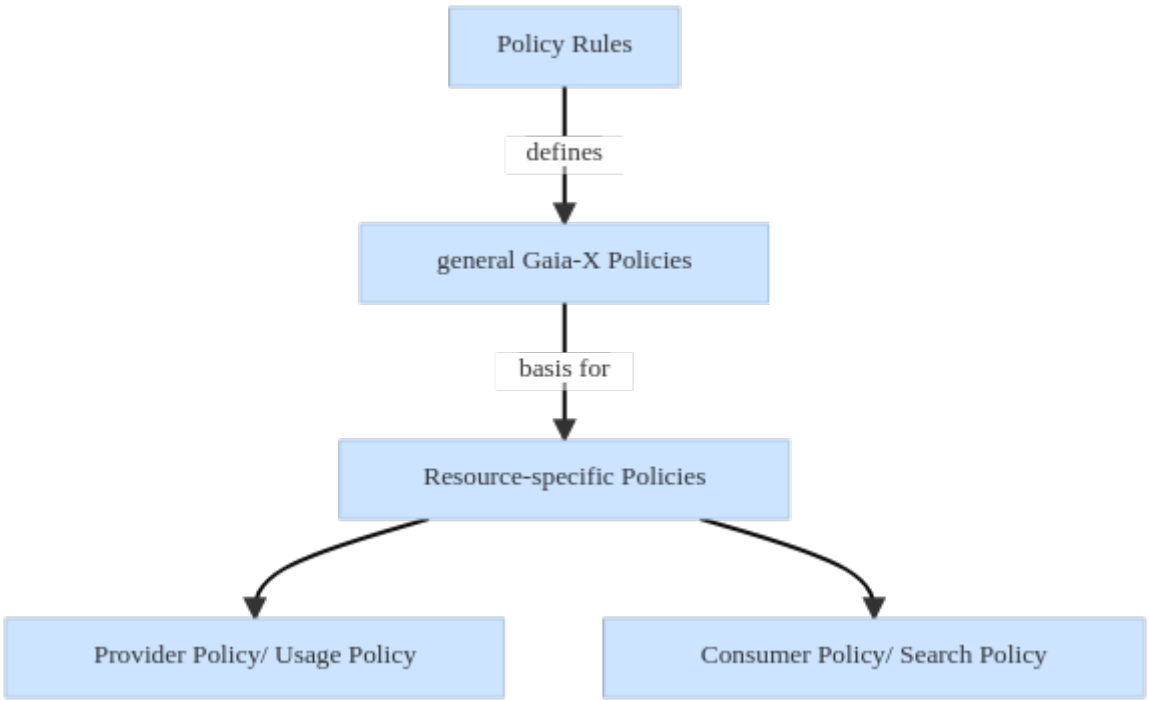
Policy is defined as a statement of objectives, rules, practices, or regulations governing the activities of Participants within Gaia-X. From a technical perspective Policies are statements, rules or assertions that specify the correct or expected behaviour of an entity[23].

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 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 a 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 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 Resources. The specific Policies have to be in line with the general Policies in the Policy Rules Document.



3.4 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 Resources, Participants and interactions between Ecosystems. The four service groups are Identity and Trust, Federated Catalogue, Sovereign Data Exchange and Compliance.

3.5 Service Offering

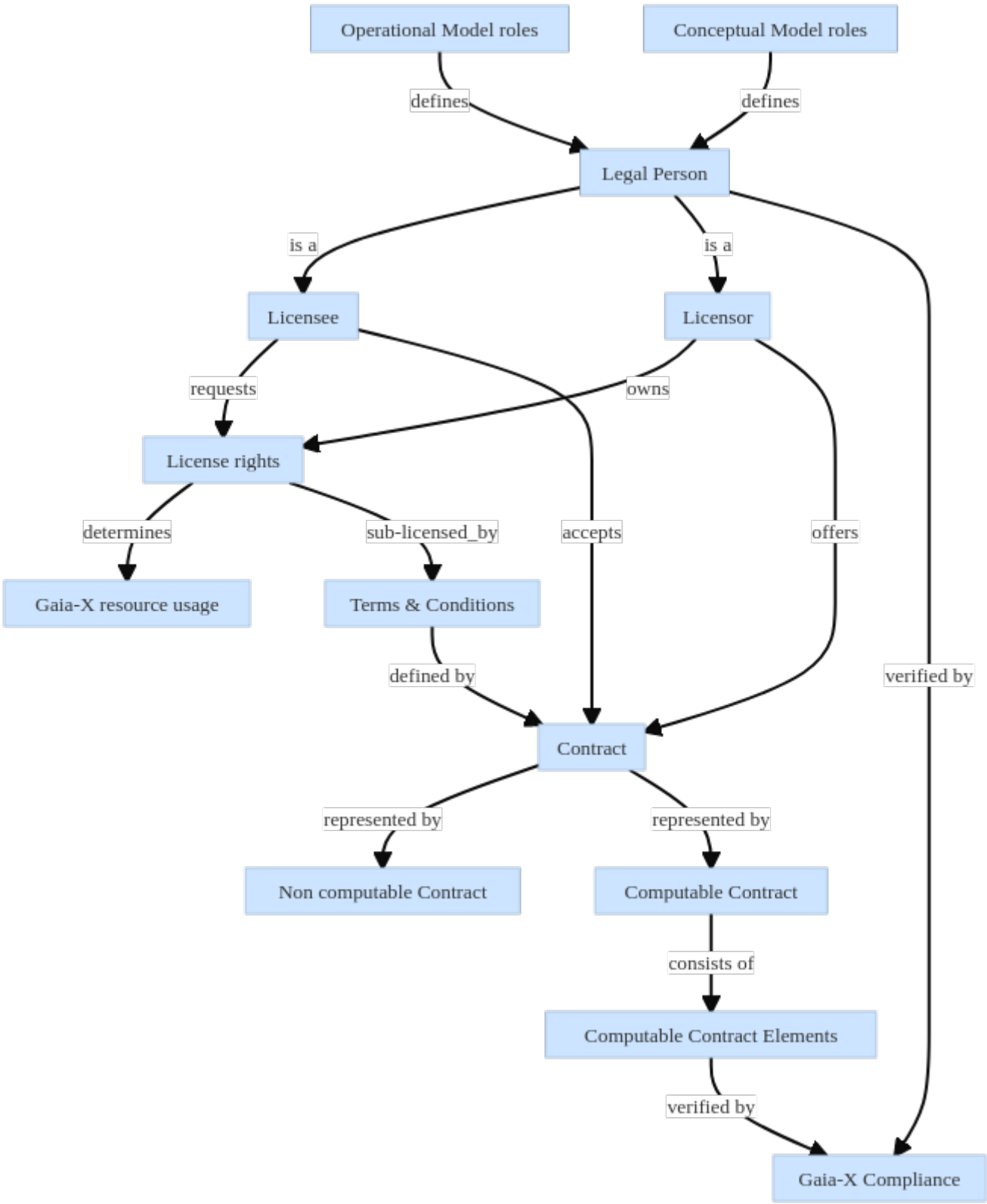
A Service Offering is defined as a set of Resources which a Provider aggregates and publishes as a single entry in a Catalogue. Service Offerings may themselves be aggregated realizing service composition. The instantiation of a Service Offering is the deliverable of a Provider to a Consumer. The Federation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

3.6 Contract

Gaia-X association is not getting involved into the realisation of the `Contact`. However, in order to ease participants with the establishement and to enter into a contractual relationship, we are defining below a common model for `Contract`.

3.6.1 Concept: Computable Contracts as a service

- Contracts are the basis for business relationships.
- Whereas a licensor has rights with respect to a resource and is willing to (sub-) license such rights by a defined set of conditions.
- Whereas a licensee would like to get license rights with respect to a resource by a defined set of conditions.
- Licensor and licensee agree on it in form of a contract.
- Every role of the GAIA-X conceptual model as well as of operational model can be seen as legal persons and therefore may have a role as a licensor or licensee or both.
- In traditional centralized driven eco-systems the platform provider which is very often the eco-system owner, defines the contractual framework and participants need to accept without any possibility for negotiation.
- In distributed and federated eco-systems individual contracting becomes much more important to support individual content of contractual relations e.g. individual set of conditions.
- The ability to negotiate on contracts is key for a sovereign participation. The ability to observe if all parties of a contract behave the way it is agreed, to validate their rights, to fulfill their obligations and ensure that no one can misuse information is key for a trustful relationship.
- Computable contracts aim to easy the complex processes of contract design, contract negotiation, contract signing, contract termination as well as to observe the fulfillment of contractual obligations and compliance with national law.



3.7 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 Resource Owners.

Resource Owners describe a natural or legal person, who holds the rights to Resources that will be provided according to Gaia-X regulations by a Provider and legally enable its provision. As Resources are bundled into a Service Offering and nested Resource compositions can be possible, there is no separate resource owner either. 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-Descriptions and Policies.

3.8 Examples

3.8.1 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 **Resource Owners** for the bank statements, which are **Resources** composing the **Service Offerings** (`Jane` is the data subject as per GDPR[4]).
The associated **Resource 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

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

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

1. The operating model must provide clear and unambiguous added value to all Participants
2. The operating model must have a transparent governance and trust model with identified accountability and liability, that is clearly and fully explained to all Participants
3. The operating model must be easy to use by all Participants
4. The operating model must be financially sustainable for the Gaia-X Ecosystem
5. The operating model must be environmentally sustainable.

The first part of this chapter introduces the Gaia-X Ecosystem(s), as well as Trust Anchors. Trust Anchors are defined, including details about who defines them and how they will be nominated.

The second part defines Gaia-X Compliance, and how to become compliant. It introduces the Gaia-X Compliance Service as well as the usage of Gaia-X Labels.

Finally, the last section will cover the Gaia-X Self-Descriptions life-cycle and the Gaia-X Registry, which provides essential support for the Gaia-X Decentralized Autonomous Ecosystem.

4.1 Gaia-X Ecosystem and Ecosystems

Gaia-X Participants may want to simultaneously provide and/or consume certain services with the greatest number of other Participants and provide and/or consume other types of services with a restricted set of Participants under custom policy rules. Furthermore, Gaia-X Participants may want to provide and/or consume certain services across ecosystems, i.e. within the Gaia-X Ecosystem. This operating model defines one global ecosystem with the possibility for Participants to create further ecosystems.

The main reasons to create an ecosystem are a combination of:

- maintenance of Self-Descriptions that are private to an Ecosystem
- usage of customs Gaia-X Compliant Trust Anchors

Gaia-X Ecosystem	Ecosystems
Self-Descriptions are public	Self-Descriptions can be kept private
Gaia-X Participants shall use Gaia-X compliant Trust Anchors	Ecosystem's Participants can use their own Trust Anchors
Gaia-X Compliance on Self-Description is mandatory	Only Self-Descriptions using Gaia-X compliant Trust Anchors are eligible to be awarded as Gaia-X compliant
Service Offerings are eligible to Gaia-X Labels	Only compliant Service Offering Self-Descriptions are eligible to Gaia-X Labels
Uses decentralized applications interoperable with the Gaia-X Federation Services	Uses compatible Gaia-X Federation Services

Examples of Ecosystems:

- Catena-X - Automotive ecosystem
- Agdatahub - Agriculture ecosystem

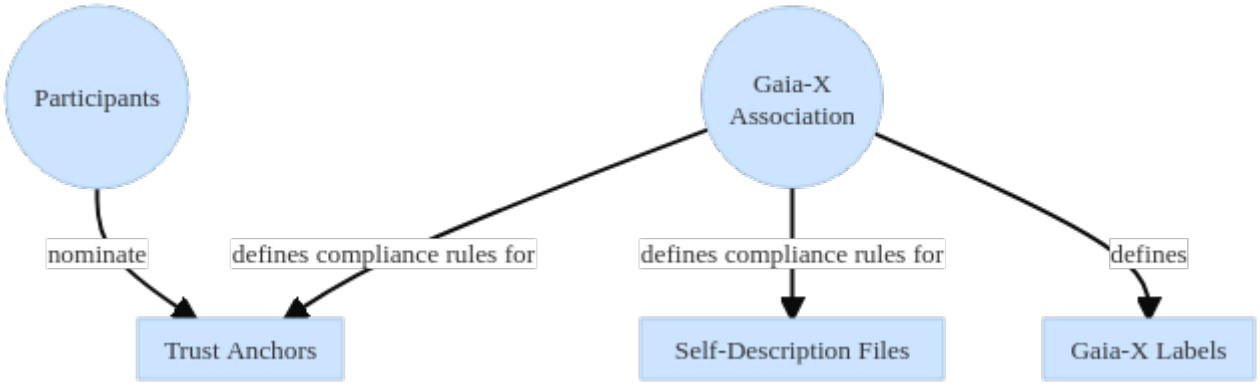
It must be noted that by default, all Service Offerings shall include a policy using Open Digital Rights Language (ODRL) to describe Permissions, Requirements and Constraints. **These rules enable Providers, Federators, Consumers to express constraints, filtered out by requirements and to enforce permissions without needing to create an ecosystem with their own Trust Anchors.**

4.2 Trust Anchors

For a given ecosystem, the Trust anchors are the entities considered by all Participants to be trustworthy when establishing the chain of cryptographic certificates.
Ecosystems can select their own Trust Anchors, however, cross ecosystem trust requires the selected Trust Anchors to comply at least with the same rules that the common Gaia-X ecosystem Trust Anchors shall comply with.

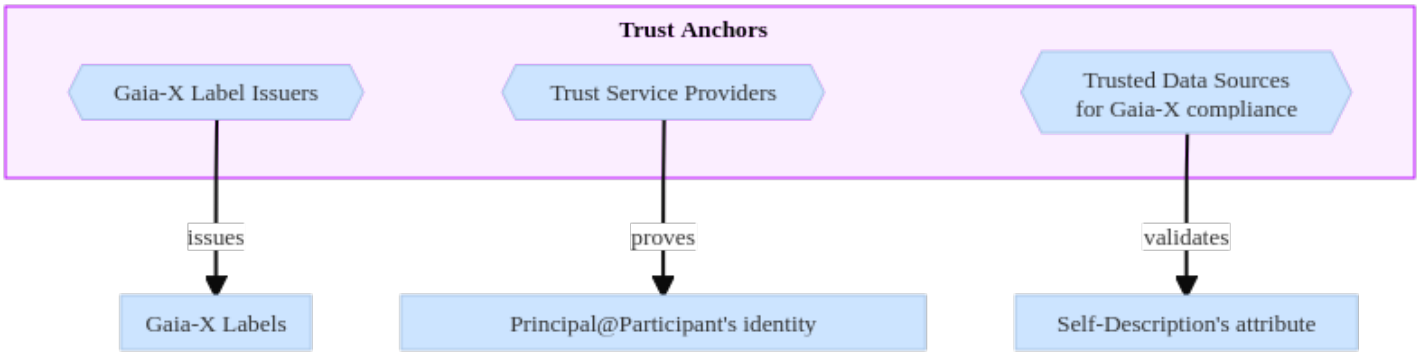
The Gaia-X Association defines:

- the sets of rules to define the Trust Anchors:
  - Trust Service Providers.
  - Gaia-X Label Issuers
  - Trusted data source for Gaia-X Compliance
- the format of the Self-Descriptions and their compliance rules
- the Gaia-X Labels rulebook.



The Trust Anchors are nominated by the Participants. The validation of the nominees is done automatically by validating the rules defined by the Gaia-X Association and supervised by the Gaia-X Association.

In turn, the Trust Anchors are used by the Participants to operate the Ecosystem(s).



Identity Providers are needed to verify a company's status and the mandate of the physical person over a company. A set of private/public keys will be issued to the company's representative and the public keys can be shared via a resolvable entry, like DKIM, DID:DNS or DID:WEB, combined with the use of Verifiable Credentials, to create the links between the identities and the services URLs.

Note: Conformance Assessment Bodies (CABs) are just a special type of Provider, providing assessment services, and are therefore considered Participants. Therefore, "Participants issuing VCs for other Participants" includes "CAB issuing VC to Providers".

4.3 Ecosystem Launching Phase

To kickstart the Gaia-X ecosystem during the initial months, the Gaia-X Association will nominate itself as a Gaia-X Label Issuer and Trust Service Provider in order to showcase and validate the operating model. This is only a short-term, temporary situation.

For the European Participants, the National and EU eIDAS Trusted Lists of Qualified Certificate for Electronic Signature are considered to be Gaia-X compliant Trust Service Providers.

4.4 Gaia-X Compliance

The Gaia-X compliance is defined as the process of going through and validating the set of automatically enforceable rules to achieve the minimum level of Self-Description compatibility in terms of:

- serialization format and syntax.
- cryptographic signature validation.
- attribute value consistency.
- attribute value verification.

Whenever possible, the verification of Self-Descriptions' attribute values is done either by using publicly available open data, and performing tests or using data from Trusted Data Sources as defined in the previous section. These catalogues can then be referred to as Trusted Gaia-X Catalogues.

Gaia-X Compliance has been referred before as Regulation by Automation.

It is important to note that this compliance is independent of the Self-Description’s attribute validation done by the Issuer as defined in the W3C Verifiable Credential.

The set of rules is versioned and will evolve over time to adapt to legal and market requirements.

One of the first Gaia-X added values is the creation of a FAIR (findable, accessible,interoperable, reusable) knowledge graph of verifiable and composable Self-Descriptions.

The rules will be implemented using open-source code and a service instance of that source code is called a Gaia-X Compliance Service.

For ecosystems, and to keep their Self-Descriptions private, the Gaia-X Compliance Service could be embedded, as a software library, into local Ecosystem catalogues. The catalogues able to provide a code attestation demonstrating the execution of the unmodified source code are referred as Trusted Gaia-X Catalogues.

4.4.1 Initial Set of Rules

Below is a non-exhaustive list of automatic checks to be performed:

- **serialization format and syntax**.
  - The Self-Description must parse as a well-formed JSON-LD. The RDF graph defined by this serialization must validate against the SHACL shapes defined by Gaia-X.
  - All European Providers shall specify their company ISO 6523 EUID as specified in the section 8 of the Commission Implementing Regulation (EU) 2015/884.
  - ...
- **cryptographic signature validation**.
  - The Service Offering Provider identity must be verified by one of the Gaia-X approved Trust Service Providers.
  - All Self-Description's mandatory attribute signatures must have at least one of the Trust Anchor as root Certificate Authority.
  - ...
- **attribute value consistency**.
  - The value of the `service.jurisdiction` attributes must be consistent with the `service.provided_by.location` attributes.
  - The value of the `service.jurisdiction` attributes must be consistent with the Governing Law from the Terms&Conditions document `service.terms_and_conditions` attributes.
  - ...
- **attribute value verification**.
  - If declared, the value of GDPR compliance must come from one of the European Data Protection Board - EDPB approved Code of Conducts, such as CISPE or EUCloudCOC.
  - If declared, the value of European Cybersecurity Certification Scheme for Cloud Services compliance must come from one of the ENISA recognized scheme such as C5 or SecNumCloud.
  - ...

4.4.2 Usage of data from Trusted Data Sources

It is expected that checking the validity of Self-Descriptions using data will introduce costs. In the context of the main Gaia-X Ecosystem, a proposal to cover the operating cost is described later in this document with the introduction of a Gaia-X Decentralized Autonomous Ecosystem.

ℹ Other ecosystems are autonomous and this operating model doesn't cover how the operating cost of ecosystems should be handled.

Example of potential data Trusted Sources: CISPE, Cloud Mercato, to be completed with a call for action from Gaia-X Association members

4.5 Gaia-X Labels

From the European Data Governance Act proposal:

> As a compulsory scheme this could generate higher costs, which could potentially have a prohibitive impact on SMEs and startups, and the market is not mature enough for a compulsory certification scheme; therefore, lower intensity regulatory intervention was identified as the preferred policy option. However, the higher intensity regulatory intervention in the form of a compulsory scheme was also identified as a feasible alternative, as it would bring significantly higher trust to the functioning of data intermediaries, and would establish clear rules for how these intermediaries are supposed to act in the European data market.

The decision for the Gaia-X Association is to adopt a compulsory scheme for Gaia-X compliance - see previous section - and an optional scheme for Gaia-X Labels, to ensure a common level of transparency and interoperability while limiting the regulatory burden on the market players.

Labels are issued for Service Offerings only and are the result of the combination of several Self-Description compliant attributes, that individually would be insufficient to support business or regulatory decisions.
The issued Labels must include a version number to allow continuous evolution of the set of rules and the precise set of rules in a “rulebook” defined by the Gaia-X Association, which must include a workflow for compliance re-validation.

From a technical point of view, a Label is a W3C Verifiable Credential, similar to Self-descriptions’ attributes credentials that are described in the next section.

The management of the rulebook and its governance is described in the Gaia-X Labels document expected in October 2021.

4.6 Gaia-X Self-Description

Gaia-X Self-Descriptions describe in a machine interpretable format any of the entities of the Gaia-X Conceptual Model.

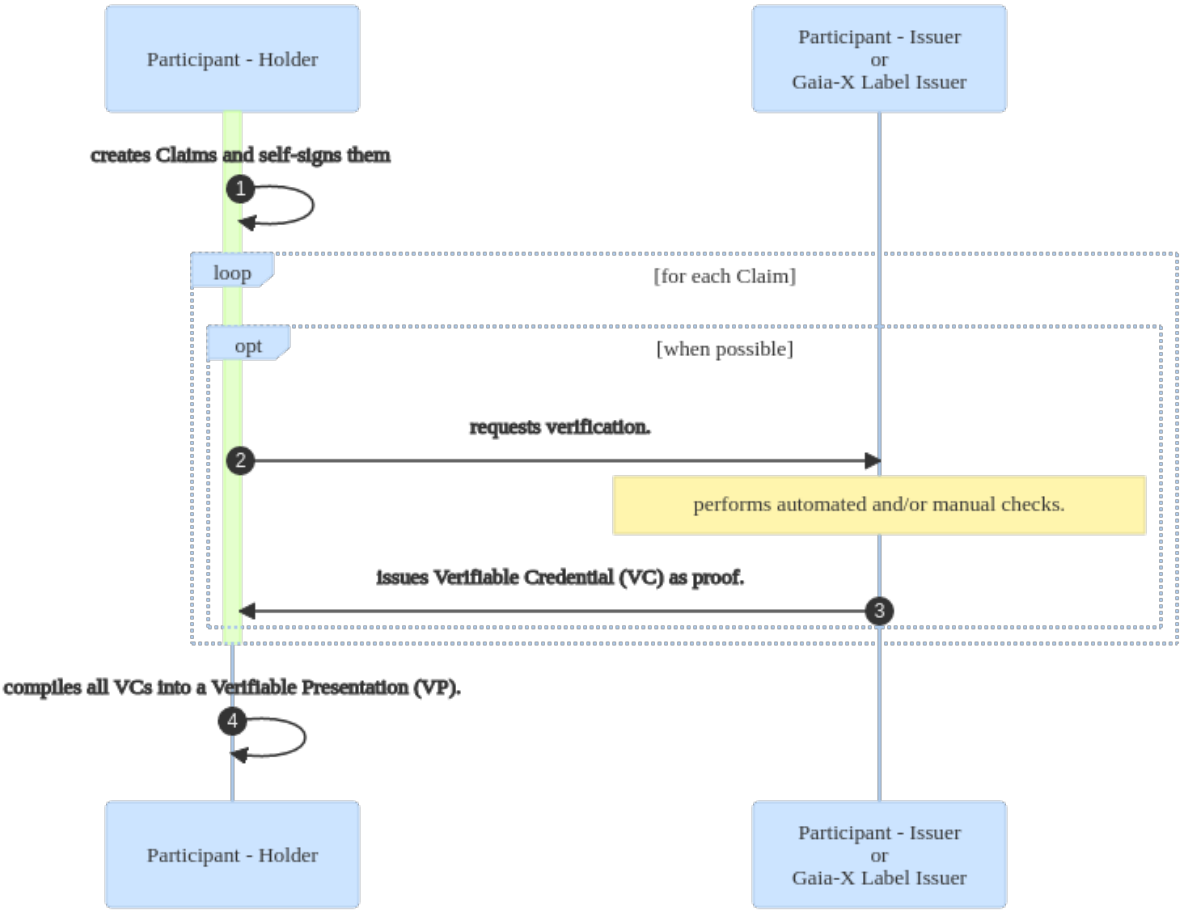
It means that there are Self-Descriptions for all Participant's Roles: `Consumer`, `Federator`, `Provider` and all the other entities in an Ecosystem's scope such as `Resource` and `Service Offering`.

Each Gaia-X entity makes Claims, which are validated and signed by 3rd parties. Those signed Claims are defined as Verifiable Credentials and presented by the entity as Verifiable Presentations.

Technically speaking, Self-Descriptions are W3C Verifiable Presentations in the JSON-LD serialization of the RDF graph data model.

The following workflow describes how Gaia-X Self-Descriptions are created following the vocabulary of the W3C Verifiable Credentials Data Model standard.

W3C Term	Example with a car
Claim	My car is red
Verifiable Credential	The garage's attestation that my car is red
Verifiable Presentation	Me showing to my friend the garage's attestation that my car is red
Issuer	The garage
Holder	Myself
Verifier	My friends



4.6.1 Difference between Self-Description’s proofs (VC), Gaia-X Compliance and Gaia-X Labels.

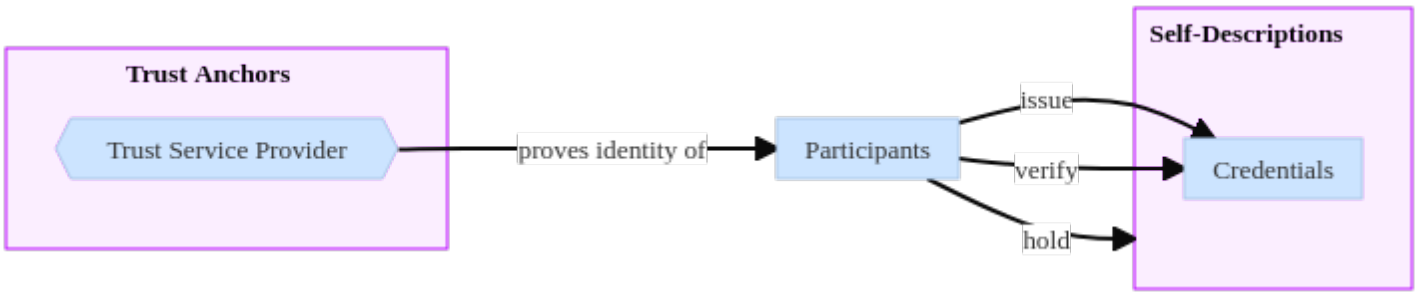
The Verifiable Credentials are issued by other Participants, including Conformity Assessment Bodies. Verifiable Credentials can also be used to build a reputation system in the knowledge graph.

The Gaia-X Compliance insures that the required level of information for the users to take educated decisions is available and the information is verified or verifiable.

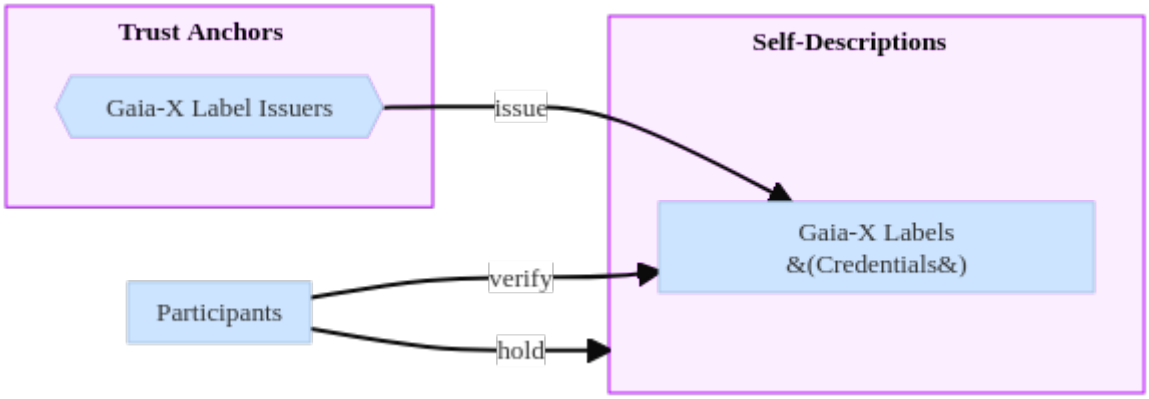
The Gaia-X Labels set thresholds for specific industries, markets or regulated activities.

	Attribute’s Verifiable Credentials	**Gaia-X Compliance**	**Gaia-X Labels**
Technical implementation	W3C Verifiable Credentials	W3C Verifiable Credentials	W3C Verifiable Credentials
Credential Issuer	Any Gaia-X Participant	Gaia-X Compliance Service	Gaia-X Label Issuer
Application scope	All Self-Descriptions	All Self-Descriptions	Service Offerings
Assessment method(s)	Manual or Automated	Fully automated	Manual or Automated
Issuance’s temporality	Frequent updates	Frequent updates	Slow updates (~yearly)

A attribute’s Verifiable Credential is Gaia-X conformant if the Issuer of the Verifiable Credential has itself an identity coming from one of the Trust Anchors.



A Label is Gaia-X conformant if the Issuer of the Credential is one of the Trust Anchors’ Gaia-X Label Issuers.

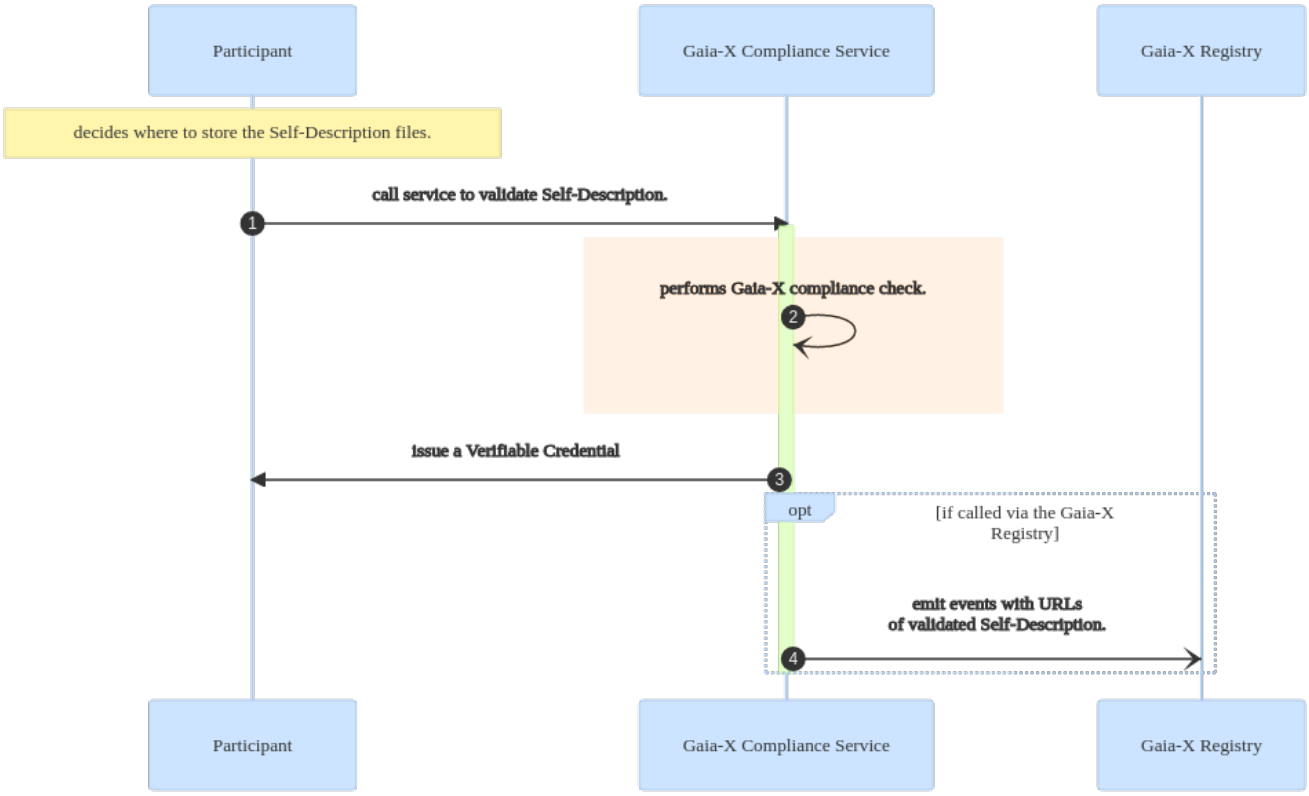


4.6.2 Self-Description compliance

A Self-Description qualified as Gaia-X compliant must be submitted to a Gaia-X Compliance Service instance as defined in the section above.

The result of that submission is captured in two ways:

- as a Verifiable Credential: If the compliance is validated, the Gaia-X Compliance Service issues a Verifiable Credential that can later be inserted into the Self-Description. This method aligns with the self sovereign principle of the holder being in charge of the information.
- If the Gaia-X Compliance Service is called via the Gaia-X Registry, the Gaia-X Registry will emit an event to synchronize Catalogues. The event contains the URL the of the Self-Description file. The Gaia-X Registry is defined in the next section.



4.6.3 Self-Description Remediation

Self-Descriptions may become invalid over time. The Chapter Federated Catalogue section Self-Description describes three states declaring a Self-Description as invalid:

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

End-of-Life and Deprecated can be deduced automatically based in the information already stored in the Gaia-X Registry or Gaia-X Catalogues. There are no additional processes to define. This section describes how Self-Descriptions are revoked.

The importance of Gaia-X compliance will grow over time, covering more and more Gaia-X principles such as interoperability, portability, and security. However, automation alone is not enough and the operating model must include a mechanism to demotivate malicious actors to corrupt the Registry and Catalogues.

The revocation of Self-Descriptions can be done in various ways:

- **Revocation or Deprecation by authorship**: The author of a Self-Description revokes or deprecates the Self-Description explicitly.
- **Revocation by automation**: The Gaia-X Compliance Service found at least one self-described attribute not validating the compliance rules.
- **Suspension and Revocation by manual decision**: After an audit by a compliant Gaia-X Participant, if at least one self-described attribute is found to be incorrect, the suspension of the Self-Descriptions is automatic. The revocation is submitted for approval to the Gaia-X Association with the opportunity for the Self-Description's owner to state its views in a matter of days. To minimize subjective decisions and promote transparency, the voting results will be visible and stored on the Gaia-X Registry or in local Ecosystem's Registry.

4.7 Gaia-X Decentralized Autonomous Ecosystem

The operating model described in this chapter motivates the creation of a Gaia-X decentralized autonomous Ecosystem following the principles of a Decentralized Autonomous Organisation[1], with the following characteristics:

- Compliance is achieved through a set of automatically enforceable rules whose goal is to incentivize its community members to achieve a shared common mission.
- Maximizing the decentralization at all levels to reduce lock-in and lock-out effects.
- Minimizing the governance and central leadership to minimize liability exposure and regulatory capture.
- The ecosystem has its own rules, including management of its own funds.
- The ecosystem is operated by the ecosystem's Participants

ℹ Other ecosystems are autonomous and this operating model does not enforce how internal ecosystem governance should be handled.

4.7.1 Gaia-X Registry

The Gaia-X Registry is a public distributed, non-reputable, immutable, permissionless database with a decentralized infrastructure and the capacity to automate code execution.

ℹ The Ecosystems may want to have their own instance of a local Gaia-X Registry or equivalent. Technically, this component can be part of the ecosystem local Catalogues.

The Gaia-X Registry is the backbone of the ecosystem governance which stores information, similarly to the Official Journal of the European Union, such as:

- the nominations of the Trust Anchors
- the result of the Trust Anchors validation processes.
- the potential revocation of Trust Anchors identity.
- the vote and results of the Gaia-X Association roll call vote, similar to the rules of the plenary of the European Parliament
- the URLs of the Self-Description Schemas defined by Gaia-X
- the URLs of Catalogue's Self-Descriptions
- ...

It also facilitates the provision of:

1. A decentralized network with smart contract functionality.
2. Voting mechanisms that ensure integrity, non-repudiation and confidentiality.
3. Access to a Gaia-X Compliance Service instance.
4. A fully operational, decentralized and easily searchable catalogue[2].
5. A list of Participants' identities and Self-Description URIs which violate Gaia-X membership rules. This list must be used by all Gaia-X Trusted Catalogue providers to filter out any inappropriate content.
6. Tokens to cover the operating cost of the Gaia-X Ecosystem. This specific point can be abstracted by 3rd party brokers wrapping token usage with fiat currency, providing opportunities for new services to be created by the Participants. Emitting tokens for the Gaia-X Association's members is also considered. A first version of the Gaia-X Business Model will be released in Q4 2021.

Each entry in the Gaia-X Registry is considered as a transaction. A transaction contains DIDs of all actors involved in the transaction and metadata about the transaction in a machine readable format. The basic rule for a transaction to be valid is that all DIDs have one of the Trust Anchors as root Certificate Authorities. Please also note that the Registry stores all revoked Trust Anchors.

This model enables the Participants to operate in the Gaia-X ecosystem, to autonomously register information, and to access the information which is verifiable by other Participants.

4.7.2 Ecosystem launching phase

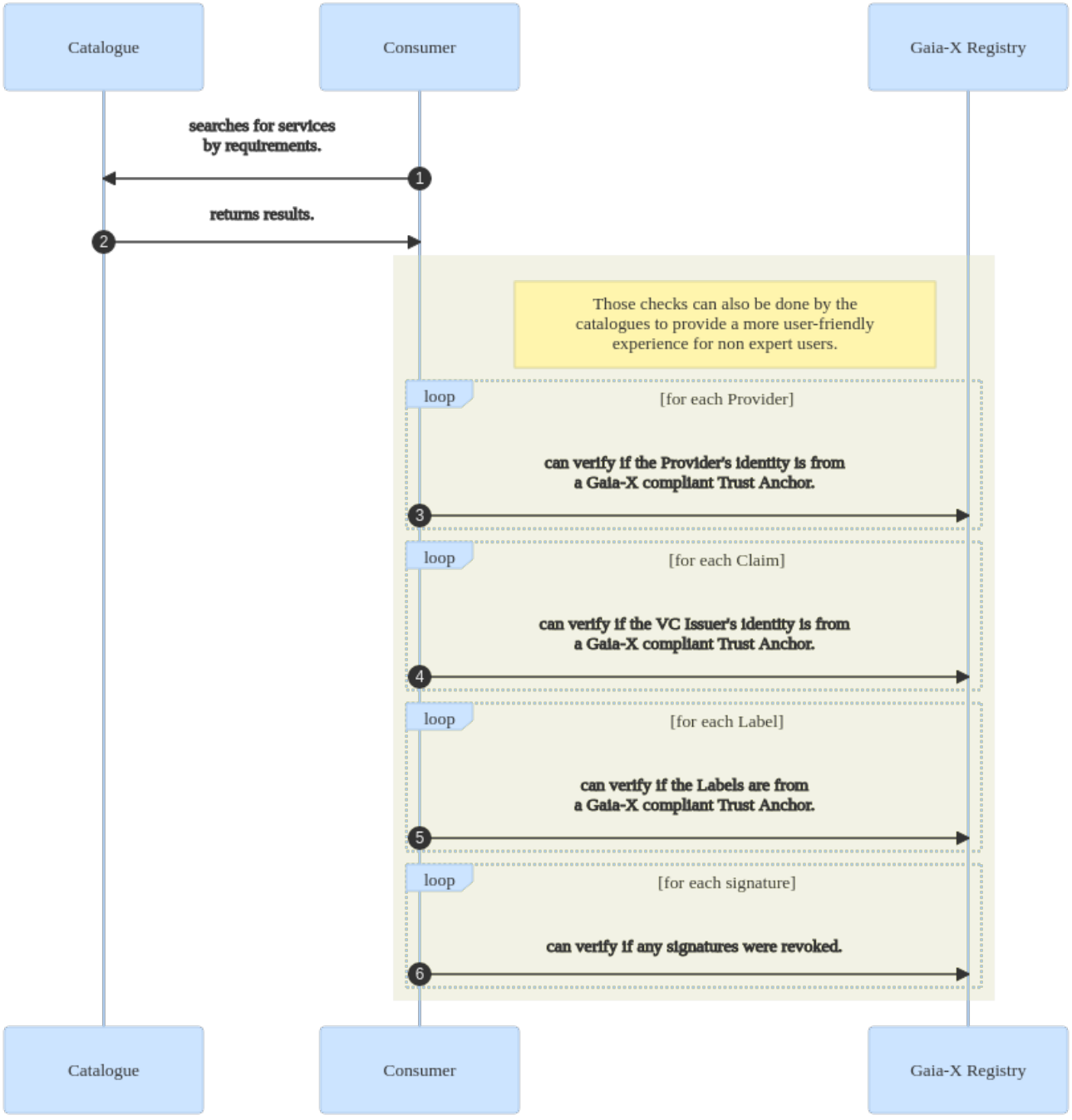
In order to enable the 1st scenario which is:

> As a Gaia-X Provider, I want to publish the self-description of my Service Offerings and I want my Service Offerings to be made available to all Ecosystems.

and until the inter-catalogue synchronization is documented, the Registry will also be used to store, directly or indirectly via an external storage, the Self-Descriptions' URLs.

4.7.3 Verifiable Presentation Verification

The Gaia-X Registry, or a private one, independently of its implementation, is the single source of truth for the Ecosystem.
It allows any `Participant` to verify the validity of signatures.



Graph: Example with `Consumer` and main `Gaia-X Registry`

1. Example of the setup of a DAO https://blockchainhub.net/dao-decentralized-autonomous-organization/ ↩
2. Example of decentralized data and algorithms marketplace https://oceanprotocol.com/ ↩

5. Federation Services

Federation Services are necessary to enable a Federation of infrastructure and data, provided through an open source reference implementation. This will open up technology wherever possible, 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 the section Gaia-X Ecosystems, with an overview shown in the figure below.

- The Federated Catalogue constitutes an indexed repository of Gaia-X Self-Descriptions to enable the discovery and selection of Providers and their Service Offerings. The Self-Descriptions are the properties and Claims of Participants and Resources, representing key elements of transparency and trust in Gaia-X.
- Identity and Trust covers identification, authentication and authorization, credential 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 within the Self-Descriptions.
- Compliance includes mechanisms to ensure that Participants adhere 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.

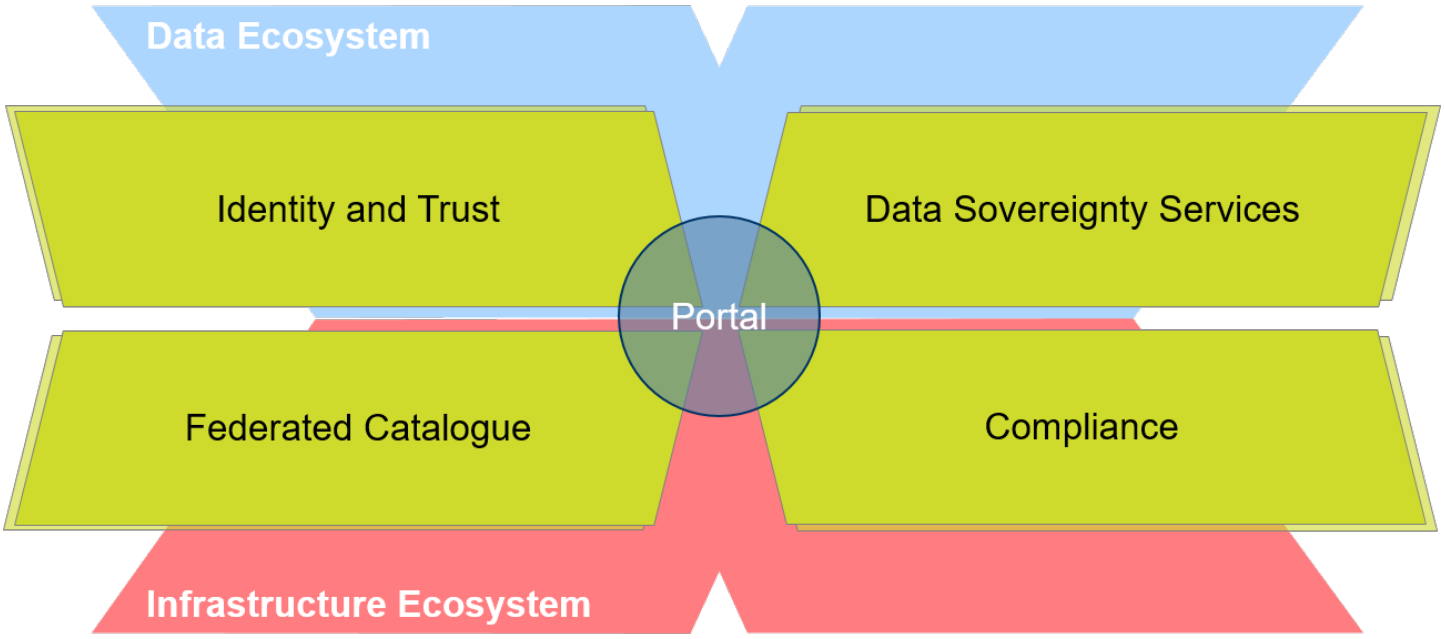


Fig: Gaia-X Federation Services and Portal as covered in the Architecture Document

5.1 Federated Catalogue

Self-Descriptions intended for public usage can be published in a Catalogue. There, they can be found by potential Consumers. Further, they form the starting point for building specific decentralized Catalogues. 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 Provider registers Self-Descriptions with their universally resolvable Identifiers in the desired Catalogue to make them public. The Catalogue's Self-Description Storage caches copies of the raw content of any such individual Self-Description. The content is an RDF graph serialized in JSON-LD, which includes Claim statements as specified below. All individual Self-Descriptions are aggregated into one overall Self-Description Graph. This is because individual Self-Descriptions can reference each other. The Self-Description Graph is the basis for advanced query mechanisms that consider the references between and among Self-Descriptions.

The system of Federated Catalogues includes 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.

In addition to Self-Descriptions, a Federated Catalogue also manages Self-Description Schemas. A Federated Catalogue should only accept the submission of Self-Descriptions that validate against a Schema known to the Catalogue, as specified below. Gaia-X develops an extensible hierarchy of Schemas that define the terms used in Self-Descriptions. Some Schemas are standardized by the Gaia-X AISBL and must be supported by any Catalogue. It is possible to create additional Schemas specific to an application domain, an Ecosystem, Participants in it, or Resources offered by these Participants. Schemas have the same format as Self-Descriptions, i.e., they are graphs in the RDF data model, serialized as JSON-LD. A Schema may define terms (classes, their attributes, and their relationships to other classes) in an ontology. If it does, it must also define shapes to validate instances of the Ontology against.

The system of Federated Catalogues comprises of top-level decentralized Catalogues 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 through inter-Catalogue synchronization functions.

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 are allowed. All states are listed below:

- 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, as well as the Schemas used by these Self-Descriptions. 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.

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 Self-Descriptions they want to share with a public Catalogue and which ones they only want to share privately. Options for private sharing include private Catalogues as well as channels external to Gaia-X, such as encrypted email.

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 Resource templates, Resources, Service Offerings and Participants and are tied to their respective Identifier. Providers are responsible for the creation of their Self-Descriptions. 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 Resources, 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:

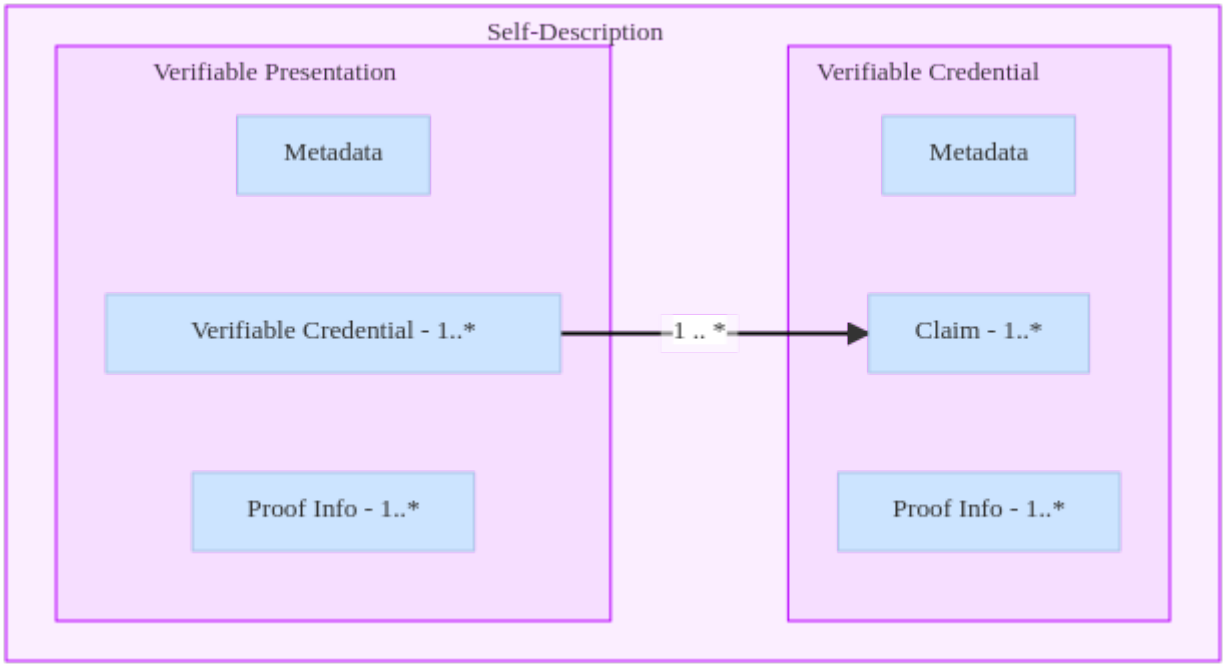
- Discovery and composition of Service Offerings in a Catalogue
- Tool-assisted evaluation, selection, integration and orchestration of Service Instances and Resources
- Enforcement, continuous validation and trust monitoring together with Usage Policies
- Negotiation of contractual terms concerning 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 Schema with an expressive semantics (ontology) and validation rules (shapes)
- 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 referenceable 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

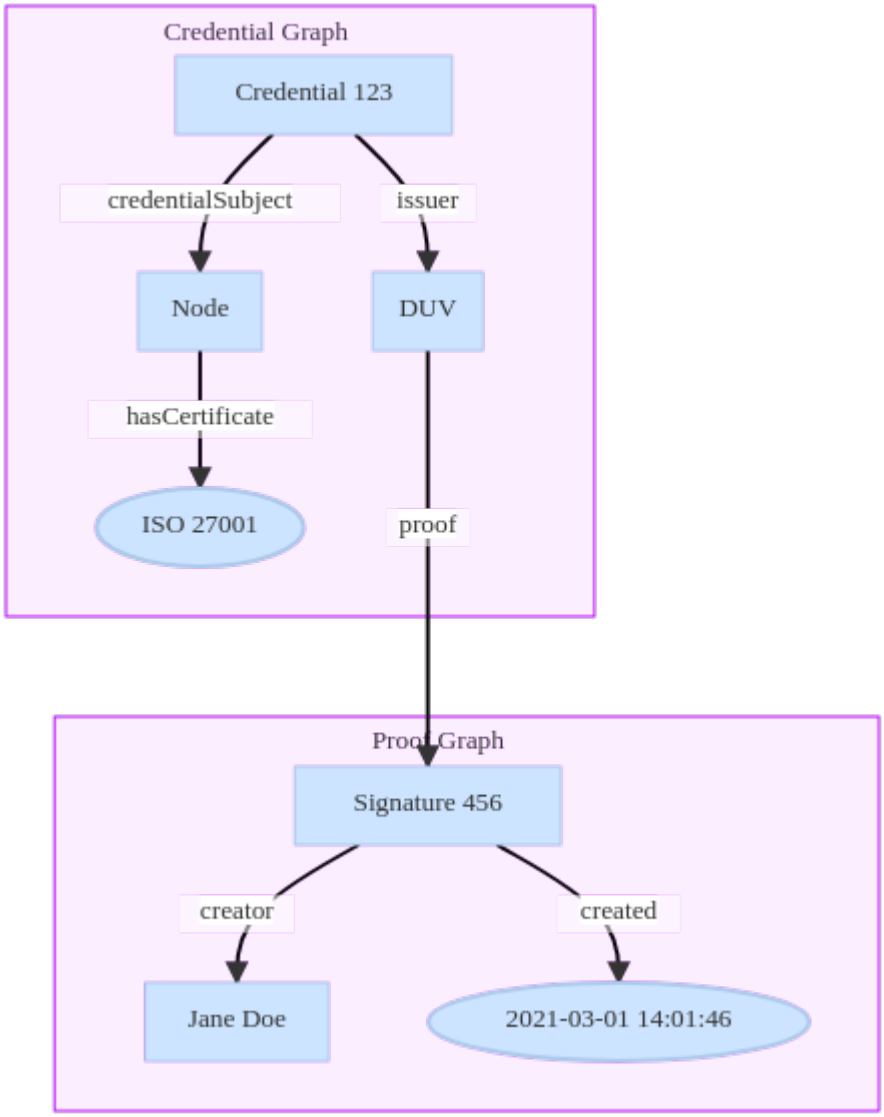
The exchange format for Self-Descriptions is JSON-LD. JSON-LD uses JSON encoding to represent subject-predicate-object triples according to the W3C Resource Description Framework (RDF).

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-predicate-object structure of the data model. The W3C Verifiable Credentials Data Model[1] is the technical standard to express Credentials and Claims using JSON-LD[2]. When there exist multiple Credentials for the thing that is being self-described, e.g., Credentials issued and signed by Providers themselves, plus other Credentials such as Certifications provided by independent external bodies, they may be bundled into a Verifiable Presentation. This most general case of a Self-Description is presented in the figure below.



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 Resources (subjects). 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 are defined. They introduce classes, i.e., sets of instances of the same type, which may form an extensible hierarchy. For each class, properties are defined that an instance of the class can have. These include attributes, having immediate literal values of some datatype (called “datatype properties” in the W3C Web Ontology Language OWL[3]), values that are instances of auxiliary classes (e.g., a class that groups all information related to the deployment of a Service as a distinct node in the graph), or reusable values that are instances of concepts from controlled vocabularies (the latter two being called “object properties” in OWL). Properties also include relationships, having values that are instances of some other class in the Gaia-X Conceptual model (e.g., the relationship between an Asset and its Provider, also OWL object properties). Self-Description Schemas should include shapes[4], i.e., sets of conditions used to validate whether a Self-Description has instantiated classes and properties according to their definition. In particular, shapes should specify which properties are mandatory to be used by every instance of a given class, and which ones are optional. A Self-Description has to state which schemas are used in its metadata. Only properties and relations defined in these schemas must be used.

The Gaia-X Federation Services specification describes how core Self-Description schemas based on the Conceptual Model are created and maintained. Individual Gaia-X Ecosystems can extend the schema hierarchy for their application domain.[5] Such extensions must make an explicit reference to the organization that is responsible for the development and maintenance of the extension.

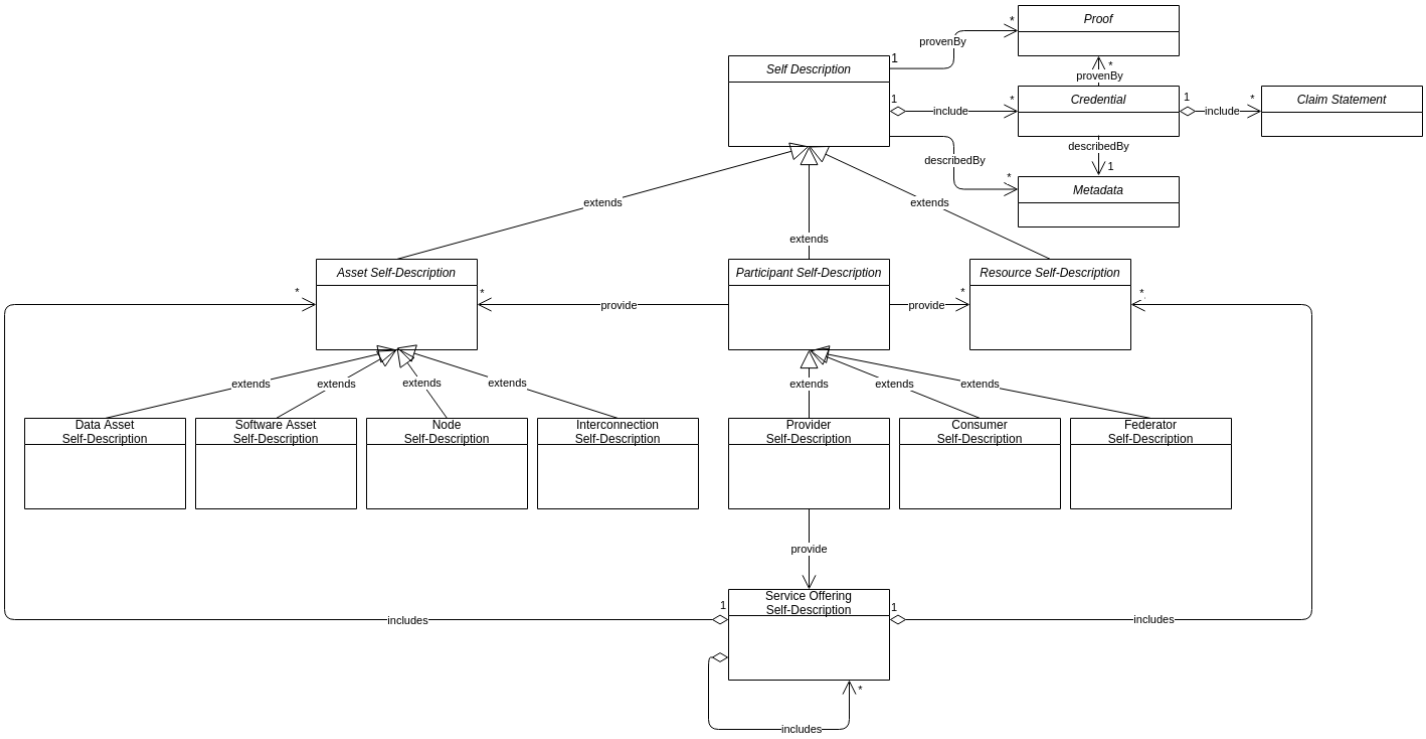


Fig: Schematic inheritance relations and properties for the top-level Self-Description

The Self-Description Schemas can follow the Linked Data best practices[6] which makes the W3C Semantic Web family[7] 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[8] 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,

.

For frequently used attribute values, it is recommended that they be maintained in the same governed process as Self-Description Schemas, i.e., by giving them unambiguous identifiers maintained in Controlled Vocabularies. Examples include standards against which a Participant or an Asset has been certified, or classification schemes, e.g., for the sector in which a Provider is doing their business.[9] It is recommended to reuse Controlled Vocabularies where they already exist, e.g., ECLASS to identify products and services. The W3C SKOS Simple Knowledge Organization System provides a way of managing Controlled Vocabularies in a way that is compatible with the RDF data model and thus with Self-Description Schemas.[10]

5.2 Identity and Trust

Identities, which are used to gain access to the Ecosystem, rely on unique Identifiers and a list of dependent 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 Participants or Resources - is established by cryptographically verifying Identities using the Federated Trust Model of Gaia-X, which is a component that guarantees proof of identity 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 digital representation of a natural person, acting on behalf of a Participant, is referred to as a Principal. As Participants need to trust other Participants and Service Offerings provided, it is important that the Gaia-X Federated Trust

Model provides transparency for everyone. Therefore, proper lifecycle management is required, covering Identity onboarding, maintaining, and offboarding. The table below shows the Participant Lifecycle Process.

Lifecycle Activity	Description
Onboarding	The accredited Conformity Assessment Bodies (CAB) of a Gaia-X Ecosystem, validates and signs the Self-Description provided by a Visitor (the future Participant/Principal).
Maintaining	Trust related changes to the Self-Descriptions are recorded in a new version and validated and signed by the relevant CAB. This includes information controlled by the Participant/Principal.
Offboarding	The offboarding 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 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 Document v1.2[11].

A ‘Secure Digital Identity’ is a unique Identity with additional data for robustly trustworthy authentication of the entity (i.e. with appropriate measures to prevent impersonation) This implies that Gaia-X Participants can self-issue Identifiers for such Identities. 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[12].

5.2.1 Trust Framework

A Trust Framework is required for the Gaia-X Participants to create mutual trust between and among peers and foster Service Offerings to be provided and consumed.

This Trust framework is not enforced by the Gaia-X Association, however, only Gaia-X Participants following the policies, technical specifications, and interoperability criteria set up by the Gaia-X Association could have their Service Offerings awarded with Gaia-X Labels.

Gaia-X Association focuses on defining the policies which consider EU regulations and open technical means to provide a transparent model supporting privacy and self-determination of all Ecosystems. The chain of trust, without the need for a global and traceable unique ID across Gaia-X is needed.

Once the Trust Framework model is in place, the Gaia-X Participants can vote and elect their own trust anchors following the rules put in place by the Association. For example, the Gaia-X Ecosystem's Participants could agree to use the EU list of eIDAS Trusted Lists[13] as one of the trust anchors for service providers and Conformity Assessment Bodies.

This model allows specific Gaia-X Ecosystems to set up their own trust anchors and Federators as long as those are following the rules defined by the Gaia-X Association. Inter-ecosystem interoperability is achieved by leveraging common GAIA-X technology while having members join each specific Federation under its own rules. In such a 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 on the Participant level, which in turn connects to the organization's Identity System on the Principal level. The trust-related part is vetted according to Gaia-X Policy and electronically signed by a CAB. Possible further changes regarding the trust related information leads to a re-verification. The Gaia-X Association in turn provides a Gaia-X Registry, which lists its policies, schemas and commonly accepted trust providers's Identities 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 Identity and Access Management approach relies on a two-tiered approach which is currently work in progress and will be part of the next release of this document.

In practice, this means that Participants use a selected few Identity Systems for mutual identification and trust establishment, SSI being the recommended option for interoperability. After trust is established, underlying existing technologies already in use by Participants (on the “Principal level”) can be federated and reused, for example Open ID Connect or domain specific x509-based communication protocols.

Gaia-X Participants 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.

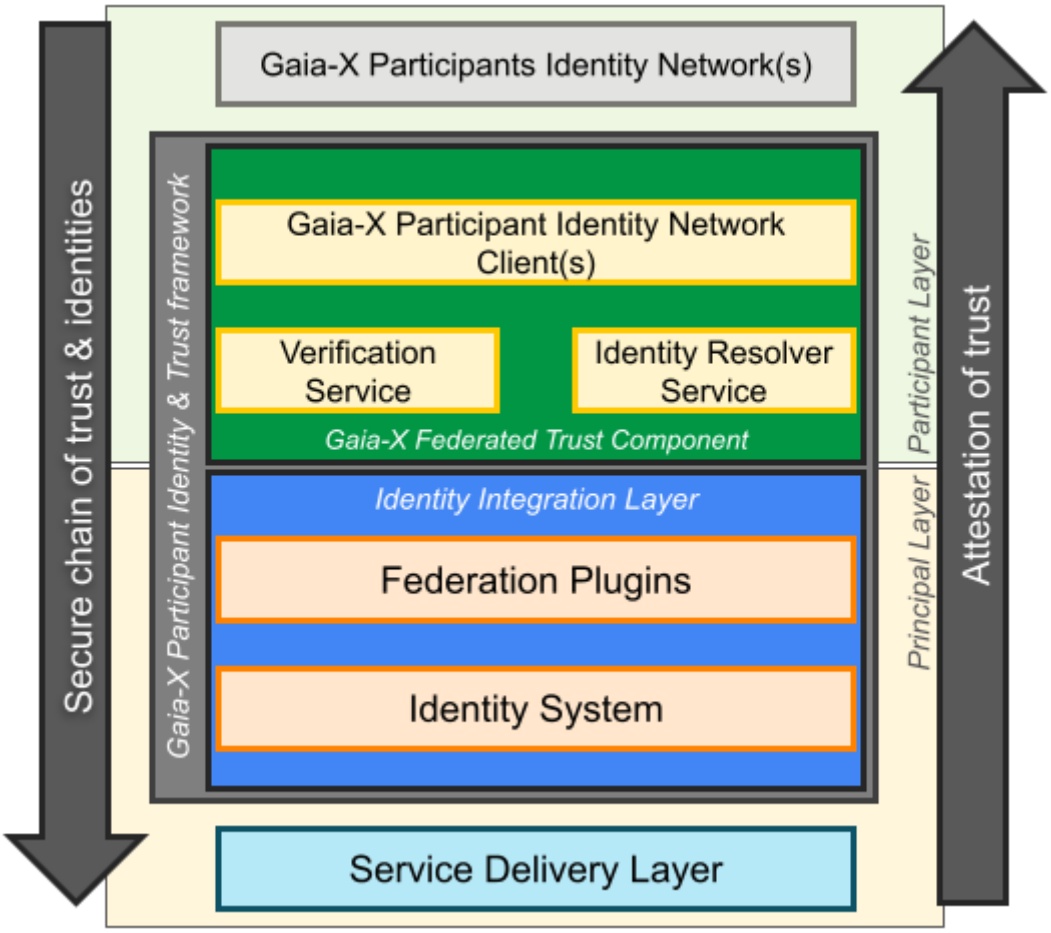
Federated Trust Model

The Federated Trust Model relies on the Gaia-X Federated Trust Component, which queries and verifies trust related information (like Gaia-X Labels, domain specific certifications) of Participants to determine whether they meet other Participants’ respective trust requirements.

This chapter describes the components required to provide an attested secure chain of trust & identities. Service implementations and the corresponding service delivery layer may include End-User services, distributed microservice architectures across multiple Participant domains, and/or cross domain data or digital service delivery

Architecture principles for this approach

Mutual trust based on mutually verifiable Participant identities between contracting parties, Provider and Consumer, is fundamental to federating trust and identities in the Principal layer. Heterogeneous ecosystems across multiple identity networks in the Participant layer must be supported as well as heterogeneous environments implementing multiple identity system standards. The high degree of standardization of Participant layer and Principal layer building blocks of the Gaia-X Federated Trust framework must ensure that there is no lock-in to any implementation of identity network and Identity System likewise.



Chain of trust and identity

The Gaia-X Participant Identity & Trust framework delivers a secure chain of trust and identities to the service delivery layer.

Mutual participant verification In the Participant layer, the Gaia-X Federated Trust Component implements the functionality to resolve and verify the Participant identity of the contracting parties. The Consumer verifies the Provider identity, the Provider verifies the Consumer identity. Successful mutual Participant verification results in a verified Participant Token representing the trust between Provider and Consumer.

Identity System federation

In the Principal layer, the Federation Plugin implements the functionality to federate trust between the Identity Systems of the contracting Participants based on the successful mutual Participant verification described above. The federation of trust between the identity systems is based on the identity system standard implemented for the service delivery layer. Required for the federation is a secure mutual

exchange of the required federation metadata. This exchange must be secured based on the Verified Participant Token. Exemplary Identity Systems standards supporting federation are: OIDC/OAuth2 (draft), SAML, SPIFFE/SPIRE. Identity System federation may also include federating the trust between certificate authorities supporting X.509 for Principals.

Identification and Authentication

Once successfully federated, the Identity Systems are enabled to identify and authenticate the Principals in the service delivery layer of the contracting parties. Federated Principal identities are mutually trusted based on the federation of the Identity Systems of the contracting Participants.

Attestation of trust

In addition to providing a secure chain of trust and identity, the Gaia-X Federated Trust framework attests the chain trust from service delivery layer to the Participant identity. The attestation may include according to required trust policies of the service delivery: * resolving the Participant identity * checking the Tags of the Participant identity * attesting the mutual Participant verification * attesting the exchanged federation metadata

Integration of the framework

The Gaia-X Federated Trust framework is in essence agnostic to implementations of identity network, verification method as well as identity system standard.

Gaia-X Participants Identity Network integration

Different networks are supported by corresponding implementations of the Gaia-X Federated Trust Component serving as a client component of the Gaia-X approved Participant identity network. Provider and Consumer do not need to be registered on the same network. On each side the respective Gaia-X Federated Trust Components need to integrate with the network the contracting partner is registered with.

Principal Identity Integration Layer

While the interface to the Gaia-X Federated Trust Component is standardized, the federation mechanism of the Federation Plugin is specific to the implemented Identity System supporting current and future standards like OIDC/OAuth2 (draft), SPIFFE/SPIRE, PKI. Furthermore, multiple Identity Systems required for complex service offerings, like for example OIDC for user Principals, SPIRE for service

Principals, are perfectly supported meaning that multiple Identity Systems on either side can be federated by corresponding plugins based on the very same mutual Participant identity verification if required for the service delivery.

5.3 Data Sovereignty Services

Data Sovereignty Services provide Participants the capability to have full self-determination of 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 includes 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 involving multiple Providers and Consumers. 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 usage, it is important to have a common policy specification language to express data usage restrictions in a formal and technology-independent manner that is understood and agreed by all Gaia-X Participants. Therefore, they must be formalized and expressed in a common standard such as ODRL[14].
Inclusion of Policies in Self-Descriptions	Informational self-determination and transparency require metadata to describe Resources as well as Providers, Consumers, 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 and agreed 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[15] ensures the policy Compliance with technical means (e.g., cancellation or modification of 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 distinct phases of data exchanges are defined:

- 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 the aforementionentioned services to enable sovereign data exchange.

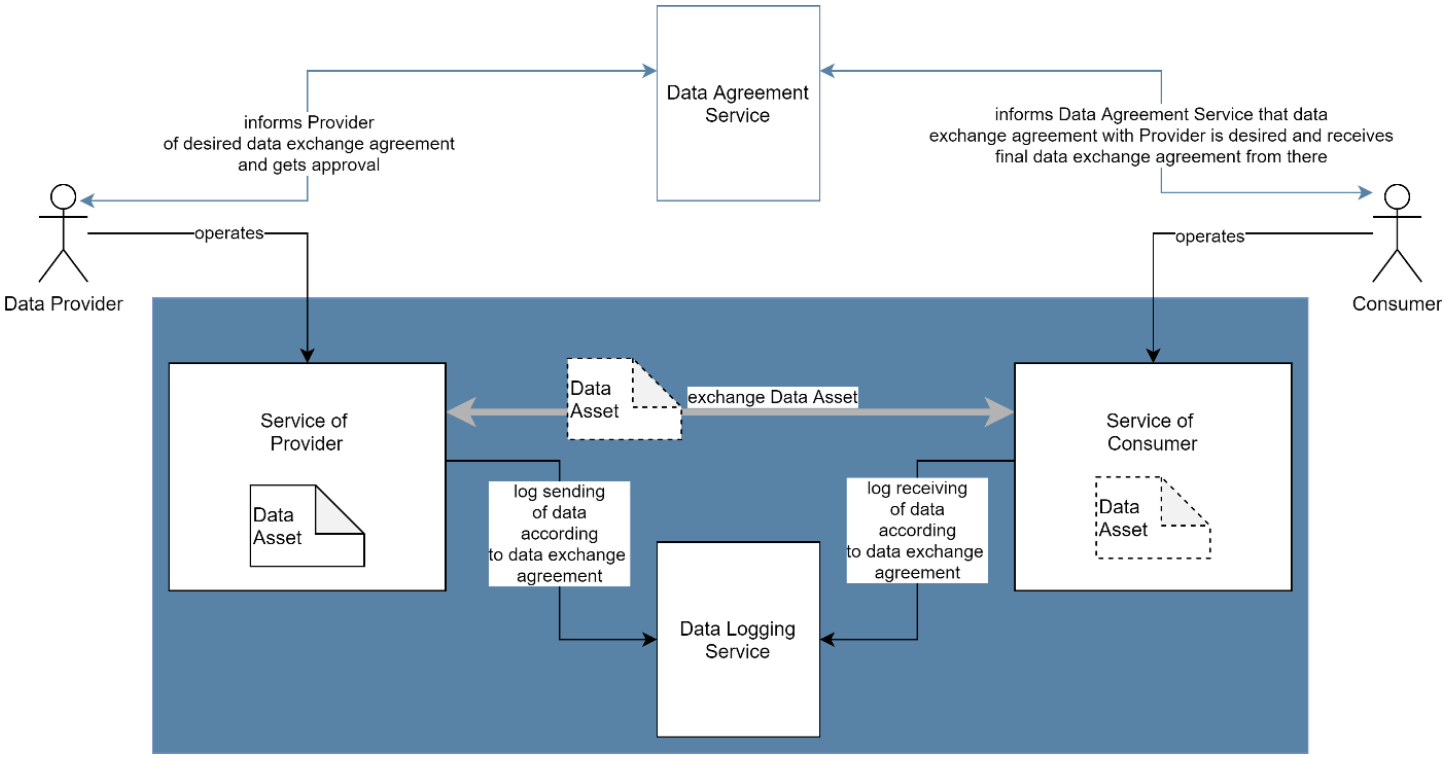


Fig: Data Sovereignty Services Big Picture

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 (which 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, 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. In addition to the general onboarding workflow, special functions must include:

- Monitoring of the relevant bases for Compliance
- Monitoring of updates to Service Offerings that could 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 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 registering as members of the Gaia-X association AISBL. Participants are supported in managing Self-Descriptions and organizing Credentials. This includes Self-Description revisions 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. W3C (2012). Web Ontology Language (OWL). https://www.w3.org/OWL/ ↩
4. Shapes Constraint Language (SHACL). W3C Recommendation 20 July 2017. https://www.w3.org/TR/shacl/ ↩
5. This is analogous to 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 ↩
6. Berners-Lee, T. (2009). Linked Data. W3C. https://www.w3.org/DesignIssues/LinkedData ↩
7. W3C. (2015). Semantic Web. https://www.w3.org/standards/semanticweb/ ↩
8. 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) ↩
9. ECLASS – Standard for Master Data and Semantics for Digitalization. https://www.eclass.eu/ ↩
10. SKOS Simple Knowledge Organization System. W3C. https://www.w3.org/2004/02/skos/ ↩
11. See the IAM Framwork version 1.2 for details: https://community.gaia-x.eu/s/P23ZJNLyjf7n7Zp?path=%2FReleases. ↩
12. 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 as well as Chapter 3.4 in the IAM Framework v1.2: https://community.gaia-x.eu/s/P23ZJNLyjf7n7Zp?path=%2FReleases. ↩
13. 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/#/ ↩
14. W3C. ODRL Information Model 2.2 [W3C Recommendation 15 February 2018]. https://www.w3.org/TR/odrl-model/ ↩
15. Currently not in scope of Gaia-X Federation Services ↩

6. Example 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 in the real word. This section focuses on the most typical kinds of actors and the list is **not exhaustive**. Examples of Gaia-X Use Cases can be found in the position paper published by the Dataspace Business Committee.

6.1 Provider Use Cases

This section describes typical kinds of commonly known actors that have the Provider role in Gaia-X. In general, all kinds of Resources can have their respective Provider.

- Providing various cloud services
  - which acts as Provider of a Service Offering consisting mostly of the Resource Software and Node. Example: a Software-as-a-Service product
- Providing data sets
  - a Provider who is mainly concerned with Data as a Resource and additional Software Resources necessary for enabling data sharing and usage control as well as monitoring. Example: A set of data to train a machine learning algorithm
- Providing Software
  - a Provider who offers single or combined software Services. Example: A domain-specific tool for data manipulation or analysis.
- Providing interconnection & networking services
  - a Provider who offers standard and elevated Interconnection Resources that can go beyond the capacities of the regular Internet connection and exhibit special characteristics. Example: Interconnection as a Service with special guarantees of bandwidth, latency, availability or security-related settings.

6.2 Consumer Use Cases

This section gives examples of different Gaia-X Consumer scenarios, where the Consumer in general can consume all kinds and combinations of Resources analog to the Provider use cases.

- Consuming software
  - A Software service can comprise a broad range of services. They range from cloud services, to high-performance computing services, data-driven software applications, or compositions of different kinds of services.
- Consuming data sets
  - A consumer of data sets may consume raw or processed data and use it as input for own software or combine it with Gaia-X software.
- Consuming interconnection & networking services
  - Consumers can obtain interconnection services as a stand-alone resource, or combine them with other services, for example, to improve stability of connections between different Nodes.
- Consuming storage or computing capacity
  - Consumers can make use of Gaia-X Nodes and combine them with other Gaia-X Resources.

6.3 Federator Use Cases

The different Federators are not distinguished as being either domain-specific or cross-domain. Only accordance to the Policy Rules and operating according to the conditions mentioned in the Operating Model, including the respective conformity assessments and trust mechanisms, distinguish whether it is an ecosystem federated by Gaia-X or not.

- 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 and conformity and trust assessment are perfomed as specified by the Gaia-X Assocaition AISBL. In this case, any entity has the option to become a Participant and participate in such Ecosystem activities if they adhere to the processes and agreements of the Gaia-X Association AISBL.
- 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 and follow the conformity and trust processes. 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 being based on Gaia-X Services and apply the Policy Rules, it cannot be called an official Gaia-X Ecosystem.

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 identification and authentication of all Participants.

Compliance is also assured during 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.

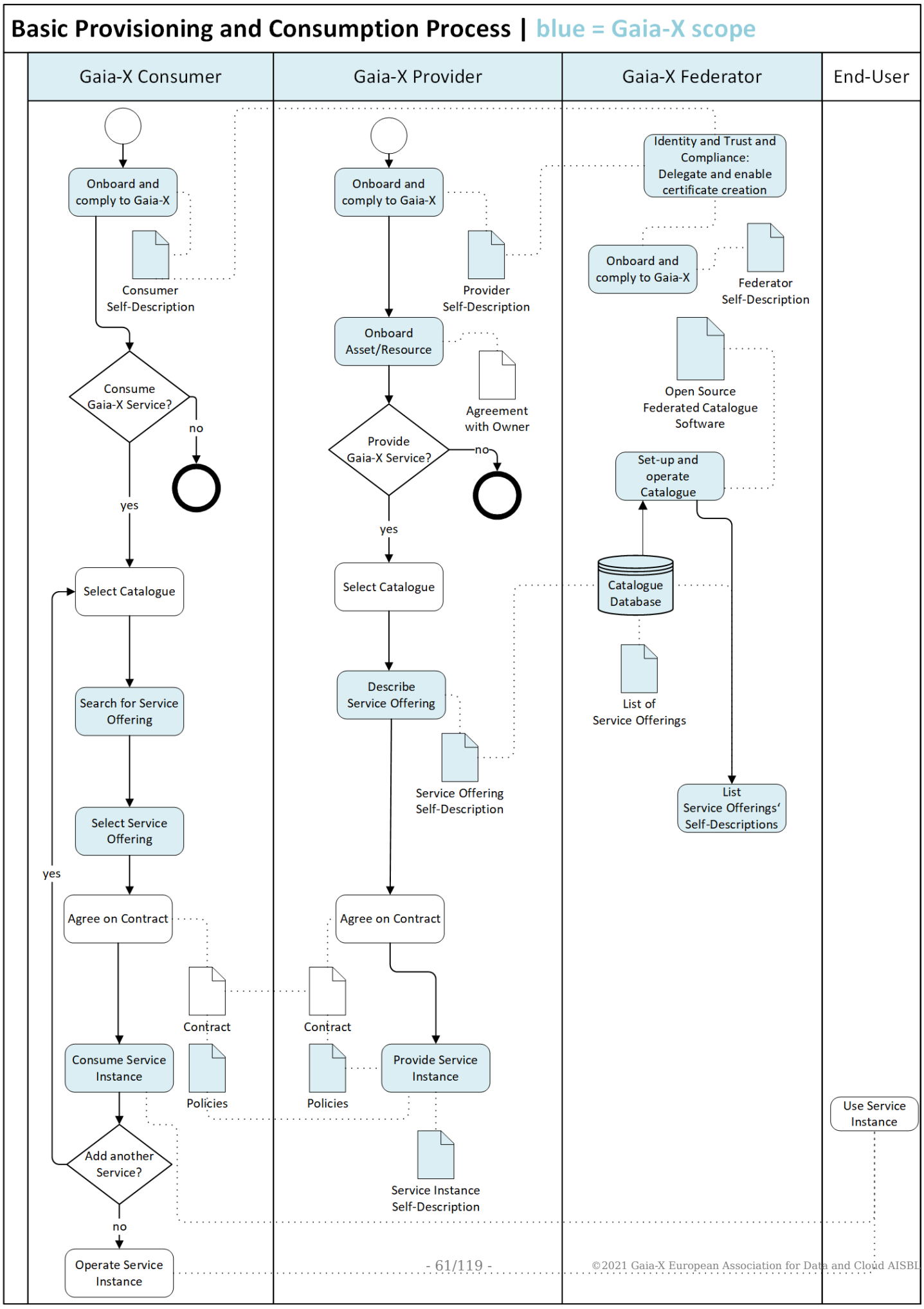


Fig: 10 Basic Provisioning and Consumption Process

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.

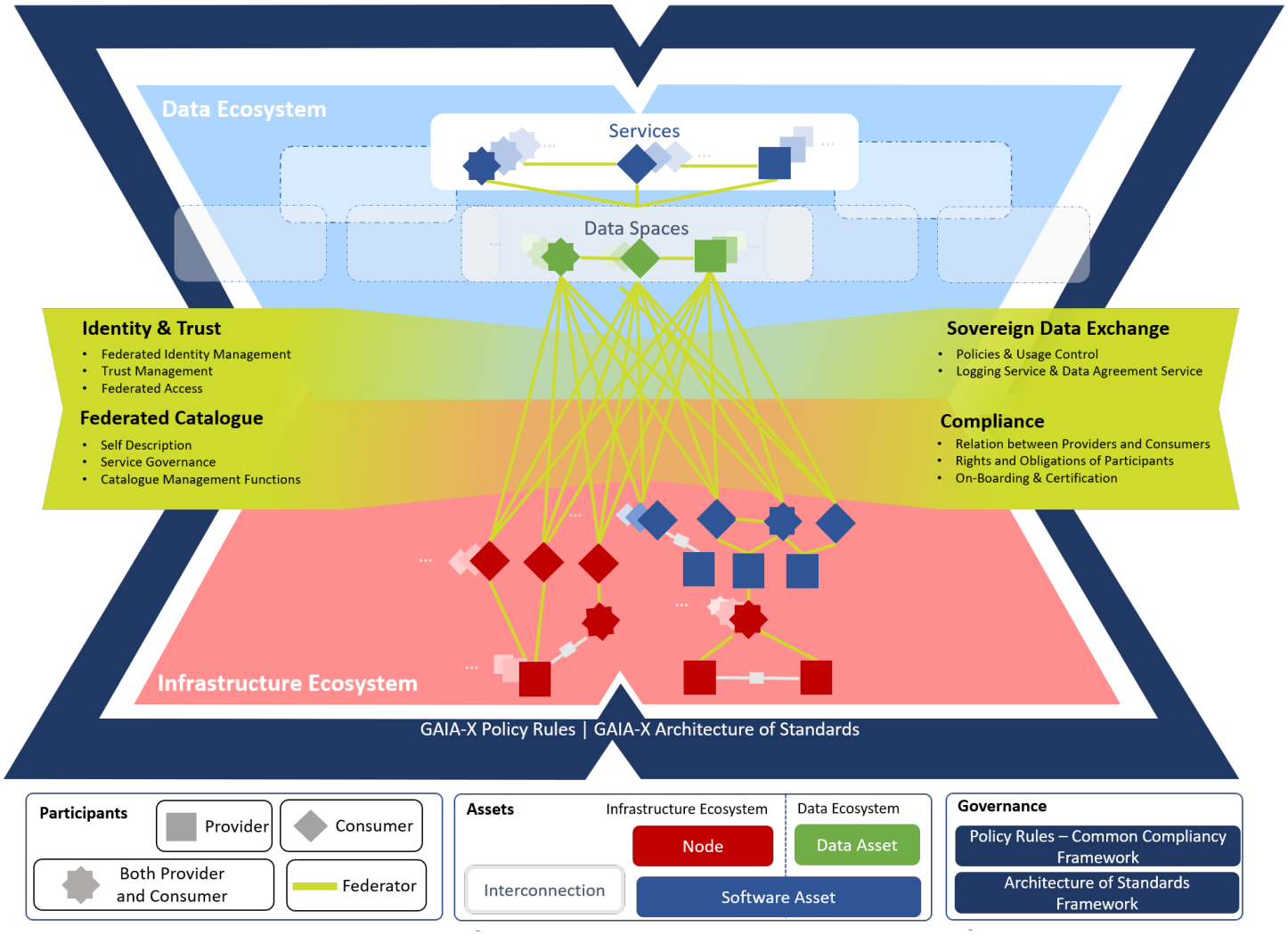


Fig: Gaia-X Ecosystem Visualization

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.

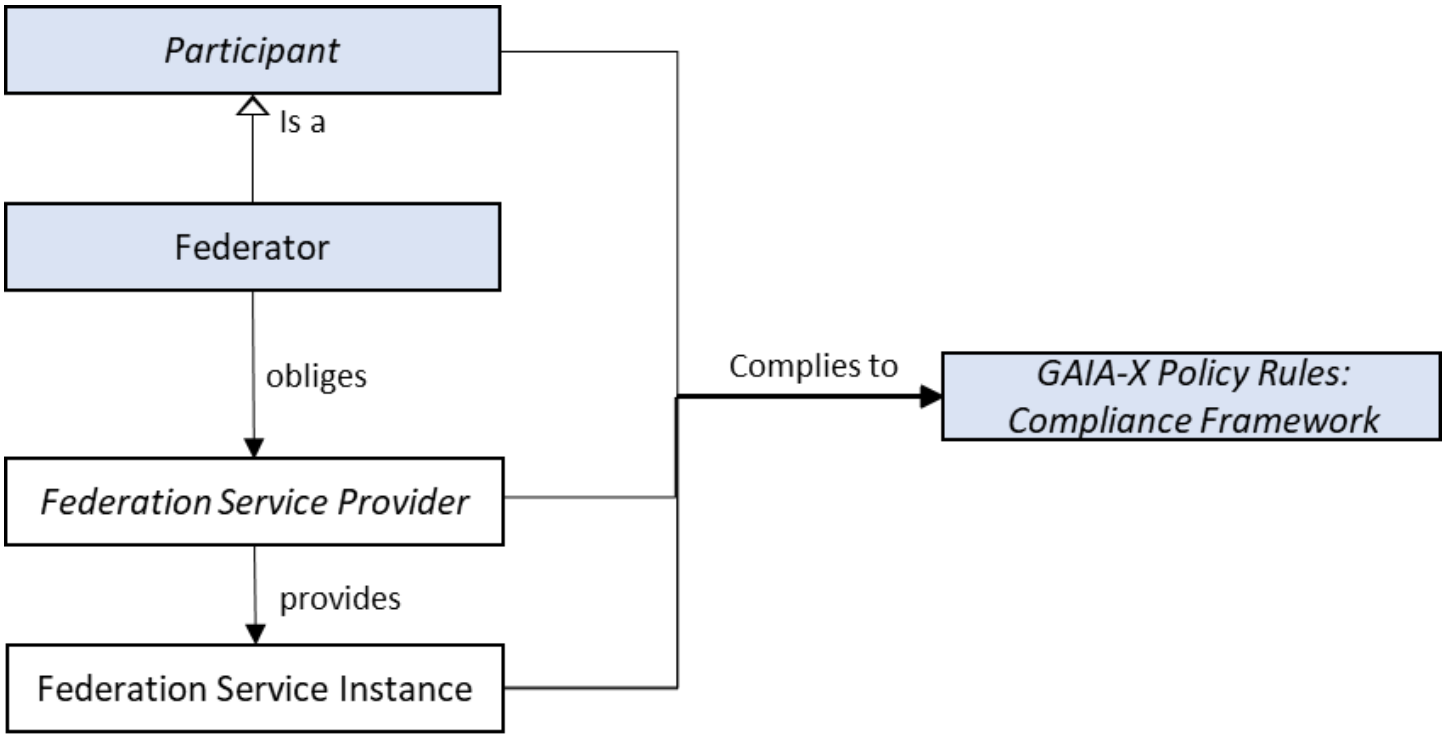


Fig: Federation Services Relations

7.2.1 Goals of Federation Services

Federation Services aim to enable and facilitate interoperability and portability of Resources within and across Gaia-X-based Ecosystems and to provide Data Sovereignty. They ensure trust between or among Participants, make 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 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 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 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 Resources.

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 GAIA-X Ecosystem these elements are designated as Nodes, Interconnections and different Software Resources. 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. The Interconnection Services are also the key enabler for the composition of services offered by diverse and distributed providers, ensuring the performance of single-provider networks on a multi-provider “composed” network.

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 Resources by different Providers spread over geographical locations. (Example: Domain Name System)	Self-Description ensures that all 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.
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.

Principle	Need for Gaia-X	Implemented in Gaia-X Architecture
Sharing	Sharing of the relevant services and components contributes to the Ecosystem development. Sharing and reuse of 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 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 infrastructure 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 resources, and others) by means of Service Composition.

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 Infrastructure and Data Ecosystems, where data is flexibly exchanged between and among many different Participants. Therefore, Interconnection Services represent a dedicated category of Resources as described in section Gaia-X Conceptual Model.

There is a strong need for Interconnection Services for the different Nodes in Gaia-X. These support 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 Role of Interconnection and Networking Services

The recent survey (08/2021) performed by the German market research company Research in Action showed that requirements on the network and interconnection vary in different sectors [2]. On average 25% of the companies in Healthcare & Social Assistance, Manufacturing & Automotive and Travel/ Transport/Logistics require a connection that is separated from the public Internet. Thus offering protection from hacking attacks and malicious third-parties, as well as ensuring the resilience and constant availability of the connection. Almost 30% of the Travel, Transport, and Logistics sector shows an interest in a high-performance, low-latency, redundant interconnection service to enable fast response times for business critical tasks.

These and other sectors are present in GAIA-X Data Spaces and can not always rely on the best-effort public Internet and in some cases require dedicated / exclusive connections, which, as alternative to single-owner networks, could be created by the composition of resources offered by different providers. As a result, Gaia-X defines interconnection and networking services as one of the key resources for

reaching its goals (refer to the [Glossary]). Consequently, and as explained in section Provider Use Cases, the Federated Catalogue must be extended with the rich variety of networking and interconnection services, considering, for instance, functional and non-functional QoS (Quality of Service) requirements; portability requirements, etc.

Currently, Gaia-X addresses the architectural needs for networking and Interconnection services via three building blocks: (i) a Self-Description model, which describes Interconnection Ressources and mandatory attributes necessary to describe interconnection & networking services Appendix; (ii) Quality of Service assesment by for example inter-Node measurements, describing connection SLA indicators (guaranteed bandwidth, availability, latency, etc.) between or among Gaia-X Participants; (iii) interoperable interconnection and networking services from different Participants based on e.g Internet, L2 point-to-point connection, private interconnection, etc. (refers to Network Service Composition) In the current release we have mainly adressed (i) and (iii) that are explained below.

7.4.2 Interconnection Resource Mandatory Self-descriptions

In this sub-section we focus mainly on the Self-Description of Gaia-X Nodes, where Interconnection and networking services are addressed via the definition of attributes. The first set of mandatory Self-Descriptions attributes describing Interconnection Resource considers QoS (Quality of Service) functional parameters relevant for real-time data services, e.g., latency, bandwidth, availability, packet loss (refer to Appendix for an exhaustive list of attributes). In case the Provider is not able to guarantee certain level of QoS, the best-effort value should be used to desribe these attributes.

For the future releases non-functional requirements for supported services must also be defined (whether mandatory or not). Therefore, Self-Description of Interconnection and networking services will not only be limited to QoS but also address quality of experience (QoE)-related attributes and consider non-functional requirements, such as security and reliability. A distinct and rich description of these functional and non-functional requirements enables differentiating between the different Service Offerings and helps to select the appropriate Interconnection and networking services from the Gaia-X Catalogues.

7.4.3 Network Service Composition

Interconnection and Networking 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. An example 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].

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.

Moreover there is a need for GAIA-X Compliant Network Service Composition Framework, talking to APIs (e.g, the open source IX-API[6], Terraform[7], etc.) of Providers (in this case Interconnection Service Providers), as well as solutions from the area of Software Defined Networking that can be used to flexibly interconnect and configure these architectures, and consider host-reachability and content-oriented developments.

This framework should also 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. To understand this concept an its relation to the defined mandatory attributes and Gaia-X Conceptual Model, let us consider the following scenario shown in Figure below.

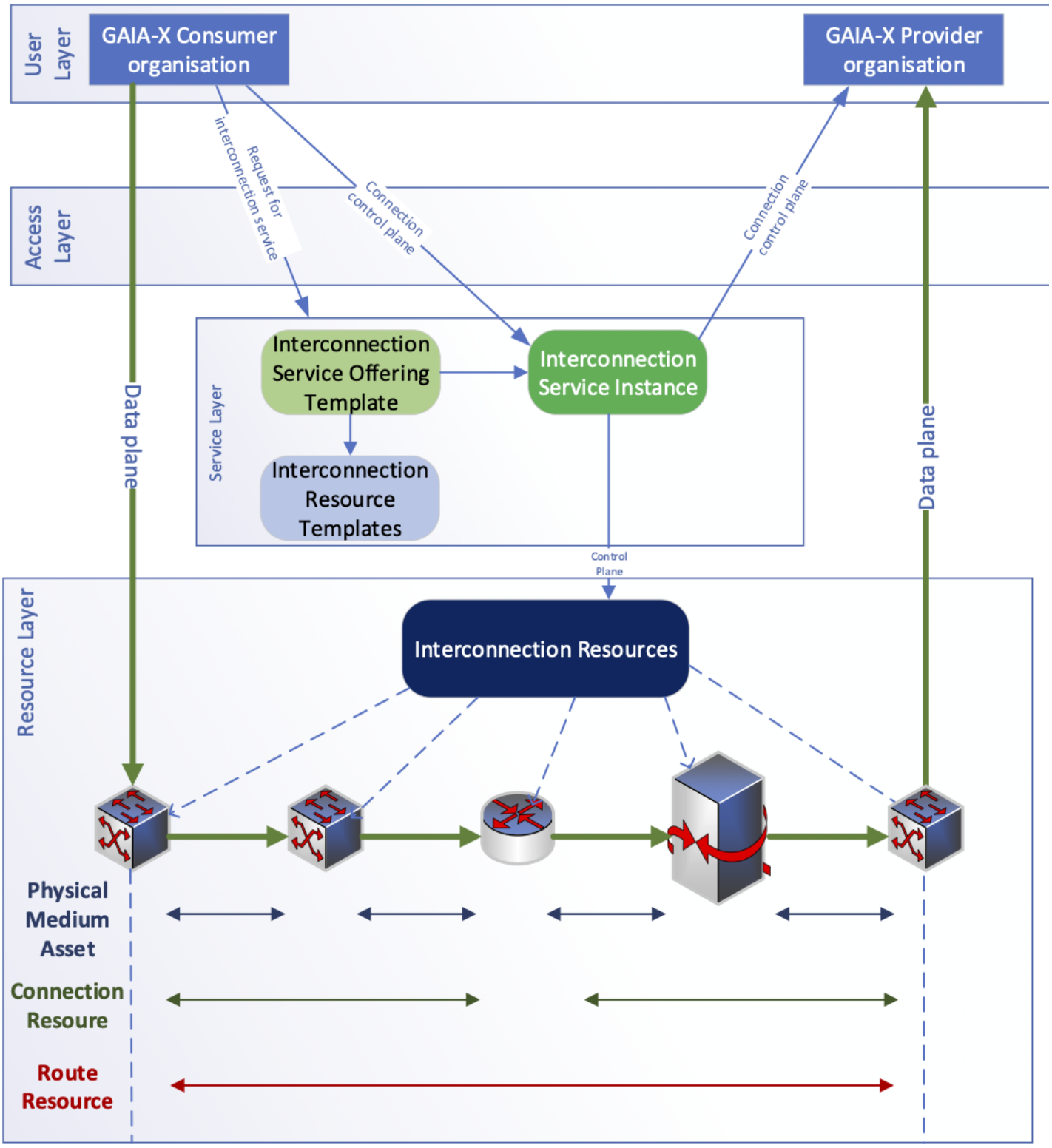


Fig: General Use Case: Ordering of Interconnection Service

A Gaia-X Consumer requests an interconnection service, providing information about the desired interconnection points (via Interconnection Service Offering Templates) from the GAIA-X Interconnection Service Provider. At this point in time, the interconnection service is instantiated (Interconnection

Service Instance) and it relies on various Interconnection resources that are responsible for the actual connection establishment. These interconnection resources can be composed of different attributes (the very first mandatory set is found in the Appendix).

First set of Elements for the composition of Interconnection&Networking services

In the scope of the Gaia-X Ecosystem a Network (and/or Interconnection) Service can be 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.

Such a 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 resources:

Networks

Networks are logical communication resources 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:[^32] 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. [^32] https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-1:ed-1:v2:en

Route Resources

A Route Ressource Template defines the reachability of one or more Networks and can be subscribed individually by users. A Route Resource provides connectivity to other networks, nodes or services by using other Interconnection Ressources or Services. These ressources or services can be explicitly defined or be abstracted by the Route Ressource itself. A Route Ressource in most cases will provide access to multiple networks, nodes or services at once and hence has a cardinality of 1..* Generally, a Route Resource will only provide connectivity in one direction, while the route back needs to be established from the connected service.

Connection Resources

Connection Resources provide a direct communication path between one or many Networks, Nodes or Services. They can use other Interconnection Resources. These services or resources can be explicitly defined or be abstracted by the Connection Resource. A Connection Resource will connect at least two Networks, Nodes or Services and hence has a cardinality of 2..* Connection Resources are generally provided as connections between two or more interconnection points which are defined in terms of location and jurisdiction.

Physical Medium Resource

Physical Medium Resources are direct physical connections between exactly two Networks or Nodes and provide a direct communication path between single Networks or Nodes. They are defined by specific endpoints and cannot use other Interconnection Resources to realize the connection and thus are the atomic instances of interconnection services. They have a cardinality of 2..2.

Service Orchestration

To allow Customers to consume any of the above-mentioned Interconnection Ressources or compose new Services from them, each Ressource needs to be available as a Ressource Template from the GAIA-X Catalogs and needs a self-description. To enable Network and Interconnection Service Composition in an automated way, any Interconnection Service Request needs to be described from a functional and non-functional requirement view. For Interconnection Ressources and the services composed from those ressources, such as Routes, Connections or Physical Medium this can include network based quality parameters such as bandwidth, latency, jitter and availability. To be able to compose Interconnection Services, Interconnection Ressource Templates need attributes that describe their dependency on other Interconnection Resources, so that Customers can query the Catalog for the dependencies and instantiate these Resources according to the requirements. In this sense, a Route Resource Template could potentially provide no quality attributes itself, but depend on a specific subset of Connection or Physical Medium Ressources that provide specific quality attributes. These attributes then are “inherited” by the Route Service composed from the Connection and Physical Medium Ressources and can be provided as a Service themselves.

A Gaia-X compliant orchestration service will then compose the full Interconnection Service required by instantiating Resource Instances from the selected Resource Templates.

Interconnection Platforms

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. Specific Interconnection Resources such as Connection or Physical Medium Resources allow for those functional requirements to be met.

As the resources and data from the Provider and Consumer use cases are located in different physical locations, namely in data centers that could be spread all over Europe it would result in a overly complex and redundant number of connections, if we would interconnect them directly, which would be expensive, insufficient and neither dynamic nor performant. In the example shown below, if we want to interconnect 8 locations or nodes we would require 28 connections (picture on the left). However, with the introduction of an 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.

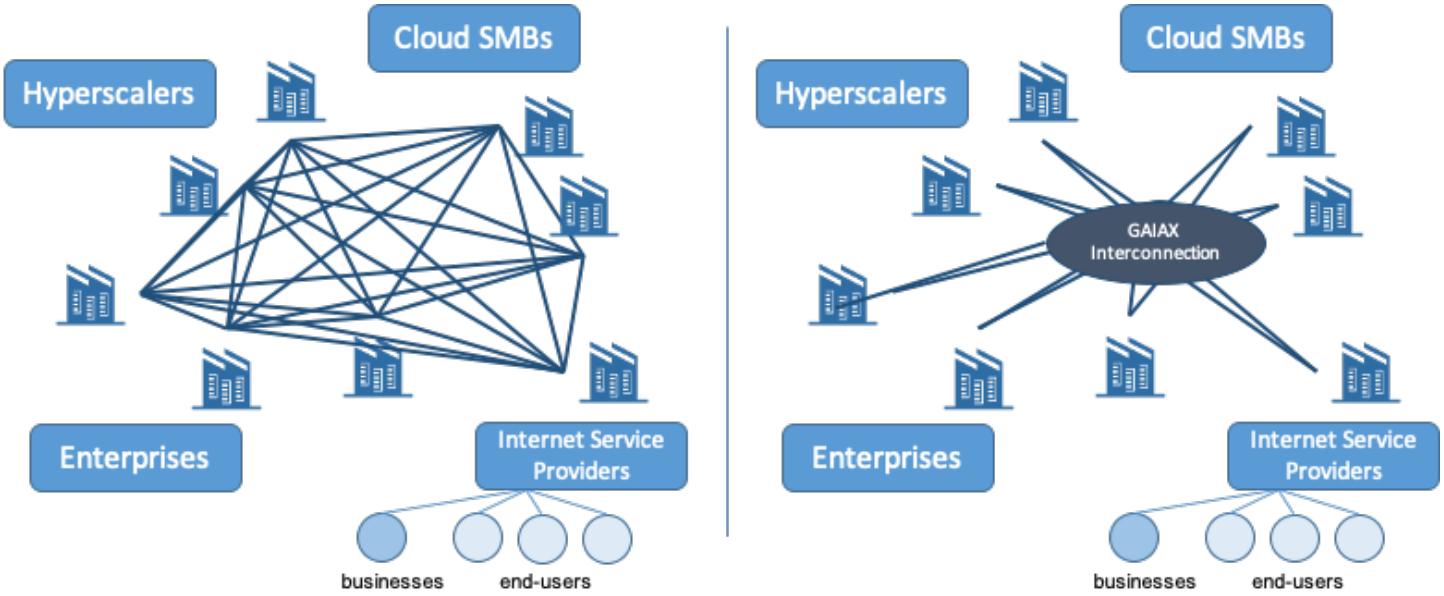


Fig: Visualization of connections via Interconnection Platform: left - without platform, right - with platform

The solution that we see is Gaia-X compatible Interconnection platforms with common or standardized APIs or Interfaces to a GAIA-X compliant orchestrator via which the interconnection Resources can be connected together. Such an Interconnection Platform can operate as a specific Gaia-X Node and provide a high number of interconnection points at one location. This platform will be provided and operated by Gaia-X Providers (e.g., Interconnection Providers).

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 (Network Resource as VPN) or to directly use private Connection or Physical Medium Resources (asan example).

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. https://www.de-cix.net/en/about-de-cix/media/press-releases/new-de-cix-market-survey-confirms-no-slowdown-in-sight-digital-transformation-continues-at-pace-in-companies-in-germany-and-the-usa ↩
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. https://ix-api.net/ ↩
7. Terraform. https://www.terraform.io/ ↩

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 Catalogue

A Catalogue presents a list of available Service Offerings. Catalogues are the main building blocks for the publication and discovery of Self-Descriptions for Service Offerings by the Participants.

8.4.1 alias

- Gaia-X Catalogue

8.5 Certification

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

8.5.1 references

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

8.6 Claim

An assertion made about a subject within Gaia-X.

8.6.1 references

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

8.7 Compatibility

8.7.1 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

8.7.2 references

- ISO/IEC 25010:2011

8.8 Compliance

Compliance refers to the accordance with Gaia-X Rules.

8.9 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.

8.10 Conformity Assessment

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

8.10.1 references

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

8.11 Conformity Assessment Body

Body that performs Conformity Assessment services.

8.11.1 references

- DIN EN ISO/IEC 17000

8.12 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.

8.13 Consumer Policy

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

8.13.1 alias

- Search Policy

8.14 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.

8.14.1 alias

- CAM

8.15 Contract

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

8.16 Credential

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

8.16.1 references

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

8.17 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.

8.17.1 alias

- DLS

8.17.2 references

- Federation Services Specification GXFS

8.18 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.

8.19 Data Agreement Service

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

8.19.1 alias

- DAS

8.19.2 references

- Federation Services Specification GXFS

8.20 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

8.20.1 references

- ISO/TS 19299:2015, 3.32

8.21 Data Resource

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

8.22 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.

8.22.1 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.

8.23 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.

8.24 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.

8.24.1 references

- Gaia-X, TAD 2020 p.3

8.25 Ecosystem

An Ecosystem is an independant group of Participants that directly or indirectly consume, produce, or provide services such as data, storage, computing, network services, including combinations of them.

Technically speaking, there is no definition of a Gaia-X ecosystem, since the Gaia-X Compliance is applicable to Participants, Service Offering and related entities only. However, it is commonly understood that a such an ecosystem would refer to a group of Gaia-X Compliant Participants exchanging Gaia-X Compliant services.

8.26 End-User

A natural person or process not being a Principal, using a digital offering from a Participant. Participants manage their relations with End-Users - including identities - outside of the Gaia-X ecosystem scope. End-Users have no credentials within the Gaia-X Ecosystem.

8.27 Endpoint

Combination of a binding and a network address.

8.27.1 reference

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

8.28 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.

8.28.1 alias

Federated Trust Model

8.29 Federation

A Federation refers to a loose set of interacting actors that directly or indirectly consume, produce, or provide resources.

8.29.1 alias

Ecosystem

8.30 Federation Services

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

8.30.1 references

- Architecture Document 2103

8.31 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.

8.32 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.

8.32.1 references

Federation Services Specification GXFS

8.33 Gaia-X AM

Gaia-X internal Access Management component.

8.34 Gaia-X Identifier

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

8.35 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.

8.36 Identity

An Identity is a representation of an entity (Participant/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.

8.36.1 references

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

---

8.37 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).

8.38 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.

8.39 Interconnection & Networking Service

Networking Service – services offered beyond the basic network functions, for example NTP, DNS, etc.

Interconnection Service – is the subclass of network service that runs on top of physical or logical interconnection. These can include best-effort connectivity and also go beyond it ensuring guaranteed bandwidths, lower latency, reliability and elevated security.

Interconnection & Networking service is a service that combines one or multiple services defined above.

8.40 Interconnection

Interconnection, rephrasing EU 2002/19/EC directive, refers to the physical or logical connection between two or multiple Nodes that enables the traffic exchange among them. In the context of telecommunications, interconnection can be implemented directly between different stakeholders or through dedicated interconnection points (e.g. IXPs).

The difference to the simple connection is that in case of interconnection we are speaking of a connectivity that involves several parties at once. It allows unification of interconnected parties into digital ecosystems. Moreover, it can exhibit special characteristics, such as latency and bandwidth guarantees, that go beyond the characteristics of a path over the public Internet.

8.41 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.

8.41.1 references

- ISO/IEC 17788:2014

8.42 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.

8.42.1 alias

- OAW

8.42.2 references

- Federation Services Specification GXFS

8.43 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.

8.44 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.

8.44.1 references

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

8.45 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 all Resources.

8.45.1 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

8.46 Portability

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

8.46.1 references

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

8.47 Principal

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

8.48 Provider

A Participant who provides 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.

8.49 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.

8.49.1 references

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

8.50 Resource

A Resource is an internal building block, not available for order, used to compose Service Offerings.

Resource Categories include:

- Data Resource, which consists of data (which may include derived data) in any form and includes the necessary information for data sharing.
- Software Resource, consisting of non-physical functions.
- Node, representing a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities.
- Interconnection, which includes details of the connection between two or more Nodes.

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

8.51 Resource Owner

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

Most Cloud Service Providers will be `Participants` with two roles: `Resource Owners` and `Providers`.

8.52 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.

8.52.1 references

- Federated Catalogue WP

8.53 Self-Description

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

8.53.1 alias

- Gaia-X Self-Description

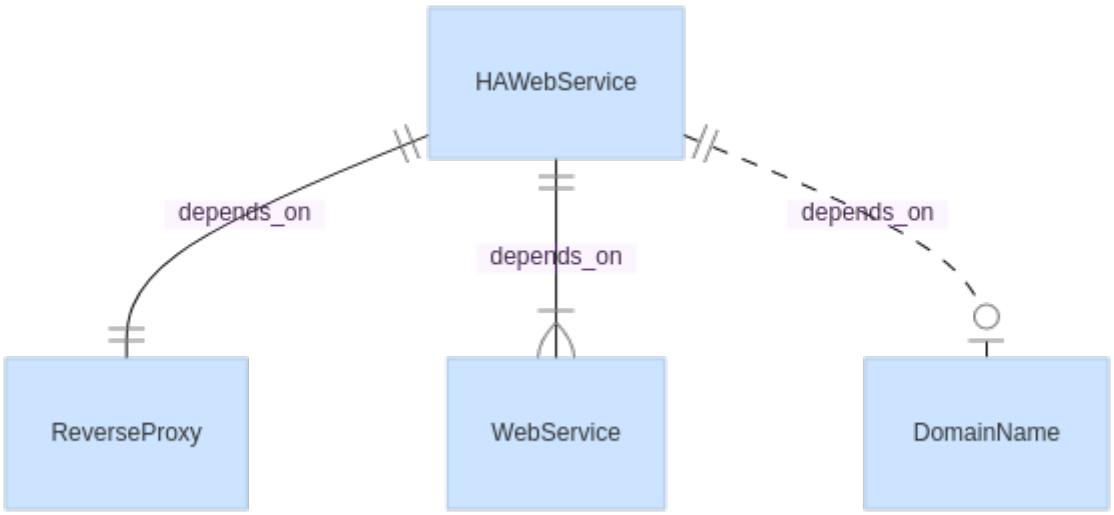
8.54 Service Composition

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

A functional dependency exposes behaviors related to external actions, which match its requirements and characteristics.

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

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



8.55 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.

8.56 Service Offering

A Service Offering is a set of Resources, which a Provider bundles into an offering.

A Service Offering can be nested with one or more other Service Offerings.

8.57 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.

8.58 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).

8.59 Usage Policy

A Usage Policy is a Policy in a technical sense, by which a Provider constraints the Consumer's use of the Resources offered.

8.59.1 alias

- Provider Policy

8.59.2 references

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

8.60 Visitor

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

9. Changelog

9.1 2021 December release

- Adding `Contract` and `Computable Contract` definitions in the Conceptual Model
- Update on the Self-Description lifecycle management
- Update on the Federated Trust Model

9.2 2021 September release

- Rewrite of the Operating model chapter introducing Trust Anchors, Gaia-X Compliance, Gaia-X Labels and Gaia-X Registry.
- Update of Self-Description mandatory attributes in the Appendix.
- Update of `Interconnection`, `Resource` and `Resource template` definitions.
- Gitlab automation improvement and speed-up
- Source available in the 21.09 branch.

9.3 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.

9.4 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.

9.5 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

The Federated Trust Model is currently being updated, the new version will appear here in the next version of this document.

11.3 A3

This appendix presents minimal core versions of central Gaia-X concepts of the Conceptual Model. That includes mandatory attributes as well as their types and cardinalities for the core concepts of Participant, its special case Provider, Service Offering, Asset, Data Asset (and Data Service Offering as a special case of Service Offering, representing the service through which a Data Asset is provided), Software Asset, Node, and Interconnection.

11.3.1 Governance of Mandatory Attributes

The following lists of mandatory attributes reflect the consensus of stakeholder workshops held by the Self-Description Work Package. The proposer of each mandatory attribute was required to justify why it should be mandatory.

Anticipating further specializations of the Self-Description Schemas, future Architecture Document releases may instead refer to a dedicated, separate Self-Description document and an official Federated Catalogue hosting the Self-Description Schemas that implement the mandatory attributes. Future changes to the mandatory attributes, including additions, modifications, as well as deprecations, will be handled through the ADR process or a specialization of it. Mandatory attributes that, in future, are deemed to no longer be mandatory, or to no longer be applicable at all, shall not be deleted, but be deprecated as specified in OWL[1]

11.3.2 Semantics of Mandatory Attributes

The focus of this section is on mandatory attributes, i.e., those for which at least one value must be specified. Other attributes, which are of interest but optional, are out of scope of this revision of the Architecture Document. Technically, the presence or absence of a mandatory attribute in a Self-Description is checked by a validation shape. This validation mechanism only has access to the Self-Description and to the validation shapes, not to an oracle that provides further information about the real world. Thus, attributes are specified as either mandatory or non-mandatory. It is not technically possible to specify that an information should be mandatory if a certain situation holds in reality, e.g., that a Provider’s parent entity must be specified if the Provider has a parent entity.

For some attributes, it it recommended to use values from Controlled Vocabularies. Gaia-X specific controlled vocabularies have not yet been standardized. In future, they may be standardized according to a similar process as the specification of mandatory attributes. All such URIs given below serve as examples. The semantics of these terms may be fixed later.

11.3.3 Participant

Unless mentioned otherwise, the following attributes have identifiers in the http://w3id.org/gaia-x/participant# namespace, abbreviated with the gax-participant: prefix (e.g., gax-participant:hasLegallyBindingName).

Attribute	Description	Type(s)	Cardinality	Example value
hasLegallyBindingName	legal name	xsd:string	1..1	“SAP SE”
hasLegallyBindingAddress	legal address	vcard:Address	1..1	(a structured object having, e.g., the attributes vcard:street-address, vcard:locality and vcard:country-name)

Provider / Consumer

A Participant implicitly becomes a Provider once they provide (i.e., possess/operate/define) at least one Asset, Resource or ServiceOffering. They implicitly become a Consumer once they consume at least one ServiceInstance. To a Provider, the following additional mandatory attributes apply:

Attribute	Description	Possible Type(s)	Cardinality	Exampl
hasLegalForm	legal form	xsd:string or controlled vocabulary entry (URI)	1..1	https://g Societas
hasJurisdiction	jurisdiction	xsd:string or controlled vocabulary entry, e.g., country (URI)	1..1	http://ga country/
hasSalesTaxID	sales tax ID / VAT ID	xsd:string	1..1	“DE 129 Germany
hasLegalRegistrationNumber	legal registration number	xsd:string	1..1	“HRB 12
hasWebAddress	web address	xsd:anyURI	1..*	https://g
hasIndividualContactLegal	contact person for legal purposes	vcard:Agent, schema:Person	1..*	(a struct e.g., the schema: schema:
hasIndividualContactTechnical	contact person for technical purposes	vcard:Agent, schema:Person	1..*	(a struct e.g., the schema: schema:

11.3.4 Service Offering

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasServiceTitle	Name of the service	xsd:string	1..1	“Image classification ML service”
hasServiceDescription	A description in natural language	dct:description	1..1	“An ML service for easily training, deploying, and improving image classifiers.”
hasKeyword		dcat:keyword	1..n	“Machine Learning”, “Classification”
providedBy	This service’s provider(s)	gax-participant:Provider	1..*	gax:Company-1
hasProvisionType	Provision type	xsd:string or controlled vocabulary entry (URI)	1..1	“Hybrid” / gax:PrivateProvisioning
hasServiceModel	Service model	xsd:string or controlled vocabulary entry (URI)	1..1	“IaaS” / “PaaS” / “SaaS”
hasWebAddress	URL of the service website	xsd:anyURI	1..1	http://example.org/ML-classification-service

Asset

As of the 21.09 Architecture Document, Assets are no longer part of the Conceptual Model. The mandatory attributes for describing the similar concept of Resource are given below. A further revision of the Resource mandatory attributes, aligned with the ones of the former Asset concept, is expected for 2021-Q4.

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.

11.3.5 Data Service Offering

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasServiceTitle	Title of the data service featuring a high level description for quick reference.	xsd:string	1..1	“Example Data”
hasServiceDescription	A more detailed description incl. markdown of the data service that contains all information not included in standardized Self Descriptions	dct:description	1..1	“This data service con data silo.”
hasLicense	Reference to the license model of the data service	xsd:string or controlled vocabulary entry (URI)	1..1	“Public Domain”, https 1.0/, “CC-BY”, “No Lic
hasCopyrightHolder	Reference to the author or copyright holder as name or DID	xsd:string	1..1	“Satoshi Nakamoto”, c 3:bafyreigh5aiij5xltuq

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasType	Type of the data asset, which helps the discovery process.	xsd:string or controlled vocabulary entry (URI)	1..1	“dataset”, http://gaia-x “container”, “video str
wasCreatedOn	The timestamp the data service has been created. ISO 8601 format, Coordinated Universal Time.	xsd:dateTimeStamp	1..1	2021-07-17T00:31:302
conformsToStandard	Provides information about standards applied, e.g., ISO 10303.	xsd:string or controlled vocabulary entry (URI)	1..n	“ISO10303-242:2014” ISO_13567-1_2017

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasStandardReference	Provides a link to the schema or additional details about the underlying standards applied, in case this link is not attached to the representation of the standard in a controlled vocabulary	xsd:anyURI	1..n	https://www.iso.org/sta

11.3.6 Example for an Extension of a Data Service Offering (File)

If the underlying resource is a file this might require different attributes than streams or software products. This shall illustrate an example for a simple data service that serves a file that is available for download or computation.

The mandatory attributes are:

Attribute	Description	Possible Type(s)	Cardinality	Example
hasContentType	File format, could be detected during the listing process and availability check.	xsd:string or controlled vocabulary entry (URI)	1..1	“text/plai assignme json
hasLocalURL	Endpoint that is used during the publishing process	xsd:anyURI	1..1	https://ra examplef
hasEncryptedURL	Contains the encrypted URL, which may be used to enable access control.	xsd:string	1..1	7f9s79fu
hasEncryptionEndpoint	Contains the endpoint responsible for URL decryption and access control	xsd:anyURI	1..1	https://ac
hasFileIndex	Index number, starting from 0	xsd:nonNegativeInteger	1..1	4
hasFileEncoding	File encoding (e.g., UTF-8).	xsd:string or controlled vocabulary entry (URI)	1..n	“UTF-8”, encoding
hasContentLength	Size of the file in bytes.	[xsd:nonNegativeInteger]	1..n	3789287
hasChecksum	Checksum of the file using your preferred format (i.e., MD5). Format is specified in hasChecksumType.	xsd:string	1..n	25d422c

Attribute	Description	Possible Type(s)	Cardinality	Example
hasChecksumType	Format of the provided checksum. Can vary according to server (i.e., Amazon vs. Azure)	xsd:string	1..n	md5

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 Resource

An interconnection resource can consist of a physical medium resource, a connection resource or a route resource. One or multiple interconnection resources compose an interconnection service. The mandatory attributes (aka resource templates) of these are listed in separate tables below.

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasPhysicalMediumResource		PhysicalMediumResource	0..1	
hasConnectionResource		ConnectionResource	0..1	
hasRouteResource		RouteResource	0..1	

Physical Medium Resource

The Physical Medium Resource can be an individual interconnection resource. It has the following mandatory attributes:

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasPhysicalMediumResourceLocation	references two locations (A and B) that require a connection (physical or virtual)	xsd:string or dct:Location	2..2	(a point of presence, a facility, a data center, or an address)
hasPhysicalMediumResourceType	the type of technology used for physical connection	xsd:string or controlled vocabulary entry (URI)	1..1	“copper cable”, http://gaia-x.eu/vocab/medium/WiFi, “fiber”, “4G/5G”, …

Connection Resource

A Connection Resource (for example an Ethernet or Dense Wavelength Division Multiplexing (DWDM)) can also be the interconnection resource on its own. It has the following mandatory attributes:

Attribute	Description	Possible Type(s)	Cardinality	Examp Value
hasConnectionPointA	source reference ID	xsd:string	1..1	MAC address VLAN I ...
hasConnectionPointZ	destination reference ID	xsd:string	1..1	MAC address VLAN I ...
hasBandwidth	contractual bandwidth defined in the service level agreement (SLA)	measure, e.g., in unit Gbps	1..1	1 Gbps, Gbps, 1 Gbps, 4 Gbps
hasLatency	contractual latency defined in the SLA. If not specified, then best effort is assumed.	measure in the dimension of time, or the controlled vocabulary entry “best effort”	1..1	1 s, 10 http://g x.eu/ vocab/ value/ BestEff

Attribute	Description	Possible Type(s)	Cardinality	Examp Value
hasAvailability	contractual availability of provider services defined in the SLA agreement. If not specified, then best effort is assumed.	measure in the pseudo-unit percent, or the controlled vocabulary entry “best effort”	1..1	99.9%, 99.99% 99.999% a
hasPacketLoss	contractual packet loss defined in the SLA. If not specified, then best effort is assumed.	measure in the pseudo-unit percent, or the controlled vocabulary entry “best effort”	1..1	1%, 10% http://g x.eu/ vocab/ value/ BestEff
notsupportedProtocols	not supported protocols among used layers should be specified	xsd:string	1..1	the spannin tree protoco not support
(optional) hasIntermediateConnectionPointsN	intermediate connection/ interconnection point ID	xsd:string	1..N	MAC address VLAN I …

Attribute	Description	Possible Type(s)	Cardinality	Examp Value
(optional)hasConnectionType	point-to-point, one-to-many, many-to-many, many-to-one	xsd:string	1..1	etherne unicast, multica broadca support

Measure

A measure is a compound of a numeric value and a unit of measurement. A measure is typically not given an identifier and reused in multiple places, but written down locally, as the value of a single attribute. I.e., in the RDF data model, it is typically represented as a blank node. It has the following mandatory attributes:

Attribute	Description	Possible Type(s)	Cardinality	Example Value
hasValue	the value of the measure	any numeric datatype, e.g., xsd:float	1..1	100
hasUnit	the unit of measurement	xsd:string or controlled vocabulary entry (URI)	1..1	http://gaia-x.eu/vocab/units/Gbps

Controlled vocabularies of units support the definition of compound units from base units, the provision of conversion factors, etc. Vocabularies suitable for reuse include QUDT[2].

Route Resource

A Route Resource can be an interconnection resource. It has the following mandatory attributes:

Attribute	Description	Possible Type(s)	Cardinality	Example Value
connected network	autonomous system (AS) number (ASN) should be provided	xsd:integer	1..1	200, 714
prefix set	CIDR Provider Identifier	[xsd:string]	1..1	10.1.1.1/24
origin node	reference to connection points	xsd:string	1..1	Node ID

1. OWL 2 Web Ontology Language. Structural Specification and Functional-Style Syntax (Second Edition). W3C Recommendation 11 December 2012. http://www.w3.org/TR/2012/REC-owl2-syntax-20121211/ ↩
2. http://www.qudt.org/ ↩