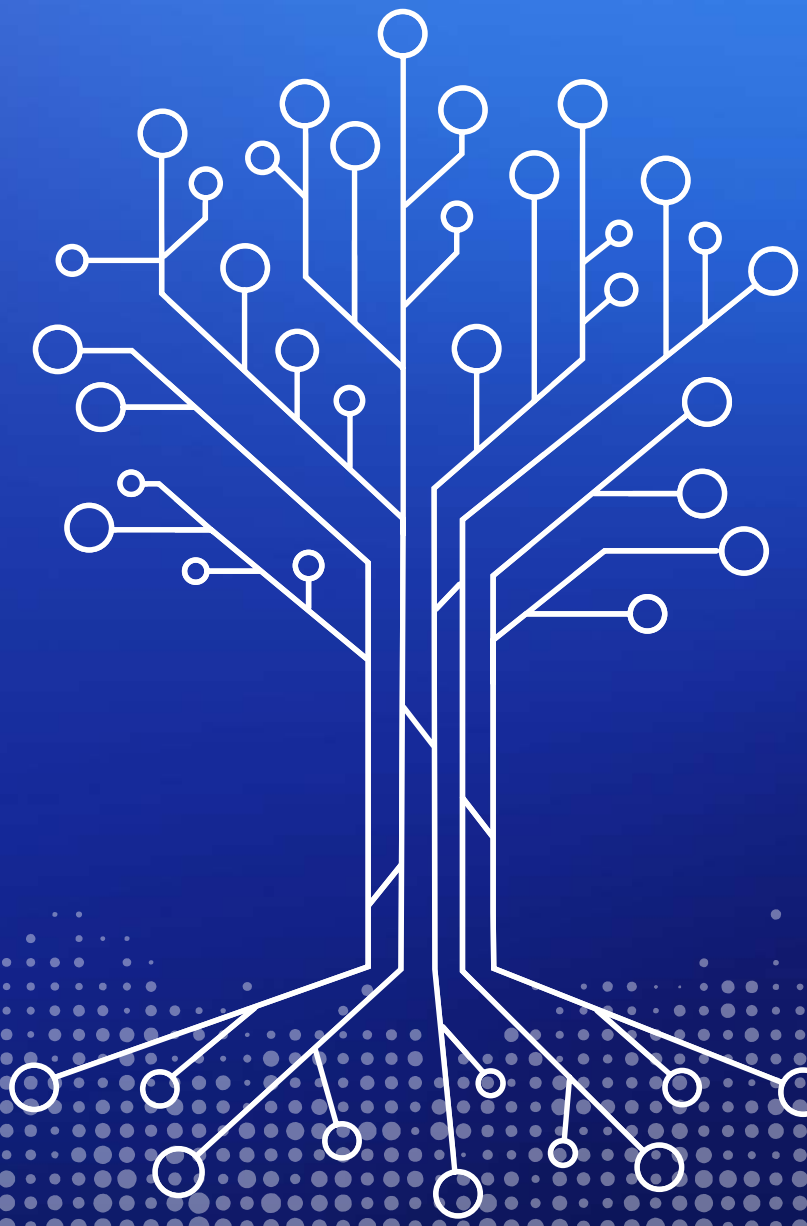
GAIA-X

GAIA-X: Technical Architecture

Release – June, 2020



Imprint

Publisher
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations Division
11019 Berlin
www.bmwi.de

Authors
DE-CIX Management GmbH
Günter Eggers (NTT Global Data Centers EMEA GmbH)
Bernd Fondermann (German Edge Cloud GmbH & Co KG)
Google Germany GmbH
Berthold Maier (T-Systems International GmbH)
Klaus Ottradovetz (Atos SE)
Dr.-Ing. Julius Pfrommer (Fraunhofer IOSB)
Dr. Ronny Reinhardt (Cloud&Heat Technologies GmbH)
Hannes Rollin (T-Systems International GmbH)
Arne Schmieg (German Edge Cloud GmbH & Co. KG)
Sebastian Steinbuß (IDSA e.V.)
Dr. Philipp Trinius (T-Systems International GmbH – Telekom Security)
Andreas Weiss (EuroCloud Germany)
Dr. Christian Weiss (Deutsche Telekom AG)
Dr. Sabine Wilfling (Scheer GmbH)

Current as at
June 2020

Design and production
PRpetuum GmbH, 80801 Munich

You can obtain this and other brochures from:
Federal Ministry for Economic Affairs and Energy,
Public Relations Division
Email: publikationen@bundesregierung.de
www.bmwi.de

Central ordering service:
Tel.: +49 30 182 722 72
Fax: +49 30 181 027 227 21

Content

Disclaimer

This document summarizes fundamentals of GAIA-X, comprising all relevant definitions, concepts, and architectural aspects; especially new GAIA-X participants are encouraged to read it diligently. Nevertheless, this document represents work in progress. As such, it consolidates the current status of discussion and will be subject to future improvements and extensions. The contents encompass several levels of detail, ranging from abstract design principles down to technical elaborations.

1 Introduction

GAIA-X is set to be an Infrastructure and Data Ecosystem according to European values and standards. This overall mission drives its architecture.[1] The architecture employs digital processes and information technology to facilitate the interconnection between all participants in the European digital economy. By leveraging existing standards, open technology and concepts, it enables open, consistent, quality-assured and easy-to-use innovative data exchange and services. Additionally, GAIA-X will become a facilitator for interoperability and interconnection between its Participants, for data as well as services.

1.1 Objectives

Digital Sovereignty is the power to make decisions about how digital processes, infrastructures and the movement of data are structured, built and managed. The GAIA-X architecture outlines technical solutions to establish Digital Sovereignty according to EU standards.

One particular important aspect of Digital Sovereignty is Data Sovereignty. Data Sovereignty is the execution of full control and governance by a Data Owner over data location and usage. By applying the core architectural principles outlined below, GAIA-X will enable Providers and Consumers to participate in a digital sovereign ecosystem. GAIA-X builds on a unique selection of technological approaches to bring digital sovereignty to life:

- Federation: Supports standardized access to GAIA-X as well as multiple decentralized implementations. This way, a rich digital ecosystem is fostered.
- Self-Descriptions and Policies: The basic elements on a technical level for the selection, initiation and coordination of interactions between Providers and Consumers. Self-Descriptions represent GAIA-X offerings. Policies represent requirements. By matching both, Provider and Consumer can start to interact within the GAIA-X ecosystem.
- Identity and Trust: Helps GAIA-X Participants to verify that their engagement with others and the services they use are plausible, authentic and backed by Self-Descriptions and Policies.

In particular, GAIA-X is aligned with the European Data Strategy[2], which aims to create a genuine single market for data, and is open to data from across the world. Data may encompass personal, as well as non-personal data, including sensitive business data. The intention is to provide businesses an easy, safe and secure way to an almost infinite amount of high-quality industrial data.

The objective is to design and implement a data sharing architecture (including standards for data sharing, best practices, tools) and governance mechanism, as well as an EU federation of cloud infrastructure, related infrastructure and data services.

1.2 Architecture Principles

The following architecture principles are directly derived from the vision and objectives of the architecture. They represent the core values this architecture should comply with.

1. **Openness and Transparency:** The specification and documentation of GAIA-X technologies and architectures will be accessible to GAIA-X Participants worldwide. The technical steering and roadmap of GAIA-X is done in public and the involvement of private sector players is disclosed. Everyone's contributions are welcomed. Technology choices will be made in order to encourage distribution of collaboratively created artifacts under open source licenses. GAIA-X is aware that these technologies are evolving and is open to future innovation and standards.

1 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.html

2 A European Strategy for Data https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

2. **Interoperability:** All GAIA-X Participants will be able to interact with each other in a well-specified way. This architecture describes the technical means to achieve that but is agnostic to and works beyond specific implementations.

3. **Federated Systems:** GAIA-X specifies federated systems of autonomous Providers, tied together by a specified set of standards, frameworks, and legal rules. The federation supports decentralization and distribution.

4. **Authenticity and Trust:** 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.

1.3 Architecture Guidelines

The following architecture guidelines enforce compliance with GAIA-X's vision and principles. They ensure that the architecture is for the benefit of all GAIA-X Participants.

In order to fulfill its vision and principles, the GAIA-X architecture imposes technical guidelines. Every Participant will directly benefit, as the architecture is built on them.

1. **Security-by-design:** GAIA-X puts security technology at its core to protect every Participant and system who is part of a GAIA-X eco system.

2. **Privacy-by-design:** The European Union puts special emphasis on privacy regulations. In order to comply, this architecture already fundamentally considers all privacy-related aspects.

3. **Enabling federation, distribution and decentralisation:** The core values should be reflected in the engineering choices. This means that it is not a goal to build up centralized, homogeneous, isolated solutions. Instead this architecture takes into account approaches like federation, distribution and decentralization, as detailed in a later chapter.

4. **Usage-friendliness and simplicity:** State-of-the-art user experience, open standards and protocols, and streamlined processes will be crucial for GAIA-X adoption and acceptance. Between two behaviorally equal alternatives, the less complex one is to be preferred.

5. **Machine-Processability:** All GAIA-X artifacts (like requests, descriptors, notifications or messages, including Self-Descriptions and policies) are machine readable. For the exchange of these artifacts, systems expose APIs ("Application programming interfaces") as the primary means of interaction in GAIA-X. Human User Interfaces will leverage APIs to enable the interaction of humans with GAIA-X. Automation is supported by this architecture.

6. **Semantic representation:** By building on machine-processability, it is ensured that a GAIA-X data model is established, which carries the semantics of the ecosystem and effectively delivers interoperability. Core elements for semantic representation are policy requirements and Self-Descriptions, enabling the translation of actual use cases into digital processes.

1.4 Architecture Overview

The GAIA-X ecosystem as a whole is structured into a Data Ecosystem and the Infrastructure Ecosystem.

Activity in the Infrastructure Ecosystem (see Section 4.1) is focused on providing or consuming infrastructure services, which in GAIA-X are represented primarily by the Asset called Node (see also section 2.1).

In Data Ecosystems (see Section 4.2), the main Asset is Data (see also Section 2.2). The architecture supports and enables Data Spaces and builds Advanced Smart Services in industry verticals. This way, GAIA-X is

developed in accordance with European Data Strategy and supports innovative data applications and innovation across industry sectors.

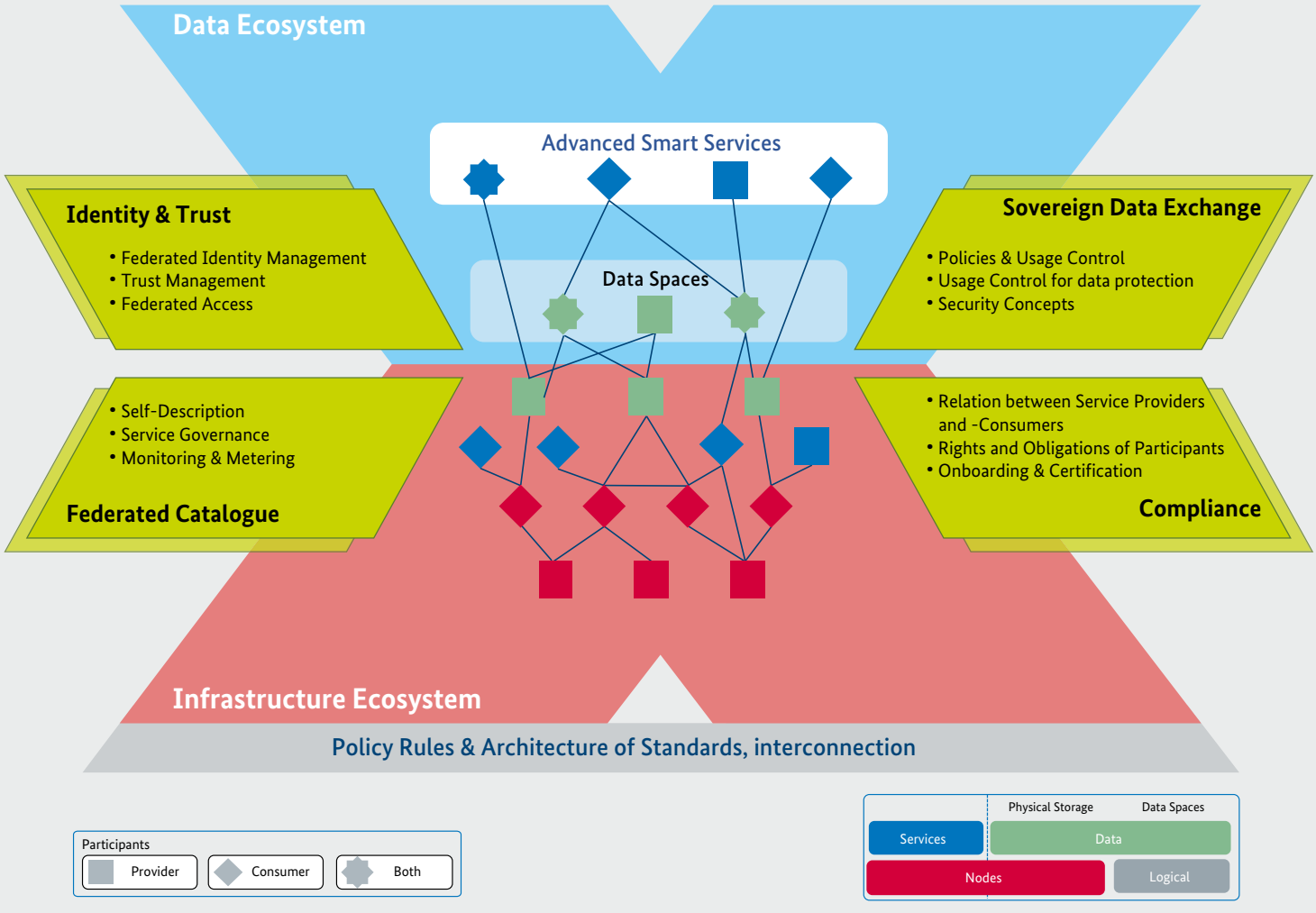
Participants, typically representing organizations engaged within these ecosystems, are differentiated into the major roles, Provider and Consumer (see section 2.3). Yet, other roles exist and will be introduced in later sections. Cases where a Participant is both a Provider as well as a Consumer at the same time, are also possible.

Data and Infrastructure Ecosystems are not separable. The binding element between Providers and Consumers are Services, ultimately also tying Data and Nodes together (see section 2.1).

The whole GAIA-X ecosystem is carried by a common and solid foundation consisting of Policy Rules, an Architecture of Standards of interconnection. Figure 1 gives a high-level overview of the GAIA-X architecture.

GAIA-X defines technical concepts, functionality for the federation and interoperability (such as for Identity and Access Management) that apply to the whole GAIA-X ecosystem. GAIA-X takes on an orchestrating role. However, it is not involved in individual transac-

Figure 1: High-level overview of the GAIA-X architecture showing the major architecture elements and functions accompanied by the Federation Services.



tions between Participants. Instead, GAIA-X provides an opportunity for Providers to enhance their existing isolated offerings to become GAIA-X-enabled.

To bring the architecture principles to life, a set of Federation Services is defined, implemented and operated. The term Federation Service relates to infrastructure services, as well as organizational support functionality, such as onboarding and certification.

Federation Services are grouped into four domains:

Identity and Trust

Identity and Trust is seen from different angles across the whole architectural stack. Detailed descriptions are provided from different viewpoints in the following sections:

- Federated Identity Management: Identity Management describes the provisioning of identifiers also used for authentication. See Section 3.3 for details.
- Trust Management: Trust Management aims at establishing trust for every GAIA-X interaction. Please refer to Sections 3.3 and 3.4.
- Federated Access: Federated Access specifies how access can be managed in a federated fashion. See Section 5.2 for a detailed explanation.

Federated Catalogue (Interoperability)

The Catalogue contains the offerings of Providers in the GAIA-X ecosystem. Section 2 contains concepts and results concerning core architecture elements and their relations to each other.

- Self-Description: See Section 2.4 for details.
- Service Governance: See Section 3 for an in-depth description.
- Monitoring and Metering: See Section 2.8 for more.

Sovereign Data Exchange

The sovereignty of data exchange is ensured by usage control mechanisms and an overarching security concept. In addition, standards for interoperability of the data exchange will be selected.

- Policies and Usage Control: See section 2.6 for details.
- Usage Control for data protection: See Section 5.5 for coverage of data protection.
- Security Concepts: Security concepts are covered in detail throughout Section 5.

Compliance

Security and Data Protection depend not only on technical solutions, but also on organizational and governance aspects.

- Relation between Service Providers and Consumers. See section 3.1 for details.
- Rights and Obligations of Participants. See section 3.2 for details.
- Onboarding and Certification. See section 6 for details.

The following sections provide a detailed discussion of GAIA-X terms and concepts.

2 Core Architecture Elements

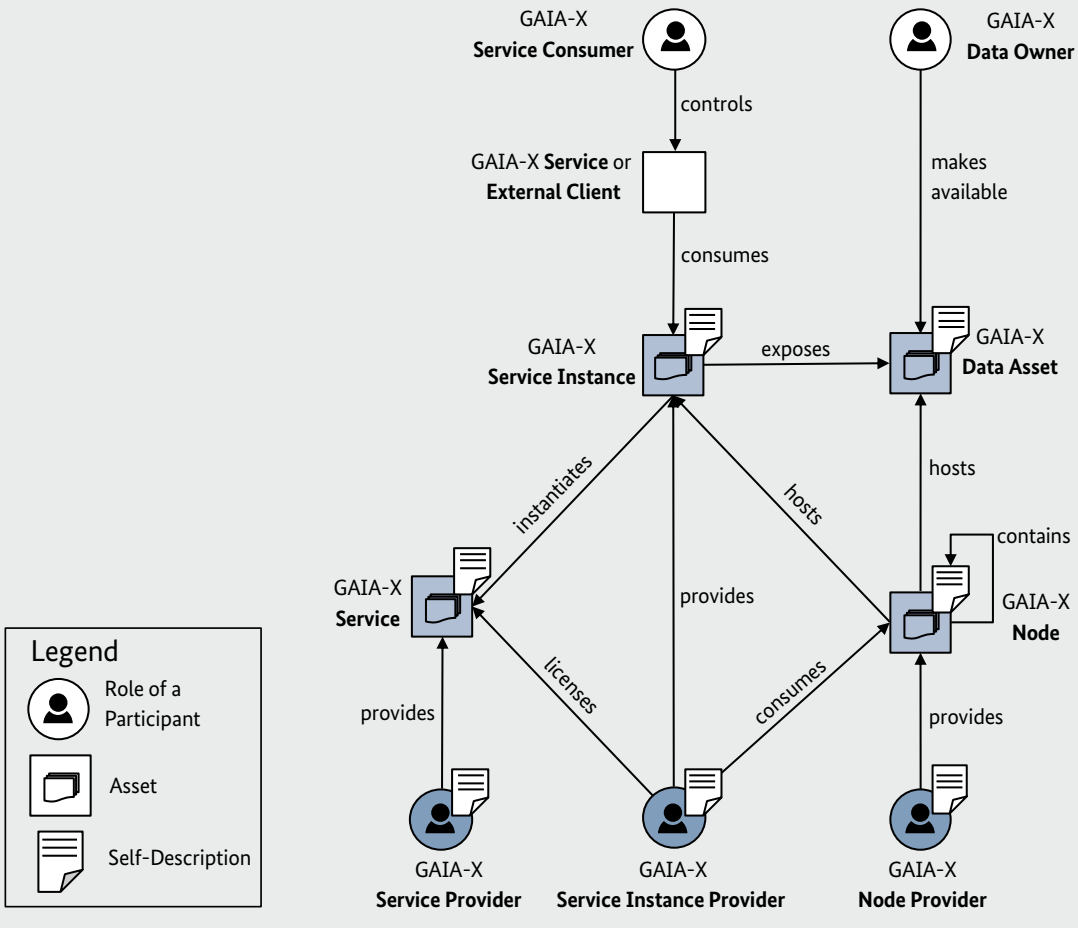
In GAIA-X, an *Asset* is either a *Node, Service, Service Instance* or *Data Asset*. These are all elements of the GAIA-X ecosystem. The term Asset indicates an intrinsic value, as it can be marketed as a product within GAIA-X. The remaining terms are defined in more detail in the following sections. An overview of the interactions between Assets and the GAIA-X Participants is given in the following diagram.

2.1 Services and Nodes

A GAIA-X *Node* is a computational resource. The scope of what a Node can represent can range from data-centers, edge computing, basic hardware, network and infrastructure operation services to more sophisticated, but still generic infrastructure building blocks like virtual machines or containers. Nodes are generic in the sense that different Services can be deployed on them. Nodes expose functional and non-functional attributes via their Self-Description, allowing Node Consumers to select them based on their requirements. One prominent attribute is the Node's geolocation.

Hierarchies of Nodes are supported by GAIA-X, so Nodes can contain further Nodes as children. An example for this is a Node representing a pan-European Node Provider that is structured into country

Figure 2: Major relations between GAIA-X Assets and GAIA-X Participants. Participants can take on multiple roles.



regions, which are themselves structured into data center locations, racks and individual servers, which themselves are exposed as GAIA-X Nodes.

A GAIA-X *Service* is a cloud offering. Services can be standalone or built in relation to other GAIA-X Services by turning them into more complex service networks. The term Service does not favor any of the common as-a-Service concepts like Infrastructure-as-a-Service, Platform-as-a-Service and so on. Services are offered by a GAIA-X *Service Provider* and consumed by GAIA-X *Service Consumer*.

A GAIA-X *Service Instance* is the realization of a Service on Nodes. Every Service might use a single Node or run distributed on multiple Nodes. When a particular Service runs on top of another Service, *Service Cascades* are formed.

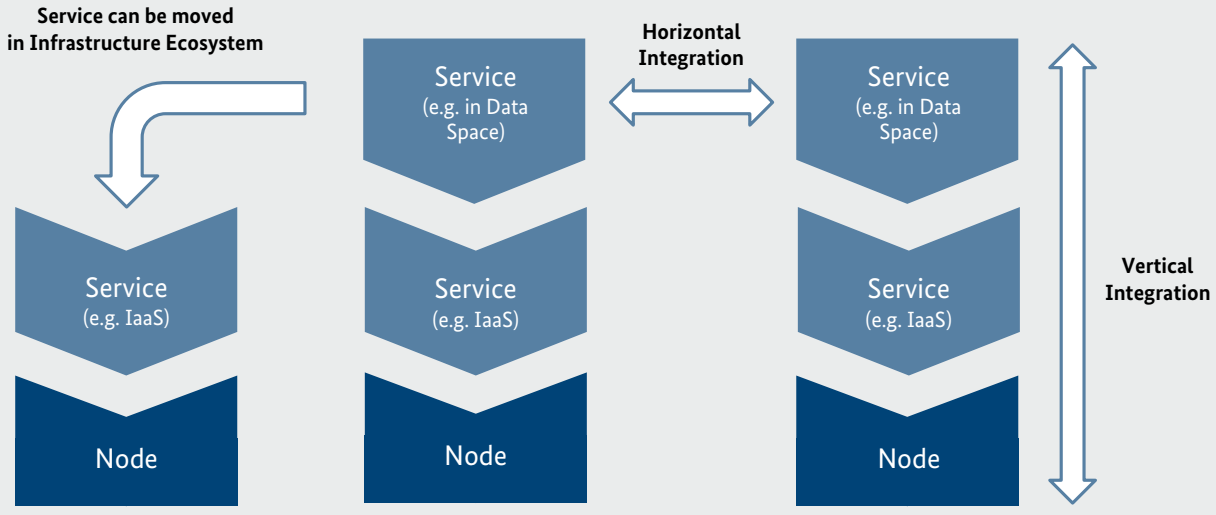
2.2 Data Assets

A GAIA-X *Data Asset* is a data set that is made available to Consumers via a Service that exposes the Data Asset. Consumers and Providers can also host private data within GAIA-X that is not made available (and hence not a consumable Data Asset).

Data Assets are exposed and provided by GAIA-X Services, where they can be searched and consumed by another GAIA-X Service or a GAIA-X Participant. From this, it follows that data being provided or consumed by a GAIA-X Service is hosted on a GAIA-X Node. A GAIA-X Participant is the Owner of a Data Asset. This must not necessarily be the same Participant as the Provider of the Service that exposes the Data Asset.

While the structure and the content of the data being used is not of relevance for the GAIA-X architecture, the GAIA-X architecture covers metadata and mechanisms to make data an exchangeable and tradable good. As the capability of Self-Description is a major aspect of the GAIA-X Architecture, Data Assets provide a Self-Description as well. This mechanism enables exchange, sharing and brokerage of data between GAIA-X Services, and between GAIA-X Services and non-GAIA-X Services.

Figure 3: Possible horizontal and vertical service integration in GAIA-X



Self-Descriptions for Data Assets should include the Owner, usage policies and provenance details, technical descriptions (data scheme, API,...) and content related descriptions. The Self-Description can provide additional details on the Data Asset, like data quality or legal aspects.

Based on the mechanism of Self-Descriptions as outlined above, a Data Asset is able to specify its own requirements with regard to Security and Data Protection as well as other administrative requirements, e.g. data lifecycle. See also the Section on Usage Control Policies.

2.3 Consumer and Provider

A GAIA-X ***Participant*** is a natural or legal person (and their representatives) that can take on one or a multiple of the following roles: Provider, Consumer, Data Owner, Visitor. The combination of multiple Roles by one GAIA-X Participant depends on the respective Business Case.

Users are technical accounts derived from a Participant. As an example, if a company becomes a GAIA-X Participant, there can be many employees of that company with individual accounts. Actions performed by a User are made on behalf of the Participant from which the User is derived. See Section 3.3 on Identity and Trust Management for details.

All Nodes, Services and Service Instances have an associated Provider. The Service Instance and Data Asset merit a more complete description of the interaction between roles:

- Service Instance Provider: Service Instance Providers provide Service Instances, which they instantiate on one or more Nodes. Service Instance Providers are often also Consumers of Nodes and Services (which they can license for the instantiation). Furthermore, Service Instances can consume further Service Instances on which they depend.
- Data Owner: Data Assets are exposed by a Service Instance. The Provider of the Service Instance is not necessarily the same Participant as the Data Owner. An example for this is a Database Service Instance provided to Consumers from a target industry. The Service Instance can make the data available to the Data Owner itself. But the data can also be exposed to further Participants, for example, as part of a Data Ecosystem. In this case, the Data Owner can attach restrictions to the usage of his data in the form of Policies.

2.4 Self-Description

GAIA-X ***Self-Descriptions*** express characteristics of Assets and Participants. A GAIA-X Self-Description describes properties and claims of an Asset or Participant. Self-Descriptions are tied to the ***Identifier*** of the respective Asset or Participant. The Providers of an Asset are responsible for the creation of the respective Self-Description. Trusted parties can sign portions of the Self-Description to establish trust.

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

- Discovery of Assets in a Catalogue
- Tool-assisted evaluation, selection and integration of Service Instances and Data Assets
- Enforcement, continuous validation and trust monitoring together with Usage-Control Policies
- Negotiation of contractual terms concerning Assets and Participants

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

- Machine-readable and machine-evaluable
- Technology-agnostic
- Adhering to a generalized schema
- Interoperable, following standards in terms of format, structure, and included expressions

- Flexible, extensible and future-proof in terms of adding new properties and property classes
- Navigable and uniquely referenceable from anywhere, in a decentralized fashion
- Expressive semantics, uniquely defined by a defined schema vocabulary
- Accompanied by statements of proof (e.g. certificates and signatures), making them trustworthy by providing cryptographically secure verifiable information

The Self-Descriptions refer to other GAIA-X Self-Descriptions. These relations can be expressed in a graph data structure with typed relations. This is called the GAIA-X *Self-Description Graph*. The Self-Description Graph can be seen as a set of relation triples. For example, a textual representation:

```
(OKORO, implements, ArchiveStorage)
(ArchiveStorage, hostedOn, NodeABC123)
(NodeABC123, providedBy, NodeProviderA)
```

Future GAIA-X Catalogue Services implement query algorithms on top of the Self-Description Graph. Furthermore, certification aspects and usage control policies can be expressed and checked based on graph information that cannot be gained from individual Self-Descriptions. For example, a Service Instance cannot depend on other Service Instances that are deployed on Nodes in a foreign jurisdiction.

A Self-Description includes the Identifier of the Asset or Participant, metadata and one or many descriptor sections. The descriptor sections are named Testimonials. They contain one or more claim statements, comprised of subjects, properties and values. Metadata describe Self-Descriptors and Testimonials by an identifier and additional properties such as issuing timestamps, expiry data, issuer references and so forth. Testimonial can have references to other Self-Descriptors that link to the particular subject. Each Testimonial can have a cryptographic signature wherein trusted parties verify the contained claim statements.

Figure 4: Self-Description assembly model

Figure 5: Example for Claim Statement

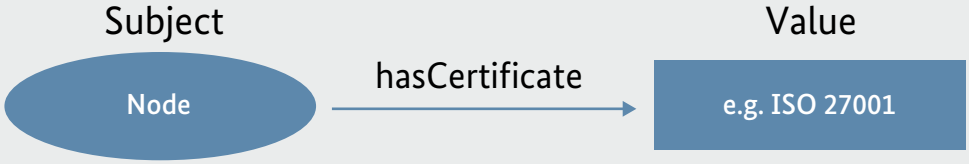
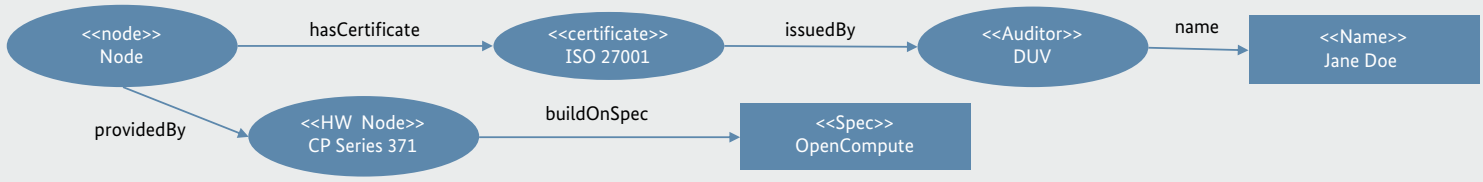


Figure 6: Linked claim statements as a graph representation



The Self-Description itself can have a cryptographic signature, including an initial set of Testimonials. Further Testimonials can be added to the Self-Description later on, but trust for them is not covered by the signature for the overall Self-Description (Figure 4).

Claims are expressed using subject-property-value relationships following resource description standards. As an example, the certification of a Node can be expressed as in Figure 5.

The generic data model for claims is powerful and can be used to express a large variety of statements. Individual claims can be merged together to express a graph of information about an asset (subject). For example, whether a Node is certified by BSI with hardware CP Series 371 based on an OpenCompute Specification[3] is expressed as shown in the Figure 6.

To get a common understanding of the meaning and purpose of any property within the claim statement, semantic description techniques are used to express the objects and properties that are linked to existing and common definitions or to a defined GAIA-X schema. The declarative representation of GAIA-X schemas will build upon Linked Data Standards like RDF/OWL[4] and JSON-LD[5] and represent these in a common format (e.g. JSON[6]) to enable broad adoption and tooling. GAIA-X builds upon existing standards for schema definitions, for example based on W3C schema definitions[7] to get a common understanding of the meaning and purpose of any property and claim statement.

Mandatory and optional claim statements for the Self-Descriptions are semantically defined in an extensive hierarchy of Self-Description Schemas. Figure 7 shows mandatory elements of the top-level Self-Description Schemas.

Individual claim statements as attributes are referred for simplicity. A number of attribute categories will be defined. A Self-Description attribute category describes any number of Self-Description attributes that have a common conceptual basis.

The requirements for provided attributes are kept to a minimum to enable a broad range of Providers, Nodes, Services and potential Consumers to participate in GAIA-X.

3 https://www.opencompute.org/

4 McGuinness, D. L., & Van Harmelen, F. (2004). OWL web ontology language overview. W3C recommendation, 10, 2004.

5 Sporny, Manu, Dave Longley, Gregg Kellogg, Markus Lanthaler, and Niklas Lindström. "JSON-LD 1.0." W3C Recommendation, 2014.

6 JSON-LD For Linked Data. https://json-ld.org/

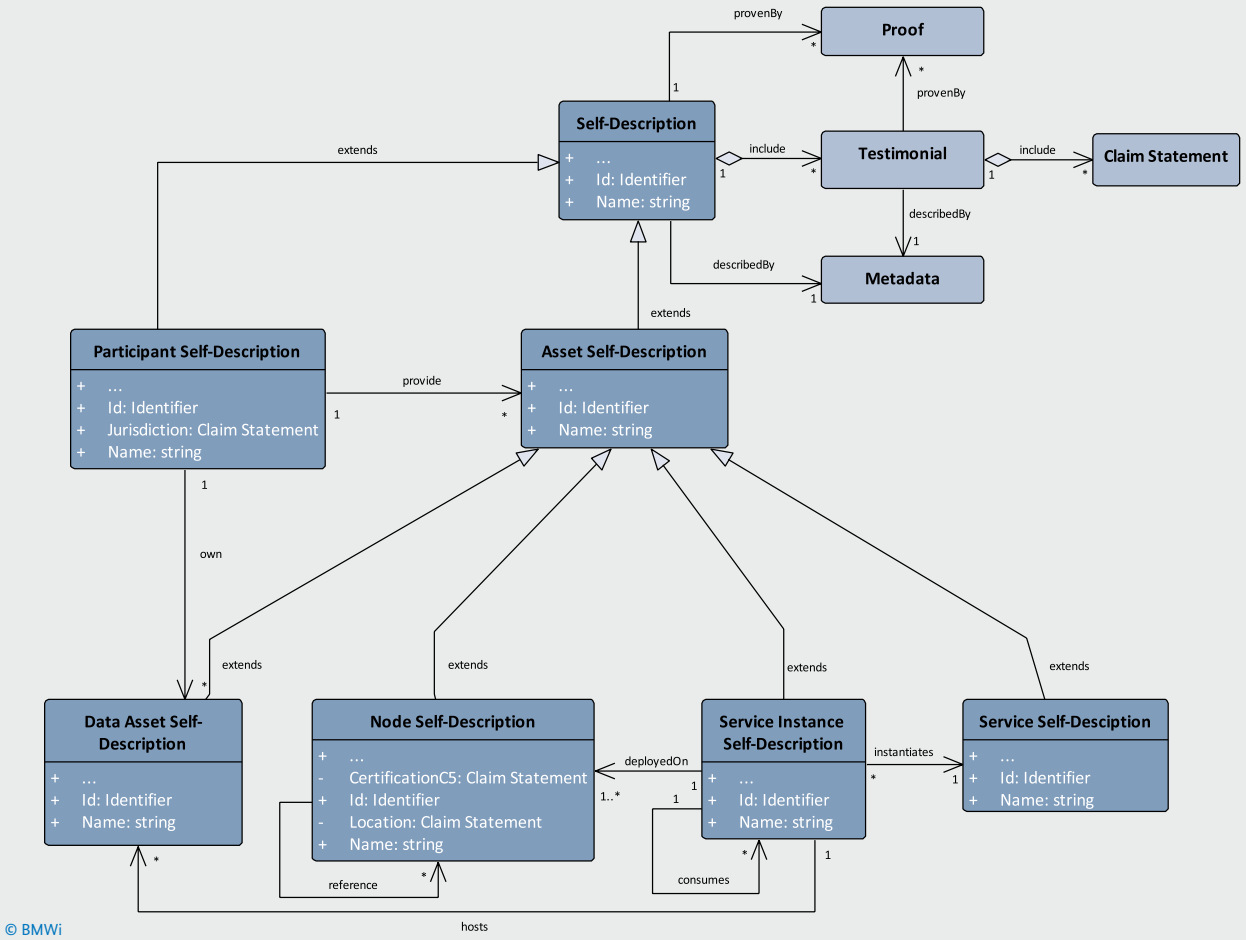
7 https://schema.org/; W3C RDF https://www.w3.org/RDF/ or W3C Verifiable Credentials Data Model https://www.w3.org/TR/vc-data-model/

Examples of Attribute Categories per Self-Description in GAIA-X are discussed below.

- **Providers:** Every Provider of Nodes and Services 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 2 (Basic Architecture Elements). The Attribute Categories comprise availability, connectivity, hardware, monitoring, physical security and sustainability.
- **Services:** Self-Descriptions of Services describe Services as defined in Section 2 (Basic Architecture Elements). Attribute Categories for Services 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.

A first, non-exhaustive collection of relevant attribute classes is attached in appendix B.

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



2.5 Catalogue

The concept Self-Description is the foundation of the federated GAIA-X ***Catalogues***. Catalogues are the main building block for the publication and discovery of Self-Descriptions of Assets and Participants. To satisfy Consumer needs and to objectively find the best fitting offerings in the tangle of registered Assets, an open and transparent query algorithm is implemented without any GAIA-X internal ranking. Beside search functionality, a graph-based navigation interface is provided to traverse the complex tangle of offered Services, Nodes and linked Self-Descriptions, including the attached claims with chain of trust statements. Consumers can verify each Self-Description individually and decide which one to select in a self-sovereign manner – GAIA-X does not act as a runtime intermediary or broker.

Catalogue Federation

Multiple federated catalogue software instances can be operated independently at different locations. Self-Descriptions in a Catalogue are either entered directly by the respective Provider, imported from another federated GAIA-X Catalogue or even imported from an external collection. The GAIA-X Catalogues act as an access point to information that verifies the content of Self-Descriptions. However the origin of a Self-Description must, be known, to prevent abuse.

A Catalogue can represent different views on existing offerings, such as domain-specific selections of Assets. This feature will be helpful as long as the Consumer is aware and able to switch off any catalog restriction in a simple way and get access to all offered Assets.

Portal and API Integration

For integration purposes, e.g. DevOps automation tools, the Catalogues provide access through an application programmer interface (API). With this simple toolbox in hand, existing integrators, cloud providers or anyall are free to integrate the GAIA-X offerings into their own offerings. Another option to offer Assets to Consumers is a graphical portal frontend that is using the same API and base functionality. To support an ease concept, custom filter and policy definitions with domain specific languages (DSL) are introduced. The policy and query statement definitions facilitate filtering to reduce the complexity and make it possible to find the best matching Asset based on the Self-Descriptions and to find relations between Assets in a human-friendly manner that can be automated when necessary.

2.6 Policies and Usage Control

In GAIA-X, Policies define a set of restrictions. They can be viewed as the counterpart of the Self-Description. It describes invariants that must be assured in a software execution environment based on the information from the Self-Descriptions of Assets and Participants.

Policies are also dynamically evaluated at runtime, and not only during onboarding and instantiation. Suitable alerting and escalation measures can be linked to Policies to handle changes in a dynamic environment.[8]

2.6.1 Data-Centric Usage Control

While access control restricts access to specific resources (e.g., a Service or a file), data sovereignty is additionally supported with Data-Centric Usage Control. The goal of Data-Centric Usage Control is to make sure that specified usage restrictions and obligations are realized even after access to data has been granted. Therefore, Usage Policies must be bound to data being exchanged and continuously controlled during the data flow of processing, aggregating or forwarding. Usage Policy enforcement is subject at sys-

8 See the position paper by the Industrial Data Space Association for possible technical refinements of the Usage Control concepts: https://www.internationaldataspaces.org/wp-content/uploads/2019/11/Usage-Control-in-IDS-V2.0_final.pdf

tem design, configuration and runtime. It also supports auditing after data processing by creating auditable logs and provenance tracking. The following examples illustrate security requirements that cannot be achieved using traditional access control, but can be achieved with Data-Centric Usage Control:

- **Secrecy:** Classified data must not be forwarded to Nodes or Services which do not have the required certification.
- **Separation of duty:** Two data sets from competitive entities must never be aggregated or processed by the same Service.
- **Usage scope:** Data must never leave the Node or Service to an external endpoint.

The project GAIA-X identified Usage Policy Enforcement as an important architectural aspect to achieve Data Sovereignty. In this context important concepts have to be defined for the context of a federated cloud system:

1. Specification of Usage Policies: The Usage Policies specified by a data provider must be both machine and human readable, and therefore interoperable. The underlying specification language and the required capabilities need to be defined. This includes:
   a. Capabilities to express technical, organizational and legal conditions.
   b. The capability to create and maintain usage policies (administration).
2. Enforcement of Usage Policies: Different kinds of obligations require different mechanisms for enforcement. Technical enforcement including auditability would be preferred for various scenarios, but this is often hard to achieve. Therefore, organizational measures to enforce usage policies must also be considered, as well as legal measures. In GAIA-X, possible and required measures for the enforcement of usage policies need to be discussed and defined.

2.6.2 Policy-Driven Workload Control

In GAIA-X, the workload can shift between Nodes at runtime. Service Instances can be deployed on multiple Nodes and can move between Nodes. Furthermore, Service Instances that consume other Service Instances can switch between equivalent offerings.

Policy-Driven Workload Control requires that the definition of restrictions confirm to the mobility of Service Instances. For example, certain tasks must be performed by Service Instances from Providers with a defined certification level, or only Nodes within a given jurisdiction can be used.

2.7 Interconnection and Networking

The GAIA-X target architecture aims at creating two ecosystems, a Data Ecosystem and an Infrastructure Ecosystem. Data and infrastructure should be combinable in nearly arbitrary ways to enable movement of

Figure 8: High level overview of interconnection and networking within GAIA-X.

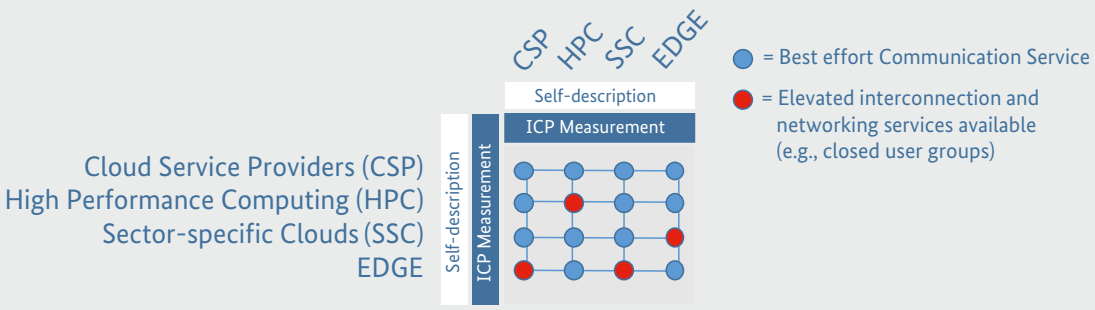
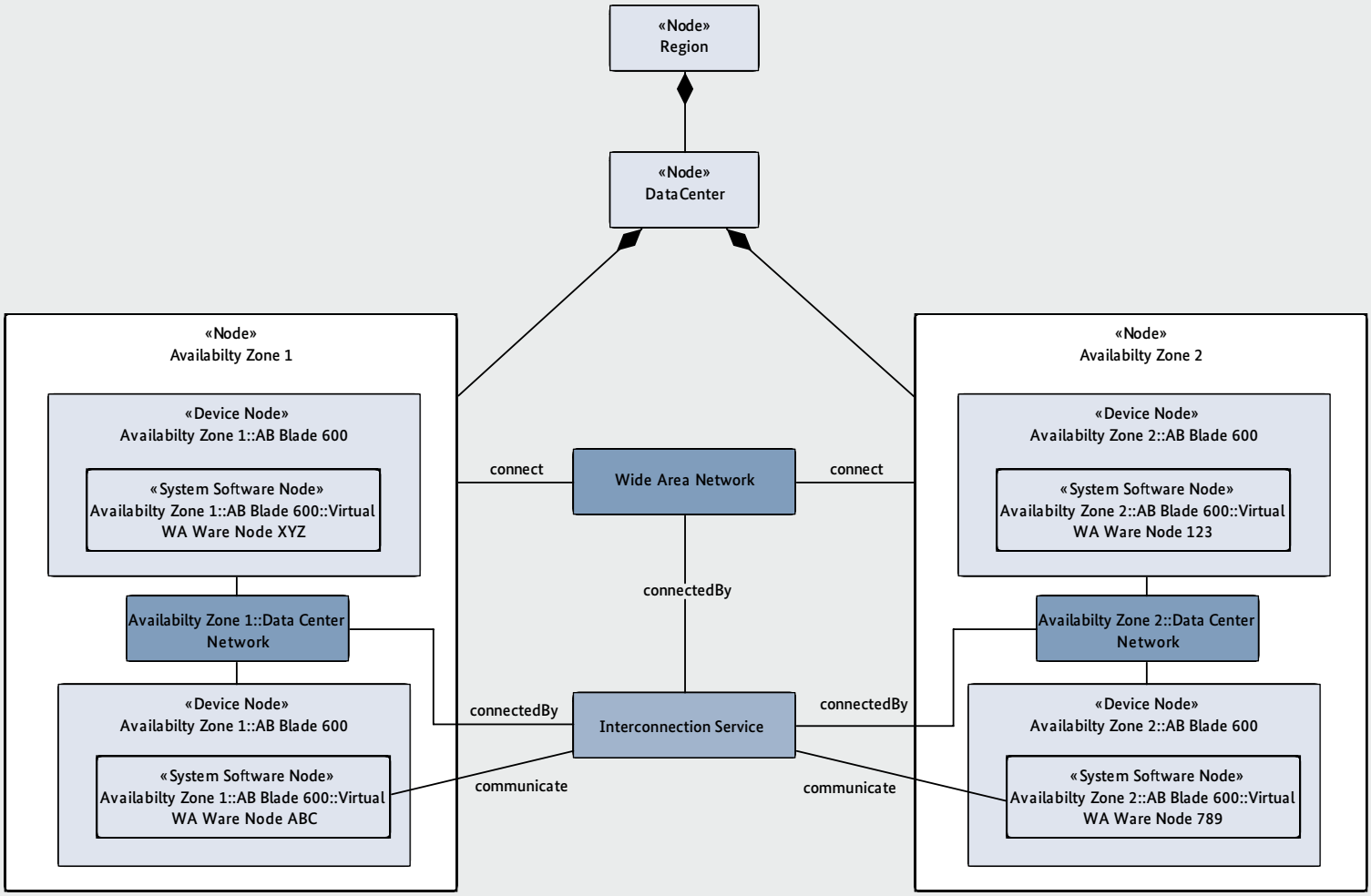


Figure 9: Simplified example of interconnection between Nodes.



data and services in a federated cloud architecture. However, regardless of their abstract virtual locations, services and data have a physical location. Obviously, the central ideas of GAIA-X require communication support by design. Thus, GAIA-X integrates interconnection and networking aspects into the architecture. The architecture considerations on networking and interconnection rely on three building blocks as described in the following.

- **Self-Description:** networking and interconnection are covered by Self-Descriptions (see Chapter 2.4). Self-Descriptions of networking and interconnection aspects exist on two levels: the first is ***cloud providers' internal network***, the second is cloud ***providers' external network***. To date, both are described as GAIA-X Node connectivity attributes. Regarding cloud provider internal networking, the networking hardware of single machines is described as the type and speed of Network Interface Controllers (NICs) (see Appendix B). Regarding

cloud provider external networking, Self-Descriptions cover the external links a cloud provider owns to connect a Node to the Internet ("interconnection"), e.g., links to any upstream network providers such as peering point presences, transit network providers, or other Internet Service Providers (ISPs). Naturally, external networking Self-Descriptions can be tied to a Node representing a larger infrastructure, such as a cloud provider's data center presence or even a whole cloud region (see Appendix B). The purpose of interconnection and networking Self-Descriptions is to support the GAIA-X matching process of Services and their execution environments, i.e., the selection process via the Catalogue.

- **Inter cloud provider (ICP) measurements:** describing connectivity between GAIA-X Nodes/Providers is an important factor, however it may be difficult to guarantee that packets travel across certain links between cloud providers without deeply interfering with routing decision made by possibly being many different organizations. Consequently, the approach of self-describing connectivity is complemented by connectivity measurements, e.g., latency measurements. By incorporating measurements modules into the overall GAIA-X architecture, GAIA-X is able to provide a consistent view of the connectivity between cloud Providers and Consumers. Together with the information contained in Self-Descriptions, connectivity measurements are a valuable input for many scenarios, e.g., optimizing the selection of Nodes from multiple cloud providers for multi-cloud scenarios or finding a cloud provider's optimal data center to serve a certain consumer or EDGE provider. However, measurement information can only give probabilistic guarantees on Quality of Service (QoS) parameters such as latency and throughput.
- **Interconnection and networking services:** interconnection and network providers can offer interconnection and networking services similar to other cloud Service Providers. This covers cloud provider internal networking (e.g., VLANs, load balancing, etc.) as well as cloud provider external networking. In the external case, GAIA-X can provide interconnection and networking service offerings to customers that provide elevated services compared to the standard Quality of Service of the public Internet (as described above). Examples for such elevated services could be interconnection with latency and throughput QoS guarantees or secure and isolated communication in closed user groups for sector-specific clouds such as the medical sector.

To date, interconnection and networking services are considered to be within the general GAIA-X architecture because they are modelled them alongside other concepts such as Providers, Nodes, and other cloud services. Moreover, the most relevant attributes required for interconnection and networking are covered in the current draft of Self-Descriptions of Nodes.

In the near future, the specifications of a measurement system for GAIA-X as well as a concept for a measuring, metering and billing network and Strong connectivity services are planned. Moreover, it is planned that an SD-WAN-like approach for the GAIA-X matching process will allow users to specify their networking requirements in terms of QoS and topology, which will be matched to the available services and infrastructure in GAIA-X in the best possible way. Over the long term, the three building blocks Self-Description, ICP measurements, and interconnection and networking services are envisioned to enable the formation of a federated GAIA-X backbone infrastructure.

2.8 Monitoring and Metering

Monitoring is an important component of federated systems and cloud services in particular. Due to a heterogeneous technology landscape, access to monitoring is a technical hurdle for the loose coupling of Services and Nodes from different Providers. Hence, to enable the development of Infrastructure and Data Ecosystems, GAIA-X aims to provide standard mechanisms for monitoring. This does not prevent the exist-

ence of specialized monitoring services with additional capabilities. The topic of monitoring is handled differently for three distinct cases:

1. Logging and Auditing
2. Status Monitoring and Alerting
3. Metering

Monitoring capabilities will be described as part of the Self-Description mechanism so that Consumers can select Services and Nodes according to their Monitoring needs. GAIA-X will not perform monitoring of Services itself. But it is possible that a third party monitors the availability of Services on behalf of other GAIA-X Participants. For example, to supervise Service-Level KPIs that are part of a certification or contractual agreement.

2.8.1 Logging and Auditing

Logging refers to the access to runtime log information that is generated by a Service or Node. This is both used during the development of distributed systems in GAIA-X (including debugging) and at runtime. Some Services and Nodes may require auditing due to legal and contractual requirements. Oftentimes, logs for auditing have to be transferred and stored in a tamper-secure manner on a separate system.

To improve the transparency and to increase the integration of Services from many vendors, standard interfaces are provided.

2.8.2 Monitoring and Alerting

Monitoring in the context of GAIA-X refers to the access to status information of Services and Nodes, as well as alerting. Monitoring is essential for the operation of large-scale distributed applications. GAIA-X will define standard mechanisms and interfaces for monitoring. The monitoring definitions of GAIA-X are on two levels: Technical interfaces for monitoring, as well as conceptual definitions, such as monitoring levels and classifications of monitoring targets. This allows the interoperability of monitoring and operations tools with the full range of Services and Nodes in GAIA-X. Furthermore, since Services can form a Service-Mesh, monitoring information can be aggregated and forwarded in a standard way to increase the visibility a Service Consumer has into the overall system.

Where possible, existing standards are used for the monitoring interfaces. There are two major models for monitoring: Pull-Monitoring where logs can be retrieved by the Customer and Push-Monitoring where updates and alert notifications (with optional filtering) are automatically sent to the Consumer. There can be different levels of granularity and detail for monitoring. The details of the access to monitoring are established between the Provider and Consumer.

All GAIA-X Nodes and Services must have monitoring capabilities. Consumers get monitoring access to Nodes and Services according to the usage agreements they have with the respective Provider. A failure of monitoring on the Provider side is seen as a service outage with respect to Service-Level Agreements.

2.8.3 Metering

Metering is similar to monitoring, but specifically refers to the access to performance indicators and consumption statistics. Metering is not only important for transparency with respect to billing, but also crucial to the resource-efficient scaling and operations of large-scale cloud applications. GAIA-X itself does not act as a billing provider or clearing house. But GAIA-X will define standard interfaces and mechanisms for metering to be used by the Consumers and Providers. Where possible, these are based on existing standards.[9] The availability of standard metering interfaces will be part of the Self-Description of Nodes and Services.

9 For example, ISO/IEC TR 23613: 2020, Information technology – Cloud computing – Cloud service metering elements and billing modes

3 Organization and Governance Viewpoint

GAIA-X is a federated ecosystem with distributed and decentralized components. It's challenging to ensure trust in such an environment, which is why GAIA-X uses these techniques:

- Federated Identity Management
- Decentralized Identifiers
- Cryptographical Verification of Self-Descriptions
- Accreditation and Certification Processes

Identity Management has been defined in ISO/IEC 24760-1[10] and denotes processes handling exchange of identity information. Identity Management is used to manage identification and authorization, so that it's known *who* you are (identification) and *what* you're allowed to do (authorization). While transparency is key, it's important to prevent traceability outside the interacting parties and adhere to the concept of *Self-Sovereign Identity*: Everybody owns and controls their identity without intervening administrative authorities.

To boost confidence in GAIA-X Participants and Assets, cryptographically safe verification based on state-of-the-art protocols will be used. Also note that GAIA-X Identity Management builds upon available technologies.

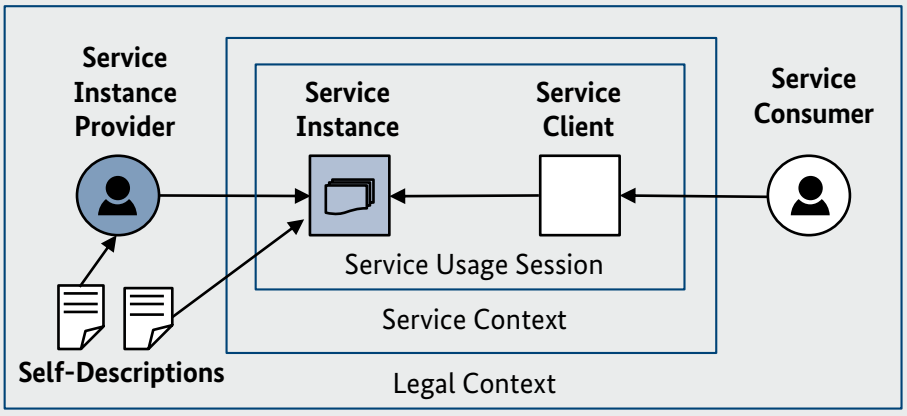
3.1 Relation between Service Provider and Consumer

A *Legal Context* exists between two or more Participants. Legal Contexts are not necessarily explicitly represented in technical systems. Consumption of Services is made inside a *Service Context*, which is the space where Policies live. Service Contexts are part of a Legal Context. One of the Participants must be the Provider of the Service Instance. The other Participant is the Service Consumer. Metering and Billing of Service consumption is tied to the Service Context and done by the Provider.

A *Service Client* is a technical system controlled by the Service Consumer. The Service Client interacts with the Service Instance. A Service Instance can act as a Service Client to consume further Service Instances.

Technical connections between a Service Instance and a Service Client are called *Service Usage Sessions*. Service Usage Sessions are created within a Service Context. The Service Provider and the Consumer verify each other's Identity to enable the Service Usage Session.

Figure 10: Legal Context and Service Context between Service Provider and Consumer.



10 ISO/IEC 24760-1:2019, IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts

A *Policy* is a set of assertions that restricts the behavior and usage of an Asset. Note that both Consumers and Providers may provide a Policy: A *Provider Policy* is a usage restriction (e.g., requiring users to be solvent EU residents), while a *Consumer Policy* restricts the attributes of the Asset to be consumed (e.g., requiring a Node to be physically secured to such-and-such a degree). The Consumer Policy is matched against the Asset's Self-Description, just as the Provider Policy is matched against the Consumer's Self-Description (see also 2.6).

3.2 Rights and Obligations of Participants

Rights and responsibilities of each Participant are summarized in table 1.

3.3 Identity and Trust Management

The GAIA-X *Identity*, which is the key to gain access to the ecosystem, contains a unique identifier and a list of attributes which describe an identity.

In GAIA-X, *Trust* – confidence in the Identity and capabilities of a Participant or Asset – is established by cryptographically verifying Identities using the federated Identity Management of GAIA-X.

Assets in GAIA-X contain capabilities (e.g. GDPR compliance, encryption, certifications, ...) which are stored as attributes in the Self-Description of the individual Asset. These attributes must be painstakingly validated and cryptographically signed to prevent manipulation.

GAIA-X Participants need to trust GAIA-X Assets and Participants. It is important that the GAIA-X Federated Identity Model provides transparency for every-

Table 1: Rights and Obligations of GAIA-X Participants

Participant	Rights and Obligations
Provider	A Provider must pass the GAIA-X registration process so that his identity can be confirmed. A Provider must fulfill GAIA-X Service agreements. After registration, the Provider's responsibilities are commissioning and decommissioning of its provided GAIA-X Assets. Each Asset has its own Self-Description which must be validated. The provided information must be sufficient and correct. A Provider has functional responsibility for its Assets. A Provider has to adhere to agreements negotiated with Data Owners and Consumers.
Consumer	A Consumer must pass the GAIA-X registration process so that his identity can be confirmed. A Consumer must fulfill GAIA-X Service agreements. All Consumers will be treated equally by GAIA-X. Consumers can search Assets according to their requirements. Contract negotiation happens between Provider and Consumer. GAIA-X does not play an intermediary role but supplies trustworthiness for both parties.
Visitor	Visitors can browse, navigate and search for GAIA-X Assets without restrictions. If the Visitor wants to consume an Asset, he must register or login as a Consumer.
Identity Provider	An Identity Provider (IdP) has to comply to GAIA-X legal requirements. An IdP guarantees the identity of GAIA-X Assets and Participants. It is responsible for the Identity Lifecycle Process.
Data Owner	A Data Owner offers data through a Service Provider – Data as a Service. A Data Owner must adhere to the agreements negotiated with a Provider.

Table 2: Identity Lifecycle Process

Lifecycle Activity	Description
Onboarding	The governing body of GAIA-X receives the registration form of the GAIA-X Participant or Asset – the famous Self-Description – which is then validated and signed.
Maintaining	Changes related to GAIA-X Identities are validated and signed by the governing body of GAIA-X. This includes both information controlled by the Participant/Asset and information coming from the IdP.
Offboarding	The offboarding process of a Participant or Asset is time-constrained and includes all dependent GAIA-X Participants and Assets.

one. Therefore, proper lifecycle management is required, covering identity onboarding, maintaining, and offboarding. Table 2 shows the *Identity Lifecycle Process*.

The GAIA-X focus is to provide a trusted, independent digital ecosystem which will span across different domains and countries. To be successful with this endeavor, two concepts are mandatory: identity and trust.

An identity is the unique representation of an individual or asset in the digital world. Identity Management is answering the question, is it really the person or asset, which he/it claims to be. It covers the lifecycle of the identity information starting from creating, changing until deletion of an identity, whereas the function of trust has the function of proofing the predetermined identity. A federated identity is the linking of a digital identity with attributes, which can be spread across different identity management systems.

Within GAIA-X, a federated Identity Management will be facilitated by existing national and international identity providers (IdPs), which can be unique identity provider companies, or it is also possible that existing identities will be handed over by businesses or companies, which are deemed trustworthy by GAIA-X.

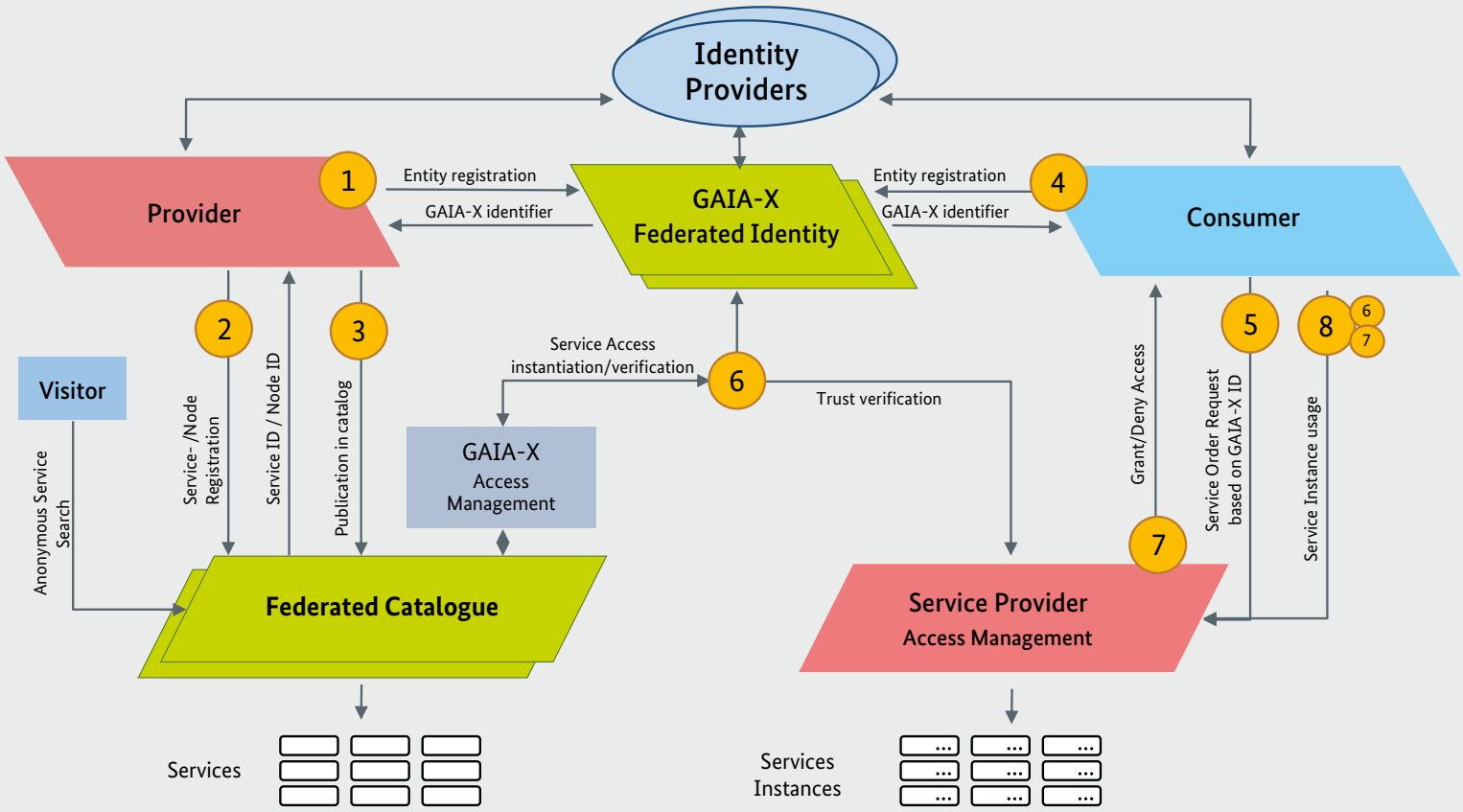
The GAIA-X Identity Management system must be trustworthy and secure and hereby assure individuals and assets that the digital information is handled in such a manner that any kind of manipulation is not possible. The self-sovereignty of the identity has to be fully respected over its complete lifecycle.

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

It is not intended that the GAIA-X Federated Identity Model will limit or influence design and technology decisions and implementations. Instead it should support the incorporation of new solutions and ideas and hereby support the GAIA-X idea of creating a federated digital ecosystem.

Figure 11 will show the actual design of the GAIA-X Federated Identity Model, which will include the outlined proceedings from above. GAIA-X Participants involved are Provider, Consumer, IdP and Visitors. Between them, the trustworthiness must be achieved, as this is the guiding principle for all further digital business. This is realized with the following components involved.

Figure 11: HLD of the Federated Identity Model



HLD of the Federated Identity Model

Components	Description
GAIA-X Federated Identity	This component guarantees identity proofing of the involved Participants to make sure that GAIA-X Participants are who they claim to be.
GAIA-X Federated Catalogue	The Federated Catalogue is a logical combination of a Self-Description repository and search algorithms so that Self-Description-based attribute searches can be processed.
Service Provider AM	The Service Ordering Process will involve the Consumer and the Service Provider. The Service Provider will create the Service Instance and will grant access for the Consumer.

Table 3: Elements of the Federated Identity Model

Steps	Short Description	Detailed Step Description
-	Anonymous Service Search	A Visitor accesses the GAIA-X Federated Identity, browses the GAIA-X Catalogue and starts a Service search query. A list with possible services matching the service search criteria will be displayed to the Visitor.
1	Provider Entity registration	The Provider entity will register in GAIA-X. One of the mandatory fields is the input of the IdP. An IdP must confirm the identity of the provider entity. A GAIA-X ID (identifier) will be provided to the Provider. Result: The Provider is verified and registered in GAIA-X.
2	Service Registration	The Provider is able to register a Service in the GAIA-X Federated Catalogue. A Service ID is generated by GAIA-X and obtained by the Provider.
3	Publication in Catalogue	The registered Service will be published to the GAIA-X Federated Catalogue and is publically available for the search algorithm.
4	Consumer registration	A Consumer will register in GAIA-X. One of the mandatory fields is the input of the IdP. An IdP must confirm the identity of the Consumer entity and can be verified itself by GAIA-X. A GAIA-X ID (identifier) will be provided to the Consumer entity. Result: The Consumer is verified and registered in GAIA-X.
5	Service Order Request	The registered Consumer contacts the Service Provider to order a specific Service.
6	Trust Verification	The Service Provider checks the trust worthiness of the Consumer. The GAIA-X Federated Identity checks the identity via the IdP. The GAIA-X Federated Identity verifies the Service Access (Consumer attributes –> health data) The results will be returned to the Service Provider. Service Provider validates the received attributes and creates an identifier for the Consumer.
7	Grant/Deny Access	Deny: The Service Provider will provide the result to the Consumer. Grant: The Service Provider will trigger the service orchestration engine to create the Service for the Consumer (= Service Instantiation process). The Service Provider will forward the Service Instance identifier to the Consumer.
8	Service Usage	The Consumer is now able to use the ordered Service Instance. During the Service Usage, the Service Provider AM will check/verify for each access the identity of the Consumer to guarantee that the Consumer attribut match the required ones (see step 6/7).

3.4 Trust Framework by certified Self-Descriptions

Beside human trust in identities, GAIA-X Participants strongly request trust in any offered Assets.

Two parties should be able to check immediately when exchanging data or using Services whether the Asset comes from a trustworthy source and fulfills all requirements with valid proof statements.

Trust is established by interpretation of the relevant claims in the Self-Description. This also depends on trusting the party that has signed the claim in the Self-Description.

GAIA-X will define a trust framework on established standards and EU regulation that incorporates with

Usage Policies and Self-Descriptor statements to answer typical Consumer questions: is the selected service GDPR conform[11], is the issued certification statement really from an authority that I trust, are the Service or Nodes attested by GAIA-X, or in general can I trust any property or statement expressed in the self-descriptor.

The technical trust framework requires cryptographical material and verification methods for trustworthy operations. It is under consideration that a decentralized public key infrastructure concept (DPKI) in combination with decentralized identifiers (DID)[12] be used, to support the privacy and self-sovereign requirements and gain the chain of trust without the need of a global and traceable unique ID across all providers.

3.5 Service Classes

GAIA-X provides *Service Classes* – think of labels or quality seals – to simplify Service choice and to introduce different Service qualities, such as noteworthy security, performance, resilience, or sustainability.

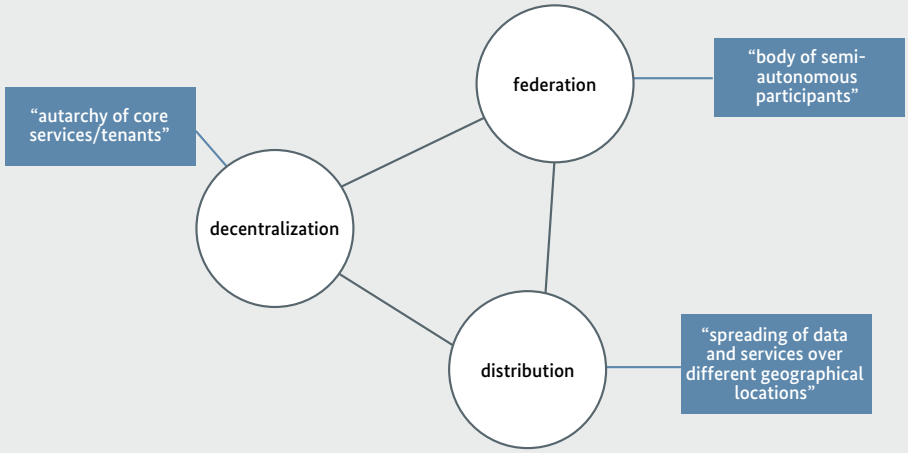
As elaborated in section 6.2, Services – like all Assets – pass through an onboarding process where their Self-Description is validated. Once completed, the Service will be registered and becomes visible in the Federated Catalogue. When all post-registration processes are finalized, which may include time-consuming and manual procedures, the Service will be labeled as belonging to a specific Service Class, if the appropriate combination of attributes is present. The label of the "classy" Service is then included and highlighted in the Catalogue.

Service Classes describe qualitative categories, but they are unrelated to the concept of Assurance Levels (see Section 6). Naturally, the concept of Service Classes could be extended to other Assets like Nodes and Data Assets.

3.6 Federation, Distribution and Decentralization

The internet has many examples where it makes use of federation (e.g. Autonomous Systems), distribution

Figure 12: Relationship between federation, distribution and decentralization



11 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

12 IEEE Decentralized Identity; https://ieeexplore.ieee.org/document/9031542
W3C Decentralized Identifiers; https://www.w3.org/TR/did-core/

(Domain Name System) or decentralization (IP address assignment).

Acceptance of GAIA-X depends on key properties regarding the control over Nodes and Services as well as how Participants interact and establish a trusting relationship with each other. Therefore, GAIA-X embraces a federated, distributed, decentralized and trustworthy architecture.

Distribution fosters the usage of different Nodes, Services or Providers spread over geographical locations, potentially the whole world. The Node concept itself is a distributed concept, other concepts of GAIA-X will be distributed, too.

Decentralization will ensure GAIA-X is not controlled by the few. Decentralization strengthens the participation of everyone, even small Participants. 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 is able to reflect all requirements of its Participants.

Finally, federation is key to supporting interaction between Participants, fosters and ease-of-choice for everyone while preserving decentralization and distribution. Federation technically enables connections and a Web of Trust between different (distributed, decentralized) parts of the ecosystem. It ensures that GAIA-X can be one common large ecosystem and prevents unconnected silos or the break-up into numerous de-facto ecosystems.

4 Ecosystem Viewpoint

GAIA-X fosters the development of ecosystems for infrastructure and data services. GAIA-X ecosystem is enabled by interoperability on a technical and organizational level. This allows the seamless integration and use of offerings across vendors. GAIA-X specifically addresses the following topics to enable interoperability in ecosystems (infrastructure + data):

- Identity and Trust Management
- Discovery (Catalogue, Self-Description)
- Standards for Interoperability (Architecture of Standards)
- Enforceable Usage Policies
- Contracting (Between Provider and Consumer)
- Monitoring and Metering

Two types of ecosystems are described in more detail in the following sections:

- Infrastructure Ecosystem
- Data Ecosystem

These ecosystems are tightly linked. They have, however, sufficiently distinct concerns to warrant separate descriptions.

4.1 GAIA-X Infrastructure Ecosystem

The Infrastructure Ecosystem exists of services and necessary infrastructure components to store, transfer and process data.

The federated GAIA-X concept provides Services across multiple Providers and Nodes of the ecosystem.

Infrastructure services can range from low level services like bare metal computing up to high sophisticated offerings, such as high-performance computing.

Strong connectivity services ensure secure and performance data exchange between the different providers and services.

With open interfaces and the combination of individual Service Providers, high-value offers are conceivable, such as High Availability and Disaster Recovery.

A strong open Infrastructure Ecosystem is the foundation of Digital Sovereignty.

In the following, the role and incentives for the participation of the different stakeholders within GAIA-X will be described. ***As GAIA-X is defined to be an open system, the following list is non-exhaustive and may be extended in the near future***. The stakeholders are discussed in a bottom-up fashion starting with the Infrastructure Ecosystem which provides the base of GAIA-X.

- **Cloud Service Providers:** the group of Cloud Service Providers covers all sorts of general-purpose cloud infrastructure providers ranging from small regional providers, specialized providers like bare-metal providers to large hyperscalers. Cloud Service Providers can describe all relevant criteria of their offers to GAIA-X and will be listed in the Catalogue. This provides visibility of cloud Service Providers' unique selling points as well as transparency of their offers to customers. GAIA-X will ensure the correctness of Self-Descriptions where necessary and will thus create an environment of trust for Customers to use federated cloud infrastructures across cloud Service Providers while avoiding lock-ins.
- **High Performance Computing:** this group covers providers of high-performance computing resources such as universities and industrial labs. The general openness of GAIA-X is a good fit for the research community, as their resources are often funded by the public. Moreover, the federation approach of GAIA-X securely bundles resources whenever needed, for scientific workloads or cooperation between industrial and academic partners. An additional incentive is the possibility to integrate and share research data in specialized Infrastructure Ecosystems, which is a main driver in some areas of research (e.g. the human genome research).

- **Sector specific Clouds:** the group is comprised of cloud Service Providers offering services to specific sectors, e.g., cloud Service Providers adhering to regulations necessary for processing medical data. Their role is similar to general purpose cloud Service Providers but is addressing a subset of all GAIA-X Customers with special requirements. In addition, sector specific cloud providers can take advantage of the GAIA-X Infrastructure Ecosystems by complementing their hardware offerings with an appropriate Infrastructure Ecosystem.
- **Edge Clouds:** Edge clouds are an integral part of the GAIA-X Infrastructure Ecosystem. In the context of GAIA-X, edge clouds are clouds that are not co-located with other cloud providers in data centers, e.g., on premise clouds in factories or privately-owned data centers. GAIA-X is especially interesting for edge clouds because the federated approach of GAIA-X enables a simplified setup of hybrid clouds as well as an ecosystem to analyze data and to create business models on top of data, e.g., in the Industry 4.0 context.
- **Interconnection and Network Providers:** GAIA-X has a strong focus on interoperability of data, services, and infrastructures across different cloud providers and thus data centers. Consequently, GAIA-X requires an appropriate communication infrastructure to enable hybrid cloud and multi-cloud scenarios. Communication infrastructure in GAIA-X is provided by interconnection and network providers offering interconnection services and communication infrastructure. Their offerings enable a secure, auditable communication between all other GAIA-X Providers. Moreover, they enable advanced features like closed user groups for sector specific clouds and guarantees for latency and bandwidth that cannot be provided otherwise. In the long term, interconnection and network providers can profit from GAIA-X by providing end-to-end services across multiple networks in a federated, dedicated GAIA-X communication infrastructure.

4.2 GAIA-X Data Ecosystem

Data is the raw material for innovation. For data to unfold its full potential, it must be made available in cross-company, cross-industry business ecosystems. These arising data value chains range from capturing data by means of sensors to preprocessing, storing, and transferring data to data analysis, data processing, and data usage.

In such scenarios, data sovereignty is ensured if data usage rights are guaranteed and enforced at every stage of the data value chain. This may include contractual agreements prohibiting the processing, linking, or analysis of data (or allowing it), or preventing third parties from accessing data (or granting such access). If third parties are allowed to retrieve, store and use data, data sovereignty also must be ensured within their digital infrastructures (e.g. networks, clouds, software).

The Data Provider, the Data Consumer, and should the situation arise, the Service Provider (who exposes the data) have an agreement on the conditions under which the data can be made available. An example by agreed usage control policies or minimum certification levels of the Consumers who receive access to the Service or data set. GAIA-X as a trusted infrastructure constitutes the basis for ensuring data sovereignty in the first place. GAIA-X provides a number of mutually-adjusted operational components (e.g. identity provisioning or (dynamic) trust management) and allow for unambiguous digital identities for organizations and components. If either of these two preconditions is missing, data sovereignty cannot be enforced. It is these components and identities, together with additional features (such as a metadata-broker Service Provider or functions for data quality assessment), that make an Infrastructure Ecosystem based on data sovereignty valuable for its users.

To complement the description of stakeholders in the Infrastructure Ecosystem, a description of stakeholders in the Data Ecosystem is given – consisting of parties exchanging data in data spaces while consuming

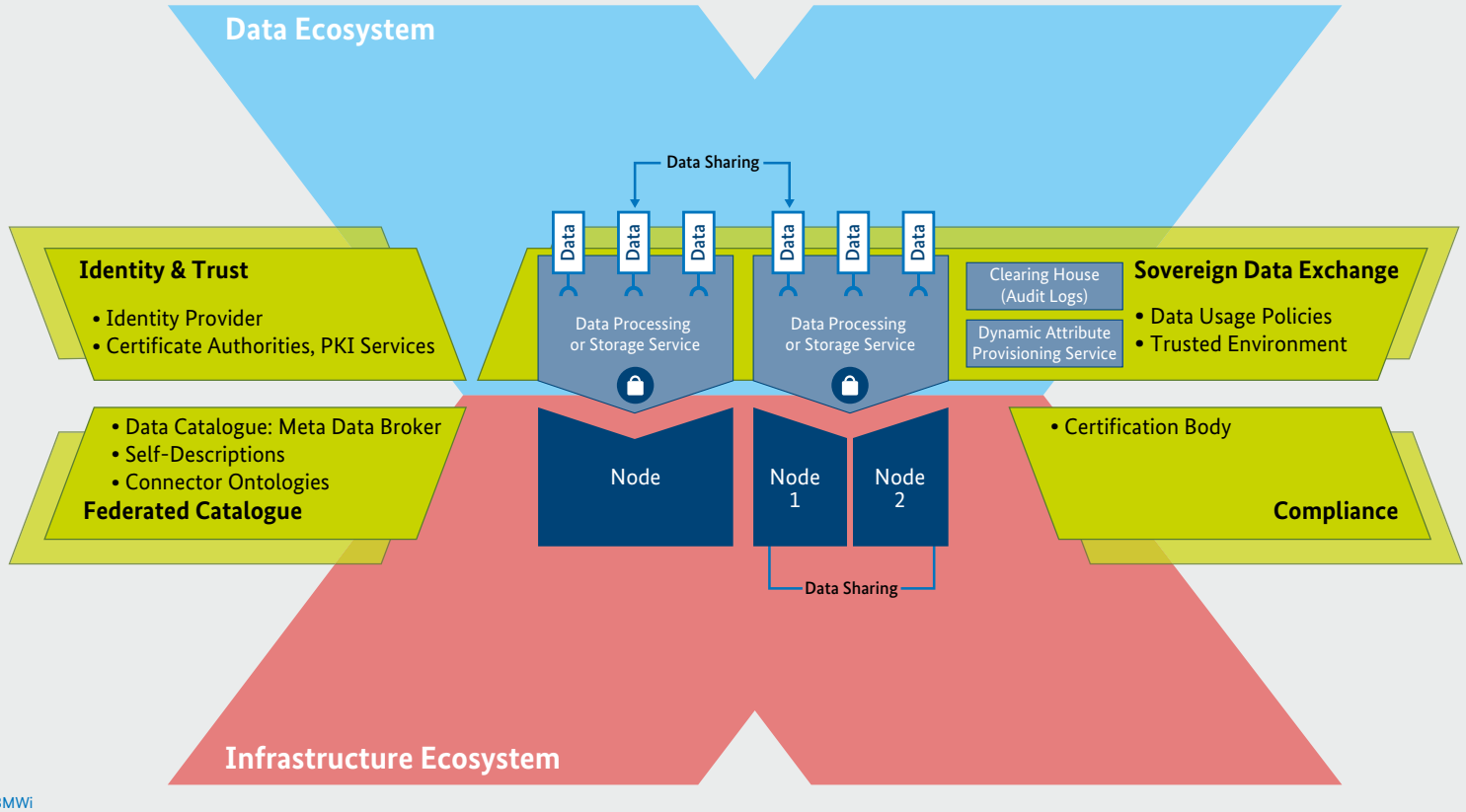
the data sovereignty services within the federation layer.

Stakeholders in data spaces:

GAIA-X leverages work that has been done in the various industry and technology associations providing integration of the different Ontologies, Semantics, and References. Through its federated Identity Access and Data Sovereignty services it enables connection across data spaces and therefore supports the creation of innovation and smart service business models.

- **Data Provider:** The Data Provider makes data available to being exchanged. To submit metadata to a Broker, or exchange data with a Data Consumer, the Data Provider uses software components that are compliant with the Reference Architecture.
- **Data Owner:** The Data Owner is the original author or legal owner of a Data Asset. He can make the Data Asset available in GAIA-X. A Data Asset has a usage license. Further, the Data Owner can attach Usage Control Policies to restrict access and use. In that sense, the Data Owner retains self-sovereign control over the data.
- **Data Consumer:** The Data Consumer receives data from a Data Provider. From a business process modeling perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore similar to the activities performed by the Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets by making an inquiry at a Broker Service Provider.

Figure 13: Data Sovereignty Services overview



- **Providers of Advanced Smart Services:** Providers of smart services provide higher order services within GAIA-X, e.g., services based on Artificial Intelligence, services for Industrial Internet of Things applications, and Analytics services. GAIA-X enables these providers to enable cross-sector innovations in different value chains and to utilize the next generation GAIA-X Infrastructure Ecosystem to enable growth in digital ecosystems.

Data Sovereignty Service Providers:

- The GAIA-X Federation Services include Sovereign Data Exchange Services which allow each Infrastructure Ecosystem Participant to exercise data usage controls when exchanging data without the need to create individual agreements and technological solutions with each party.[13]
- Sovereign Data Exchange is enabled by data connectors who comply to defined standards and make use of the following federation services:

  Sovereign Data Exchange:

  - The attributes (identity, master data, security, certifications) for all Participants in sovereign data exchange are stored in a Dynamic Attribute Provisioning Service (DAPS).
  - The Audit Logs are provided by a data Clearing House service.

The sovereign data exchange services rely on the other federation services:

- Identity & Trust: to validate the Identity of data providers and Consumers and the necessary electronic certificates[14] for the data connector endpoints of the data connectors: this information is used in the connector and referenced in the DAPS.
- The data end points are part of the Federated Catalogue services which include a Meta-Data Broker (based on Self-Descriptions) and a Connector Ontology to provide a clear attribution to the semantics and ontology of the data provided.
- Compliance: Compliance of the Connector and the technological standards and agreed polices is provided though certification bodies.

4.3 Standards for Interoperability

To assure end-to-end compliance interoperability and portability across the entire architecture stack in a horizontal and vertical form, an initial methodology to reference technical standards (e.g. for IAM, Common Data Standards...) and to collect relevant standards, policies and open APIs as key enablers for Data Sharing, Portability and Interoperability must be set.

"Architecture of Standards" will extend the concept of policies with a set of regulatory and technical standards which shall ensure that a provider is being compliant to the GAIA-X "Architecture of Standards".

Mapping the standards to the objectives and policies enables an ecosystem, which gives assurance to all Participants. Smart services built on top support the creation of compliant innovation services, fulfilling the key objectives of GAIA-X.

4.4 GAIA-X Federated Ecosystems

The high-level federation concept addresses the following challenges:

- Decentralized processing locations
- Multiple actors and stakeholders
- Multiple technology stacks
- Special policy requirements or regulated markets

13 See the IDS RAM for the definitions of the concepts Sovereign Data Exchange Services, Clearing House, Meta-Data Broker and Connector: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf

14 for example, PKI / X.509 https://www.itu.int/rec/T-REC-X.509-201910-I/en

Therefore, GAIA-X is designed for the enablement of federated eco systems, with common specifications and standards, harmonized rules and policies and a multi stakeholder governance to balance the provider and Consumer requirements with respect to the following set of guiding principles, which are aligned with similar specifications like NIST CFRA[15]:

- Security and collaboration context are not "owned" by any one user or organization
- Participating entities shall have ***membership*** in a specific federation
- Participating members can jointly agree upon the common goals and governance of the federation by acceptance of core GAIA-X governance principles
- Sites can participate in a federation by selectively making some of their resources discoverable and accessible by other federation members in compliance with GAIA-X standards and by accreditation from the Catalogue service
- Resource owners retain ultimate control over their own resources. A resource owner can unilaterally change their discovery and access policies but might lose the GAIA-X conformity level

15 https://www.nist.gov/system/files/documents/2019/07/09/nist_cfra_20190709_draft_v1.0.pdf

5 Information Security and Data Protection Viewpoint

The vision of GAIA-X is to enable an accelerated and broad use of secure and trusted data services. The data services will be hosted in an open ecosystem which allows secure and compliant sharing as well as processing of the data across different parties in a sovereign way. To ensure the highest level of data protection, security, transparency and portability for all services, GAIA-X defines guidelines, policies, and a target architecture and determines the technical Federation Services which must be implemented by GAIA-X Participants.

Information Security is one of the core principles of GAIA-X. Ensuring security is not only mandatory for the governing body of GAIA-X but also for all Participants in the GAIA-X ecosystem. GAIA-X will provide a trusted and open ecosystem for autonomous Services and Data Providers and Customers. In order to create, maintain and strengthen the trust between the Participants, GAIA-X will provide full transparency concerning the technical implementation and the security level of the GAIA-X Federation Services. Federation Services which are developed and/or operated by the governing body of GAIA-X or on its behalf will be implemented in accordance with Security by Design principles. GAIA-X will utilize state-of-the-art security tools to verify the security and compliance during the entire development, integration, operations and decommissioning phase (DevSecOps). The source code of GAIA-X Federated Services will be auditable. GAIA-X Federation Services will operate on certified cloud platforms and the governing body of GAIA-X itself will also apply for appropriate information security and data protection certificates for each Federation Service.

5.1 Shared responsibility

GAIA-X is a federated system of autonomous providers, for instance, all Services and Nodes are developed and operated by several Service Providers. In accordance to the shared responsibility model each GAIA-X Participant is responsible for the service and data which is controlled by him. GAIA-X Providers who are offering a Service or Node are responsible for the security of those. Equally, a GAIA-X Provider who is offering data is responsible for the protection of data.

GAIA-X is not releasing any Participant from his/her responsibility regarding information security and data protection but rather providing technical Federation Services to enable GAIA-X Participants to carry out their duties in an automated and user-friendly way.

The complexity of the GAIA-X shared responsibility model is a direct result of its overarching objective to implement an open ecosystem which avoids lock-in effects, provides trust and fulfills highest data privacy standards. Open standards and the mandatory use of open APIs are the basis for a wide acceptance of GAIA-X and many Participants will implement services by utilizing or consuming other GAIA-X Services from the service-mesh. Moreover, most GAIA-X Service Providers – like start-ups - will not offer any GAIA-X Nodes. Consequently, a GAIA-X Service instance will most probably consist of Services and Nodes of several GAIA-X Providers to process data of a further one.

GAIA-X will implement and secure the retrieval and integration of the Services, Nodes and Data Assets of autonomous providers in one GAIA-X ecosystem through the Federation Services. The technical and contractual implementation of the data exchange and utilization of Services and Nodes must be agreed upon between the involved parties.

5.2 Access Control

Data-driven ecosystems build on the availability, the storage, and the processing of data, or in general, the usage of data. In this regard the provider (or owner) of the data provides access to the data, but still demands control over the usage of the data to comply his responsibility. Therefore, mechanisms beyond access control are required and must be part of negotiations between the data Provider and data Consumer. After access to data has been granted by these mechanisms, data can be arbitrarily altered, copied and disseminated by the

recipient. Data usage control offers possibilities to control future data usages beyond the initial access (also known as obligations). Usage control[16] is an extension of traditional access control. It is about the specification and enforcement of restrictions regulating what must (not) happen to data. Thus, usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

In information security, access control restricts access to resources. The term authorization is the process of granting permission to resources. Several access control models exist, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC), Attribute-based Access Control (ABAC), etc. Although such a plethora of access control models exists, RBAC and ABAC are most commonly used. GAIA-X itself enables fine grained access control based on Policy Usage Control that allow attributes evaluation which is derived from metadata, Self-Description and includes runtime context attributes like user identity and associated properties. For example, a Visitor will be able to browse the whole GAIA-X Catalogue but might not be able to see every attribute of the Self-Description of a specific Asset.

GAIA-X will not implement central access mechanisms to control the access of any Consumer to a specific Asset. The responsibility stays with the Provider of this asset. However, GAIA-X will provide an API which enables the Provider and Consumer to query and verify the identity and Self-Description of the respective other party based on cryptographical signatures.

5.3 Compliance

Compliance to the GAIA-X principles must be demonstrated by all GAIA-X Participants. The GAIA-X Compliance Services will ensure that all Participants (except Visitors) and Services or Nodes comply with these internal requirement as well as external regulations and policies. These include but are not limited to information security and data protection requirements.

During the onboarding process, the GAIA-X Providers must demonstrate their compliance according to requirements. The governing body of GAIA-X will verify this Self-Description regarding completeness, integrity and honesty. This initial check will be differentiated according to different quality characteristics of Services and Nodes the GAIA-X Provider wants to offer. It may include the need to apply for a certification by a 3rd party auditor. GAIA-X will recognize existing certifications and audit reports substantiation, which meet the requirements of GAIA-X (see also 2.4).

The assurance level of the Participant will be recorded in his Self-Description. To provide transparency over subsequent changes of the Self-Description GAIA-X will cryptographically sign those parts which were essential for passing the onboarding. The signed Self-Description and the policies are visible to other GAIA-X Participants and are used to ensure a continuous assurance level across all Service, Nodes and Data Assets of a service chain (Policy Enforced Workload).

5.4 Federated Catalogue

Every Asset must be registered in GAIA-X Federated Catalogues. The basis for this registration is the Self-Description (see 2.4) which must be provided by the previously registered GAIA-X Provider. This Self-Description will be validated and cryptographically signed by GAIA-X as part of the onboarding process (see 6) of the Asset.

16 Introduction and definition of Usage Control and Usage Policy Enforcement base on the document Usage Control in IDS, published by International Data Spaces Association ,2019, https://www.internationaldataspaces.org/wp-content/uploads/2019/11/Usage-Control-in-IDS-V2.0_final.pdf

In addition, GAIA-X will aim for an automated basic security and vulnerability check based on the recommendation of the EU Cyber Security Act. The criteria of this check will reflect best practices and standards for information security and will be publicly available. This mandatory security check will ensure that all GAIA-X Services and Nodes comply with the minimum standards for IT security. The automation of these checks will guarantee a fast processing of new registration processes.

GAIA-X will distinguish between three assurance levels of Services and Nodes which are differentiated by service qualities and degrees of assurance.

The basis assurance level is mandatory for all GAIA-X Services and Nodes. Therefore, the GAIA-X Federated Catalogue will only contain Services and Nodes which have passed the basic security and vulnerability check.

Based on the recommendation of the EU Cyber Security Act, for higher assurance levels the examination extent of the onboarding process will increase. The Service Provider will have to provide in depth information on the service (e.g., internal security approval, authentication mechanisms, encryption mechanisms, applied firewalls etc.), Node (e.g., location, construction, security technology, power supply, fire protection, alarm and extinguishing systems, air conditioning and ventilation) and the relevant processes (e.g., revoking user permissions, help desk, security incident handling, training employees etc.). The mandatory security checks will be extended as well, to cover more sophisticated threat scenarios and whitebox compliance checks. GAIA-X will recognize existing certificates and audit reports as substantiation which meet the requirements of GAIA-X during the onboarding.

To ensure compliance of Services and Nodes at any point in time, GAIA-X will implement mechanisms for continuous monitoring. The first automated checks will be performed during the onboarding process. During the lifecycle of the Service or Node the checks will be repeated regularly and expended by enhanced security tests, e.g., whitebox compliance checks, penetration testing and red team testing. The enhanced security tests provide a higher level of assurance but will also cause more effort for the Service Provider and the governing body of GAIA-X.

5.5 Data Protection

Modern and state-of-the-art approaches do not regard information security and data protection as competing concepts, but recognize each other as complementary. Following certain principles described regarding information security can be transferred to data protection with small adjustments.

The data protection concept of GAIA-X is generic and can be utilized to ensure compliance to any data protection standard. For simplicity, the example of GDPR is used in the following subsections.

In order to facilitate the development of a trusted GAIA-X environment and to wellutilize existing standards, a short explanation of mechanisms under GDPR is described.

Processing parties, no matter whether they are controller or a processor, can declare themselves subject to two mechanisms to voluntarily underpin their compliance with GDPR requirements, whilst also taking advantage of legal incentives under GDPR. These mechanisms are Codes of Conduct (Art. 40, 41 GDPR) and Certifications (Art. 42, 43 GDPR)[17]. Voluntarily declaring oneself subject to any of these options will ease leveraging of risks or defend oneself against judicial or administrative actions, as compliance with such standards needs to be considered.

17 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3875-1-1

Both mechanisms provide such legal incentives as both require an independent third party to verify the processing party's compliance next to the supervisory authorities' approval. Hence, Participants of GAIA-X shall be able to refer to any of these standards if and to the extent they have declared themselves subject to them and if and to the extent they have been verified compliant.

A challenge GAIA-X must address is that GDPR allows both mechanisms to each define their scope individually. Hence, it is unlikely that there will be one overarching standard that already verifies compliance with all possible and applicable GDPR requirements. It is expected that GDPR standards relevant for GAIA-X – both Codes of Conduct and Certifications – will either address specific market sectors or specific processing activities. Upcoming standards that e.g. only address very particular requirements (e.g. specific retention periods) are likely to be irrelevant for the overall GAIA-X verification – at least for the first GAIA-X, whilst standards besides others that safeguarde appropriate procedures to determine adequate retention periods, may likely be respected in the GAIA-X onboarding.

GDPR posits requirements for operations for processing personal data. Data processing is any process or sequence of processes carried out with or without the aid of automated methods, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data. A data processing operation can include both technical and automated, as well as non-technical and thus organizational (e.g., manual, personal) procedural steps, which can encompass data protection concepts and management systems. The entire processing operation must comply with the requirements of the GDPR. Nevertheless, the complete cloud service can be regarded as a set of processing operations.

5.5.1 GDPR compliance of GAIA-X Federated Systems

Privacy by Design and Default are architecture guidelines of GAIA-X. Every Federation Service which is developed and/or operated by the governing body of GAIA-X or on its behalf will certainly follow the same principles as defined for its Participants. The technical and organizational requirements will be developed against existing and state-of-the-art standards.

The governing body of GAIA-X itself will apply for appropriate data protection standards as they become available. Several standards regarding cloud computing are currently developed, including the European Cloud Service Data Protection Certification (AUDITOR), that has been supported by the German Government.

5.5.2 GDPR compliance of GAIA-X Participants regarding Customer user data

Whilst most standards relate to the processing of Personal Data within Data Assets, the processing of Personal Data of employees of GAIA-X Participants may be of interest to GAIA-X Participants as well.

If and to which extent specific provisions are necessary in this regard will depend on the respective domains. Keywords in this regard may be: (constant) performance review of employees, use of Customer end user data for marketing / analytical purposes, etc. For the moment it expected that such requirements will not be part of the first iteration of GAIA-X, whilst at the same time this perspective can be of utmost importance in certain domains, and therefore implemented as a pilot in such domains.

GAIA-X will (at least in the first phase) not implement any technical measures to prevent a violation of GDPR by GAIA-X Participants. The compliance to GDPR and the necessary capabilities, like internal controls or processes of the Participants, will be verified during the onboarding process and continuously

monitored by GAIA-X. Nevertheless, the final decision and responsibility are with the GAIA-X Participants (see also 5.2).

5.5.3 GDPR compliance regarding Customer/ Provider relation (GDPR capability of Participant, Service, Node)

GDPR provides different relationships of Customers and Providers stipulating specific requirements. Whilst a Provider may be a „provider" pursuant to Art. 28 GDPR[18], it may also be a joint-controller pursuant to Art. 26 GDPR[19] or just a „receiver" of personal data. GDPR allows also for any combinations thereof.

All of those relationships share at least the requirement of a written agreement (electronic form may suffice). GAIA-X will stipulate transparency requirements for all scenarios and refer to existing, more detailed (sectoral) standards. Most of the latter currently focus on the most relevant relations pursuant to Art. 28 GDPR.

Processing personal data comes along with a comprehensive set of technical and operational requirements. Therefore, Service or Node Providers will have to opt-in for the processing of personal data pursuant to GDPR. The very moment a Provider opts-in it shall be legally bounding its guarantee compliance to GDPR. To the extent a Provider does not opt-in, in its Self-Description (part of the respective policy), GDPR related requirements will not apply. Vice versa, the Data Owner of a Data Asset will have to document in the Self-Description if GDPR protected data is contained in the data set.

GDPR requires appropriate measures. Appropriateness depends on several aspects like the actual type of personal data, the associated risks with each single data and the cumulation thereof, the means of processing, the expected amount of parties and individuals accessing and processing, etc. Consequently, GAIA-X requirements related to GDPR will not be able to reflect any individual case. Whilst GDPR requirements related to the security of processing may be aligned with those already defined for general IT security, others – necessity to appoint a data protection officer, adequate policies and/or capabilities regarding retention and/or deletion, etc. – are likely to be addressed by transparency obligations. By information provided, GAIA-X Participants shall be able to make an informed decision whether a Service, Node or Data Asset is meeting individual requirements. This also follows the principle of GDPR, whilst the engaging party needs to apply appropriate due diligence in selecting its processors. The final decision and responsibility are up to the GAIA-X Participants (shared responsibility model).

5.6 Terms and Conditions & Assurance Levels

For the participation in the GAIA-X ecosystem, the adherence to the principles of GAIA-X is a mandatory requirement. Those principles address, among other things, information security and data protection requirements. The declaration of adherence should consist of a "Statement of Conformity" and the "Terms and Conditions".

This statement of conformity is a declaration by the applying Provider that the content of the Self-Description is complete and accurate and that the fulfilment of the requirements set out by GAIA-X has been demonstrated, at least in internal testing. By issuing such a statement, the applying Provider shall assume responsibility for the compliance of the Service/Node to GAIA-X. The declaration of adherence should also cover the Terms and Conditions for the Provider, with the obligation to act according to the GAIA-X principles, especially the non-technical aspects and further obligations. Such Terms and Conditions will address

18 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3150-1-1

19 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3083-1-1

capabilities of the governing body of GAIA-X to verify a provider's declaration of adherence, take actions in case of non-compliance, as well as govern aspects related to the constant evaluation and updating of GAIA-X requirements, its principles and Terms and Conditions.

GAIA-X will align its principles closely to existing initiatives on the European level, therefore a methodology according to the EU Cybersecurity Act[20] with a staggered evaluation according to the risk classes of services or data (e.g. mission-critical, sensitive data) will be followed.

GAIA-X Federated Catalogue will be comprised of different levels of Services and Nodes which are differentiated by service qualities and levels of assurance. To account for these levels, different assurance levels will be introduced by GAIA-X:

- "Basic GAIA-X Assurance": Required for Services and Nodes suited for the support of non-mission-critical and/or safety-critical processes or leveraging public or non-sensitive data.
- "Substantial GAIA-X Assurance": Required for Services and Nodes suited to support potentially mission-critical or safety-critical services or leveraging non-public/sensitive data.
- "High GAIA-X Assurance": Required for Services and Nodes used to support mission-critical processes and/or to process, share and store sensitive and regulated data.

GAIA-X will define different inspection depth and information security and data protection requirements for these assurance levels. This is in line with the Concept of Categories of Protection Needs as laid out in the GDPR certifications and codes of conduct. The assurance levels will follow elementary principles (as defined in the EU Cybersecurity Act):

- The high assurance level should comply with the requirements used for the substantial and the basic level.
- The substantial assurance level should comply with the requirements used for the basic level.
- The assurance attestation mechanisms should allow for a natural progression, through enhanced requirement implementation and requirement validation (which is part of any normal auditing and testing effort) for the Service or Node to progress to the next assurance level without restarting under a fully new testing or auditing process.
- The levels of non-atomar constructs of processing (e.g., service A running on Node 1 incorporating service B running on Node 2) follow the principle of consistency of the assurance level.

These levels of assurance will not eventually surrogate appropriate risk analysis by Data Owners. It is likely that GDPR related classifications comprise more differentiators than GAIA-X, as individual needs require. However, GAIA-X will – to the extent possible – align these three levels to existing standard risk classifications.

The GAIA-X assurance level of every GAIA-X Participant, Node and Service will be determined during the onboarding process and will be continuously monitored over the whole lifecycle of the Assets. The assurance level reached will be documented in the respective Self-Description (policy). It will be transparent to other GAIA-X Participants and is one crucial parameter for the search algorithm of the Federated Catalogue and the Policy Enforced Workload.

20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

6 Onboarding & Certification

6.1 Onboarding a Provider and Consumer to GAIA-X

Before offering Services and Nodes on GAIA-X, the Provider has to register at GAIA-X. An important basis for the onboarding process is the Self-Description which is to be provided by the Provider applying for integrating Services/Nodes in the GAIA-X environment. This Self-Description should be completed by the Provider using a tool made available through the GAIA-X portal and APIs. This ensures syntactical correctness as well as the possibility to perform automated checks on the statements. While the extent of the data to be provided by the Provider will depend on the kind and number of Services/Nodes applied for, the information on the applying organization is of vital importance. Since one Provider can provide a multitude of Assets, this information should be registered as ***'master provider data'*** during the Provider onboarding process to ensure consistency and minimize the effort of updating.

The Provider Self-Description (and later in the Self-Description of Nodes and Services) will be checked for completeness, integrity and honesty. Since it is presumed that not all checks can be performed in an automated fashion, an initial check by the governing body of GAIA-X or an institution appointed by the governing body of GAIA-X has to be performed and documented. This check will be differentiated according to different quality characteristics of Services and Nodes.

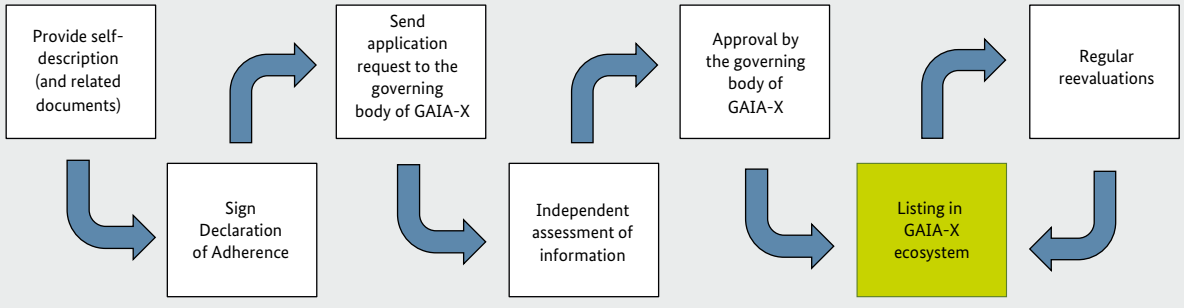
If the Provider passes these initial checks, it is required that they sign the GAIA-X terms and conditions (T&C). These will be specified later in the GAIA-X development process and require, for example, the provider to sign-up for a Service or Node shortly after the Provider onboarding is completed.

In general, the onboarding of a GAIA-X Consumer is kept very simple. The Consumer will only have to accept GAIA-X principles and service agreements during the online registration process. Adherence to further external regulations and policies might be included for simplifying the coordination between Service Provider and Consumers. To this purpose, the Consumer will have to provide a Self-Description, which will be checked for completeness, integrity and honesty.

6.2 Onboarding Services and Nodes to GAIA-X

In case the Provider onboarding was successful, the Provider can offer services or Nodes in GAIA-X. This then leads to a Service or Node onboarding described in the following. First of all, the Provider has to gather organizational, legal and technical information about the Service/Node and fill out a respective Self-Description for (each) Asset. The GAIA-X assurance levels are described in Chapter 5.6.

Figure 14: Conformity assessment for the basic assurance level.



6.2.1 Assuring Basic Level

Before participating in the GAIA-X ecosystem, a Service or Node must at least apply for the *'Basic Assurance Level'*. Figure 6 summarizes the conformity assessment steps for the basic level.

Upon applying for the *'Basic Assurance Level'*, the applying Provider has to provide to the reviewer the Self-Description in the defined format about Node(s) or Service(s) provided and all items of the pre-defined set of attributes. Other documentation provided by the applicant can include, among other things: copies of standard service agreements, documentation on IT security management, existing and valid certificates or any other documents of adherence to existing standards applicable to the system(s) application to the GAIA-X ecosystem that has been requested, and its subcontractors.

The applicant has to sign a contract which specifies his obligations (fees, notification of changes to the Node/Service etc.). Information provided by the applying Provider is legally binding and should be signed by management.

The application request is submitted to the governing body of GAIA-X or a monitoring body appointed by the governing body of GAIA-X. If several monitoring bodies are appointed, it has to be assured that all bodies are acting according to a procedures manual describing the steps of the evaluation process and the minimum criteria for acceptance.

The application request is examined by a qualified independent assurance reviewer based on a guideline manual describing the examination process. Based on this check (which can include several iteration phases), the reviewer prepares a report that is the basis for awarding the GAIA-X compliance.

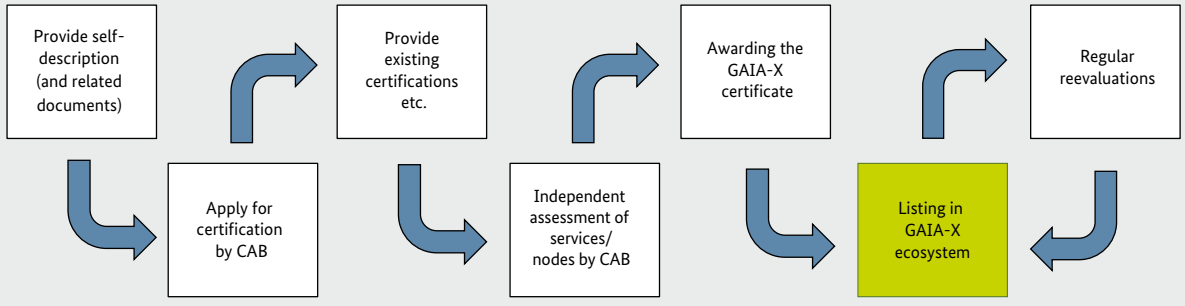
The report is to be finally approved by the governing body of GAIA-X before the issue of a ***basic declaration of assurance*** and the listing of the Node/Service in the GAIA-X Catalogue can be undertaken.

At a given interval, a re-evaluation has to be performed; if the criteria of the scheme do not continue to be met, the listing in the GAIA-X Catalogue can be suspended. Ideally this process can be performed, at least in part, automatically. Upon receiving an updated Self-Description, a check can be performed to see if the changes are relevant to the application criteria and if minimum requirements are violated.

6.2.2 Assuring Substantial and High Level

To apply for the substantial and/or high level, a third-party based certification is a required. Figure 7 summarizes the process.

Figure 15: Conformity assessment for the substantial assurance level



To ensure a higher level of assurance, the onboarding process has to be supported by existing documents proving that assessment has followed auditing standards, to show that they

1. guarantee a sufficient level of formality and rigor,
2. are based on a thorough assessment and standard and repeatable processes,
3. offer accurate reporting standard,
4. there exist clear and well-defined auditor competences requirements.

The auditing has to be performed by an accredited conformity assessment body (CAB) according to the GAIA-X conformity assessment program. To the extent applicable, this process can refer to existing certifications and attestations. The certificate will be issued for a duration specified in the conformity assessment program. This program will also specify frequency and extent of re-checks during this period.

The applying organization will present the certificate to the governing body of GAIA-X or an appointed monitoring body. After successfully completing an extended security and vulnerability test (the scope depends on the kind of Service and/or Node), the listing of the Node/Service in the GAIA-X Catalogue can be undertaken.

6.2.3 Modularity and Recognition of Existing Certification, Standards and related Schemes

In general, GAIA-X will avoid duplicating audits to reduce efforts. Where an applying Provider has obtained evidence derived from its adherence to an existing scheme (such as a certificate, attestation, standard or audit report), this evidence may be presented by to the CAB in order to issue the certification of its certification object against the GAIA-X scheme. To this end GAIA-X will define and perpetually update the relevant set of certification/auditing schemes recognized to fulfil its requirements. However, the CAB has to retain freedom of appreciation in relation to this evidence.

7 Outlook and Next Steps

This chapter summarizes the progress of the initiative from a synoptic viewpoint and gives an outlook on its future actions. Since this paper serves a synoptic purpose, work results are already being applied to viewpoints. The outlook reflects these viewpoints as structured advancements, as well as topics of the project is overarching advancements.

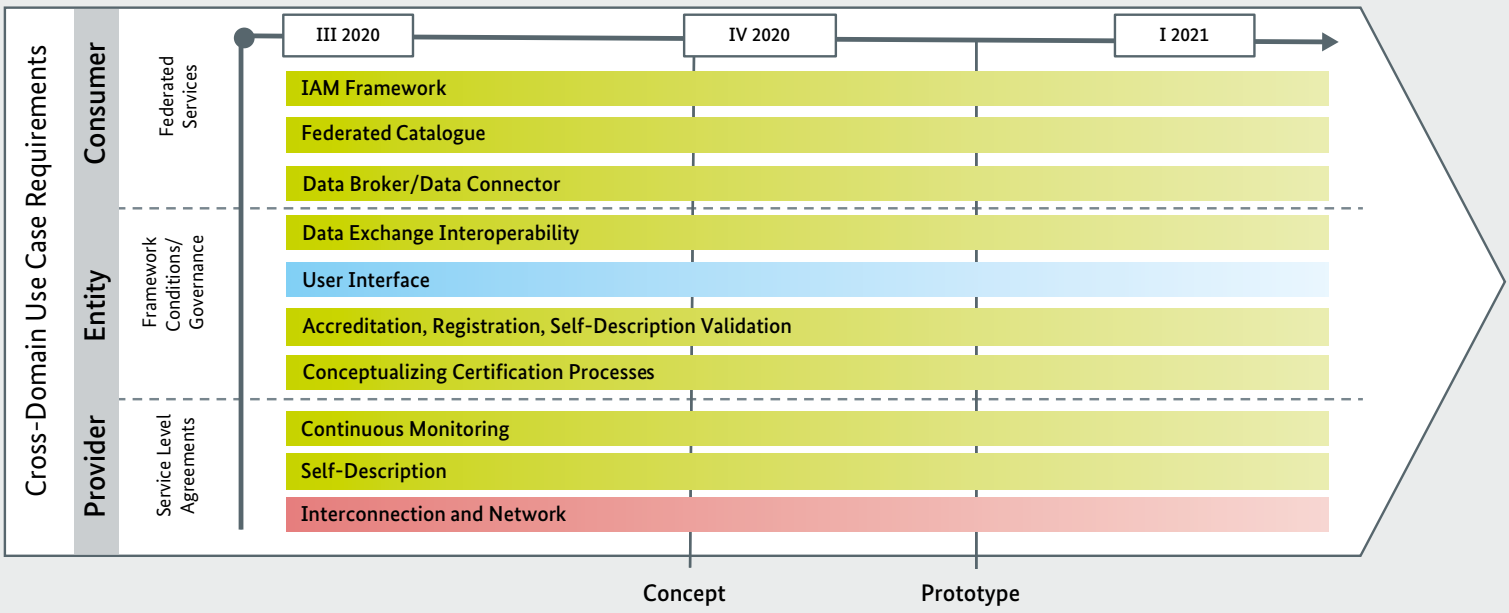
GAIA-X has the potential to serve as the European source of trust for establishing not only EU-wide but globally operating digital economies of the future. No longer will businesses be required to assimilate unknown or possibly incompatible foreign standards and values but will be able to collaborate through a mediated data exchange channel across borders.

GAIA-X does not define itself by becoming a competitor to already matured technology providers. It distinguishes itself by becoming the facilitator of the present and future digital efforts of European businesses. GAIA-X will enable highly inter-connected, modern, and consensual digital workloads built upon a multitude of technologies and approaches.

GAIA-X will facilitate the development of its competences and expertise and foster research & development (R&D) where needed. In order to ensure stable practices, align processes with technological objectives and encourage continuous improvement of business processes, GAIA-X is furthering its conceptualization approach by optimizing its future work mode in alignment with its core principles and overall vision by:

- Advancing of comprehensibility
- Expediting evaluation of prototypes during conceptualization
- Garnering testbeds from participating target industry sectors
- Defining standards of judgment for technology evaluation
- Institutionalizing the steering of architectural planning and implementation

Figure 16: Roadmap



- Structuring Efforts in alignment with the GAIA-X Executive Paper, European Commission Strategy Paper, as well as the Franco-German position paper[21]

It is an effort of the project to make the conceptualization as transparent and seamless as possible.

7.1.1 Overarching Advancements

Advancing of comprehensibility: The efforts to achieve common denominators for productivity approaches and results of contributors should be further intensified. Therefore, standardization of documentation and reporting is improved. With an unornamented standard to adhere to, collaborators will be able to focus on work results. With unified documentation, GAIA-X can easily adhere to its principles of transparency and auditability.

Expediting evaluation of prototypes during conceptualization: Besides conceptualizating of technical implementations further GAIA-X will also deliver practical results on time. Therefore, it aims to accelerate the turnover of research and engineering for faster judgment on applicability and practicability of implementations. The project will move away from the theoretical determination of the suitability of system design towards a practical -fail-fast- approach. A contemporary GAIA-X architecture is only achieved if the conceptualization happens promptly, and non-essential decisions disregarded until a later point in time.

Garnering testbeds from participating target industry sectors: The inclusion of participants from systemic (but not exclusive) industry sectors should not only bring theoretical demands and needs in the form of use-cases in to play. Rather participants should be willing to offer practical and realistic assessment of their requirements. Thus they should reflect the actual technical specifications of the scenarios and be useful for engineering infrastructure components.

Prototypes are fundamental for demonstrating valuable features based on the practical feasibility of an infrastructure component. From a technical viewpoint this practicability is considered to be of great importance. The selection of prototypes should target a broad enough market to receive adequate relevance.

Defining standards of judgment for technology evaluation: When considering the judgment of usefulness and applicability of technologies, two viewpoints are of importance. From a future Consumer or Service Provider standpoint, this may be evident. Businesses require objective assurances about how to manage their data. A Consumer may require actual proof, that the exact location of his data storage corresponds with the provider-advertised site of data storage. Rules and regulations may encourage a provider to adhere to GAIA-X's guidelines of transparency. However, actual proof is only achievable through technical means, which are yet to be determined. This type of judgment is extrinsic but makes up an essential part of the initial evaluation of a transparent and bipartisan selection of applicable technologies.

On the other hand, the assessment of technologies is a moving target and requires foresight. It is intrinsic and determines how Participants of the GAIA-X project's conceptualization can transparently find common ground for determining what technologies are applicable.

Essential technologies, which have undergone the previously-mentioned intrinsic evaluation, may have been determined as suitable by the GAIA-X project. However, the internal consensus among the stakeholders does not necessarily offer the transparency for other Participants of the project to determine adaptability for other components, as well as lay out a comprehensible roadmap for future implementations. Therefore it is a necessity to develop an objective specification framework, enabling all Participants to deliver evaluation results in a coherent manner.

21 Franco-German Position on GAIA-X
https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10

Technological freedom of choice for Consumers requires a careful analysis of a technology's underlying principles, abstracts, as well as interfaces. Especially proprietary technology, in most cases, does not offer the ability to do such an in-depth analysis. It must be GAIA-X's duty to define guidelines for determining appropriate, vendor-neutral, integrations of existing technologies without compromising the integrity of GAIA-X's core principles of sovereignty and freedom. Additionally, existing technology stacks must be seamlessly integrable into the GAIA-X ecosystem, without the modification of core application attributes. This duty is especially important when it comes to modern technology stacks like container-based virtualization. Organizations such as the Open Source Business Alliance (OSB) offer technology rating schemes in a vendor-neutral fashion.

Institutionalizing the steering of architectural planning and implementation: Even though the GAIA-X project is at a very early point in time of its development, it is conceivable that a single, loosely-organized initiative will not be suitable for dealing with the workload required to build a sustainable organization and ecosystem defined by its principles. It is a requirement to negotiate between the For-Profit market access interests and the Non-Profit interests. Following the guidelines of the GAIA-X project, an orientation towards existing, well-working approaches for similarly complex public interests is highly beneficial and will ensure steady progress over unproven assumptions. The organizational structure of GAIA-X has yet to be determined. In order to advance the above outlined architecture, committees for technical and architectural steering are established and tasked with creating and progressing the technical foundation for GAIA-X.

7.1.2 Structured Advancements

Core Architecture Elements: Efforts regarding **Self-Description** have advanced, and results include a comprehensive concept for a technical systems descriptor. Other work packages have a high dependency on the technical service descriptors and need to take these definitions into account. Upcoming advancements include the discovery of revenue aspects (including the recognition of technical monetization factors). The data exchange interoperability concept based on the GAIA-X Architecture of Standards will further facilitate the harmonizing of existing interoperability schemes by collaboration with existing initiatives. Fundamental to a future widespread interoperability, interoperability machines come into focus. These infrastructure components will be able to share data across multiple formats and meta models.

To date, the project has drafted a concept to define and structure Self-Descriptions. As Self-Descriptions are a very important part of GAIA-X, the plan is to continue working on this topic in the near future and include the participating stakeholders of the project. Therefore a dedicated Work Package on Self-Descriptions was established. Besides the activity on Self-Descriptions, another focus will be the elaboration of Interconnection and Networking principles over the next few months. It is that a central networking and interconnection concept be contributed to the project in alignment with the architecture, operations, and business viewpoints.

Monitoring aspects of GAIA-X infrastructure and provider components have been defined as an abstract, with practical applications in mind. Continuing efforts include best-practice definitions for handling complex monitoring scenarios as the basis for a top-down approach to discover required monitoring and metering facilities. In addition to scenario definitions, an explicit listing of generic entities/elements to be monitored will be made available. Monitoring related research efforts will mainly focus on abstracts and not on the technical definition of the implementation of a new monitoring solution.

The project will define facilities and requirements for establishing **Continuous Monitoring** for all GAIA-X infrastructure components, referencing candidates (elements/entities) of Self-Description. In the context of GAIA-X, there are additional objectives to be addressed by Continuous Monitoring. The design of GAIA-X aims to establish of federated digital ecosys-

tems with decentralized provider structures and distributed service and data management. For the resilience of services crossing over multiple providers and a basic assurance of Service Level Agreements, continuous monitoring should target the core requirements of transparency, service functionality and control of data.

The following key activities will be addressed:

- The specification of automatic monitoring targets (AMT) with appropriate target and threshold parameters with respect to the GAIA-X Self-Description
- Matchmaking of such AMTs into high level compliance requirements according to main GAIA-X technical objectives
- Operational frameworks for continuous monitoring-based certification
- General requirements to fulfill GAIA-X onboarding at various assurance levels

Organization and Governance: GAIA-X IAM (Identity and Access Management) focusses on ensuring the interoperability of identification, authentication and authorization, based on conceptual design and architecture by adopting accepted architectures, protocols, open standards, and frameworks.

A proper lifecycle management is required and must cover identity onboarding, i.e. registration and binding of initial credentials (establishing of identity accounts for individuals, entities and IOT devices). The onboarding process is based on credentials (entity, Node, Service), a trust infrastructure and authentication, including the verification of assurances given by GAIA-X Certification and Monitoring, and any eventual offboarding or suspension activities.

In the business alignment area, it will be necessary to support ongoing due diligence, referring to activities of actors and Consumers regarding identity and access control. Also, in this area the topic of policy management (and policy enforcement) will play a key role. A challenge to be solved in this area is a policy matching between domain specific requirements for customers to be able to choose a geography/legislation for data storage and processing offers. A definition of an identity flow is present and serves as the basis for further definitions of IAM related research and development efforts. Following the concepts of the Federated Catalog, the current iteration of this identity flow is defined as the *GAIA-X Federated Identity Model*. Work results, in conjunction with the GAIA-X Federated Identity Model, will include a detailed **GAIA-X IAM framework definition** aligned with existing industry standards and regulations, referred to as the GAIA-X Architecture of Standards. As a cornerstone for the principles of transparency and dependability, all IAM framework related efforts will require alignment with the **„Self-Description“** efforts of infrastructure components (Service Nodes, and others).

Deprioritized stretch-goals include technical evaluations of existing IAM technology stacks to be used, as well as a technical furtherment of access and authorization specifications based on the already-defined „shared responsibility model“ abstract, as well as work results of the *Franco-German Position on GAIA-X*. The specifications include **IAM policies and rules** outlining levels of assurance, and confidence.

Ecosystem: A well-defined Infrastructure Ecosystem enables the intended European single market for data. Therefore, infrastructure requirements have been defined early on, so that assumptions made around data interconnection and sovereignty are well-aligned with the factual architecture of the GAIA-X infrastructure. Measurements include:

- Adhere to established interconnection mechanisms used by (future) Participants throughout the European Union and abroad
- Establish well-defined regulatory principles for the ecosystem in harmony with European regulations
- Transparent handling of data with individual data-sovereignty as a top priority in mind

The aim is to create a single European data space, where personal as well as non-personal data, including sensitive business data, are secure and businesses have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value. This will be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market.

All efforts are well-aligned with the distinctive definition of Infrastructure and Data Ecosystem. The architectural high-level perspective serves as a catalyst for productive discussion and as an intermediary for future thorough implementations.

Information Security and Data Protection: The scope of the initial and extended security checks for Services and Nodes will be detailed based on security best practices and the recommendation of the EU Cyber Security Act. Afterward, the feasibility and integration of those checks as part of the onboarding process need to be examined.

The GAIA-X Federation Services are the core building blocks of the GAIA-X ecosystem. Collaboration, trust, identity, etc. are implemented by those services. Therefore, security and data protection requirements and standards must be considered, documented and approved for the concepts and implementations of the Federation Services.

Finally, security and data protection processes must be developed to ensure Security & Data Protection by Design principles which will be implemented for future developments. This will also support a subsequent certification of the governing body of GAIA-X[22] itself.

Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules.

Onboarding and Certification: The outsourcing of business processes and data to external Service Providers leads to heightened customer demand in terms of quality, data protection and data security supplied by the Service Provider. **Certificates** are a proven means – not only within the IT sector – to provide the customer with fast, simple, transparent and comparable information about protective measures, maintained standards and internal quality. A certificate is the result of extensive testing, which takes place in an intensive collaboration between the Service Provider and Certification Entity. High dynamics and fast technological progress within the digital service industry and the underlying technologies create a challenge in keeping compliance statements. With a high priority on establishing a trust-based service environment, certification and onboarding processes have already been defined in a detailed abstract fashion by their work groups. The **conceptualization of the certification process** has progressed to a state where a basic draft is available, detailing the groundwork, as well as the definition of a basic level of assurance. Continuing efforts include a furtherment of the assurance levels, as well as the discovery of a suitable governance model.

The same applies to **Onboarding, Registration and Self-Description Validation**. A generic description has been finalized. Furtherments of deprioritized efforts regarding processes (e.g. offboarding) are planned and will build upon the existing results of the Self-Description efforts.

The onboarding and certification process of Participants, Services and Nodes is crucial for the overall security of the GAIA-X ecosystem and the trust between all Participants. Most subsequent security controls are relying on the trustworthiness of the Self-Description provided by the Participants. Thus, the mandatory set of security and data protection requirements must be defined and mapped to the different GAIA-X assurance levels. The standing target is still to make use of existing standards and certifica-

22 For example, ISO 27001 – Information security management

tions, i.e., a mapping of those to the GAIA-X requirements will be developed as well.

Productizing and Service Exposure: GAIA-X will offer a multitude of interfaces to interact with components of the ecosystem. Even though APIs are considered „first-class citizens“ in the ecosystem context, a visual, human-friendly user interface is of high priority as well. The **user interface** will serve as a communication tool to introduce new users to GAIA-X as well as serve as an intermediary interaction mechanism for handling operational duties like monitoring, billing and others. A detailed description of required UI components and content is therefore needed and will, per the requirements, be consolidated into a set of concepts that will serve as the basis for mockups, demonstrators and prototypes. Coherent mapping of GAIA-X bids is of utter importance, since the user interface will also serve as a means of transport for the overall idea of the GAIA-X ecosystem (e.g. customer journey, use-cases, and others).

7.1.3 Conclusion

Aligned with the European Data Strategy from February 2020, GAIA-X contributes to this vision and unifies the determined efforts of single European countries into a collaborative ecosystem contributing to the creation of a genuine single data exchange market based upon European regulations and principles. These principles are already layed out and trusted by businesses as well as citizens. GAIA-X will adhere to the existing principles and will enable new business models within its community for data sharing. In this respect it will enable services to provide equal and non-discriminatory access to such an ecosystem. GAIA-X Participants will by default be enabled to enrich their regular data processings based on Advanced Smart Services like Artifical Intellingence, Analytics, Cloud and Edge computing, as well as sector-defining mechanisms, standards and technologies.

Based on common policy rules and an Architecture of Standards, Consumers and Providers will recognize GAIA-X as the initiative, to pave the way for a resilient, reliable and flexible digital infrastructure based on European values.

Appendix A: Definitions

Service
A GAIA-X Service is a cloud offer. The term encompasses all of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Function as a Service (FaaS), and so on.

Advanced Smart Services
Advanced Smart Services comprises Artificial Intelligence (AI), Internet of Things (IoT) or Big Data market places and applications within and across sectors.

Node
A GAIA-X Node is a compute and storage resource. Nodes are generic in the sense that different Services can be deployed on them. Nodes have a known certification level and a geographic location.

Service Instance
A GAIA-X Service Instance is the realization of a Service on (potentially multiple) Nodes.

Data Assets
A GAIA-X Data Asset is a data set that is made available to Consumers via a Service that reveals the Data Asset. Consumers and Providers can also host private data within GAIA-X that is not made available (and hence not a consumable Data Asset).

Participants
A GAIA-X Participant is a natural or legal person that can take on one or many of the following roles: Provider, Consumer, Data Owner, and Visitor.

The following Participants types are defined and used in the GAIA-X context.

Provider
Organization or entity responsible for making a Service/Node available to the GAIA-X ecosystem.

Consumer
Organization with users & devices, ordering Services and which maintains a business relationship to Providers. They can consume service instances, but can also provide them to End-Users.

Visitor
Anonymous, non-registered individual browsing the GAIA-X Catalogue.

Identity Provider
The Identity Provider (IdP) manages the primary identity authentication credentials of (some of the) GAIA-X Participants and issues assertions derived from those credentials. The IdP is the source of the identity credentials. The IdP guarantees an identity based on identity attributes.

Appendix B: Non-exhaustive list of Attribute Classes

Following are from a GAIA-X perspective some relevant attribute classes for Node Self-Descriptions. They have (recently) a non normative character.

(I) GAIA-X Node Attributes of Class: Connectivity

Connectivity attributes of Nodes are specified in two categories. First, there is a description of networking related IT hardware (e.g., Network Interface Controller properties), which is covered in section Appendix B (II). Second, there is the description of connectivity attributes in this section covering the Wide Area Networking (WAN) capabilities of a Node. In this context a Node may also be understood as a larger structure, e.g., multiple servers of a cloud Service Provider that are co-located in a data center or even whole cloud regions.

Consequently, the set of connectivity attributes described in this section aims at covering the majority of upstream or peering relations of cloud providers with Internet Service Providers (ISPs) and amongst each other. Currently, the following type of links are covered:

- **Business ISP links:** small cloud providers or Consumers do not run their own Autonomous Systems (ASes) to provide connectivity for their services. Usually, these Participants in the GAIA-X system have a business relation to an ISP handling interconnection for them. In this case the Self-Description aims at describing the uplink of the Node to the ISP and the properties of the ISP, e.g., the ISP's provided SLAs and the ISP's name, AS numbers, etc. The information may partially be extracted from public data sources.
- **Transit ISP links:** if cloud providers operate their own AS, they are usually connected to one or more transit provider. In this case they have their own BGP session with the transit ISP and are thus visible in the global BGP routing tables. In this case the properties of the cloud Service Provider's AS are described as its uplink to the transit provider including the AS properties and name of the transit provider as well as any SLAs. This information is helpful to assess how well the cloud Service Provider can be reached from other cloud providers.
- **Peering point links:** in order to optimize latency in certain regions and cost, cloud providers are usually present at one or more peering points. In this case, the same criteria as for transit providers apply, i.e., the uplink and the peering point are described with all relevant properties. Additionally, the peering policy is described. The peering policy describes how other ASes peering at the peering point may peer with the cloud Service Provider. As peering policies can range from "open" (everyone can peer with the cloud Service Provider) to "selective" (only selected networks may peer with the cloud Service Provider) they are an important factor to describe connectivity at peering points.
- **Private network interconnects:** commonly, cloud Service Providers establish private network interconnects with their most relevant partners. In this case, information on the remote end of the private network interconnect is described (e.g., remote AS) as well as the link's properties.

Some of the information listed above is sensitive and may be considered to be a business secret by cloud providers (e.g., private network interconnects) while other information is public information anyway (e.g., peerings). The complete set of information is helpful to enable high quality matching of customers and cloud Service Providers with respect to networking requirements. Thus, the attributes described in this section may be partially hidden from the public (i.e., only communicated to GAIA-X) or may be non-mandatory (i.e., not present at all), which is currently under discussion. A further discussion of how GAIA-X intends to utilize the provided information can be found in section 2.7.

(II) GAIA-X Node Attribute Classes: IT Hardware

Why Hardware Attributes

GAIA-X customers might be interested in ordering "Baremetal as a Service", because they need special hardware for their workloads or would just like to know more about the hardware the services they requested run on. In addition, customers interested in other services may have technology, scalability, or security requirements that would be a reflected only in the Node's infrastructure setup. For these cases, the GAIA-X Node Self-Description has a section "IT Hardware, CPU, Network Adapter, Hardware Security". All these attributes are fully optional, however the Node Providers are free to disclose these attributes to give customers a better choice where to run their services.

These Hardware attributes are assigned to a certain "pool" of hardware type and are divided into the following categories:

Compute Pools

This is about attributes describing the amount and specification of the server hardware. These include the number of servers in the pool, number of CPUs, cores, amount of memory, CPU type, server vendor. For certain workloads, customers might also have special security requirements, such as Encrypted Memory, Authenticated Memory, Server Root of Trust, Trusted Execution Environment. For other workloads customers might need Accelerator Cards. Here Accelerator Type, Number and Memory can be specified.

Storage Pools

Attributes of the "Storage Pool" are related to the Storage Type and Generation, to the capacity of the pool, Raw, Net and Exclusive Capacity, provided Redundancy, Total IOPS and Latency.

Security attributes, such as provided Encryption capabilities might also be interesting for customers.

Connection Pools

Attributes of the "Connection pool" describ the NICs in the pool – OEM, Type, Bandwidth, and also detailed connectivity attributes, such as Layer2 Technology, Traffic Class, Link Bandwidth, Link Latency, RDMA, Flow Control and Multiplex. For offloading the network processing from the server CPUs, customers would like to use Smart NICs. Node Providers are free to disclose if they are using Smart NICs and to specify the attributes of these Smart NICs – IPSec, TLS, PKI, Compression.

Hardware Security

Customers might also have special security requirements, such as the use of a TPM. The TPM (Trusted Platform Module) is a microcontroller chip that can securely store artifacts used to authenticate the server platform. These artifacts can include passwords, certificates and encryption keys. Node Providers are free to specify if their servers are using TPMs and specify the corresponding attributes – TPM Identity, Key Management, TPM Attestation.

Another security device is an HSM. A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. Common attributes of a HSM are Cryptographic Acceleration and Key Management.

Hardware Management

For "Baremetal as a Service" customers might be interested to have direct access to the server hardware management processor and would like to know what type of hardware management is supported – agent vs. agentless, and what type of management standards and protocols are supported.

(III) GAIA-X Node Attributes of Class: Sustainability

There are three sub-categories of sustainability-related Node Attributes:

- Binary criteria regarding the existence of certain sustainability-related technologies or policies at a certain data center such as waste heat utilization, free cooling, adiabatic cooling, direct hot water cooling, immersion cooling, use of renewable energy (which can be further divided into more fine-grained categories) or monitoring capabilities to provide information on CO_2 footprints on a job level
- Key Performance Indicators (KPIs) based on norms [23]
- Certificates and labels as third-party assessments of the sustainability of a Node [24]

23 for example, DIN EN 50600-4 or ISO/IEC 30134-1:2016) or research projects and papers (e.g., KPI4DCE 2.0) such as PUE (Power Usage Effectiveness), pPUE (partial Power Usage Effectiveness), dPUE (designed Power Usage Effectiveness), iPUE (interim Power Usage Effectiveness), REF (Renewable Energy Factor), ERE (Energy Reuse Effectiveness), WUE (Water Usage Effectiveness) or CUE (Carbon Usage Effectiveness).

24 for example Blue Angel for data centers (by the German Federal Ministry of the Environment), Code of Conduct for Energy Efficiency in Data Centres (by the EU), Datacenter Efficiency Label (by the Swiss Datacenter Efficiency Association), Energy Efficient Data Center (by the TÜV), Energy Star (by EU and EPA) or EPAT (by the Green Electronics Council).

Contributers

- Joachim Astel (noris network AG)
- Christian Berendt (Betacloud Solutions GmbH)
- MBA Hans Berndl (A1 Digital International GmbH)
- Fabian Biegel (SAP SE)
- Dr. Hilmar Binzenhöfer (Capgemini Deutschland GmbH)
- Andreas Bongers (GFT Technologies SE)
- Arnaud Braud (Orange S.A.)
- Uwe Brettner (IT² Consulting Solutions Services GmbH)
- Carsten Brockmann (BPS Software GmbH & Co. KG)
- Matthias Brucke (embeteco GmbH & Co. KG)
- Dr. Ingolf Buttig (Hewlett Packard Enterprise)
- Bundesdruckerei GmbH
- B1 Systems GmbH
- Diego Calvo de Nó (PROVENTA AG)
- Rajesh Chidambaram (Lufthansa Industry Solutions AS GmbH)
- DATEV eG
- Dr. Clemens Doubrava (Bundesamt für Sicherheit in der Informationstechnik)
- Günter Eggers (NTT Global Data Centers EMEA GmbH)
- Peter Eisermann (Contano GmbH)
- Tobias Erath (Hardware-Bath)
- Johannes Ernst (German Edge Cloud GmbH & Co. KG)
- EuroCloud Deutschland_eco e.V.
- Holger Fecht (OneFiber Interconnect Germany GmbH)
- Thomas Feld (STRATEGION GmbH)
- Marius Feldmann (Cloud&Heat Technologies GmbH)
- Harald Felling (]init[AG für digitale Kommunikation)
- Asst. Prof. Dr.-Ing Farshad Firouzi (Advaneo GmbH)
- Stephan Fleck (Cisco Systems GmbH)
- Bernd Fondermann (German Edge Cloud GmbH & Co KG)
- Gaël Fromentoux (Orange S.A.)
- Peter Ganten (Open Source Business Alliance e.V.)
- Kurt Garloff (Sovereign Cloud Stack)
- Joshua Gelhaar (Fraunhofer ISST)
- Michael Gollan (HYPERTEGRITY AG)
- André Gomola (Lufthansa Industry Solutions AS GmbH)
- Andreas Götz (Core-Backbone GmbH)
- GONICUS GmbH
- Google Germany GmbH
- Samir Grimm (Deloitte Consulting GmbH)
- Pierre Gronlier (OVHcloud SAS)
- Holger Grziwotz (GDV Dienstleistungs-GmbH)
- Hannes Hahkio (Nixu Corporation)
- Aaron Hänisch (Fujitsu TDS GmbH)

- Henrik Hasenkamp (gridscale GmbH)
- Timo Hauswirth (LINBIT HA-Solutions GmbH)
- Joonatan Henriksson (Nixu Corporation)
- Martin Högl (comjoo business solutions GmbH)
- Thomas Hornig (highQ Computerlösungen GmbH)
- Dr. Detlef Hühnlein (ecsec GmbH/go.eIDAS e.V.)
- Stephan Ilaender (PlusServer GmbH)
- Frank Ingenrieth LL. M. (Selbstregulierung Informationswirtschaft e.V.)
- Moritz Kaminski (Robert Bosch AG)
- Frank Karlitschek (Nextcloud GmbH)
- Tobias Kaufmann (Bundesministerium für Wirtschaft und Energie)
- Dr. Nils Kaufmann (cloudbuddies GmbH)
- Thomas Keller (1&1 IONOS SE)
- Dr. Markus Ketterl (msg systems ag)
- Lukas Klingholz (Bitkom e.V.)
- Andreas Klöber (GFT Technologies SE)
- Harry Knopf (dcOrbis Ltd. & Co. KG)
- Christian Koch (4Com GmbH & Co. KG)
- Robin Köpsel (axilaris GmbH)
- Pawel Kowalik (1&1 IONOS SE)
- Johannes Krafczyk (T-Systems International GmbH)
- Wolfgang Ksoll (Cloudical Deutschland GmbH)
- Mark Kuehner
- Tobias Kurz (ODN OnlineDienst Nordbayern GmbH & Co. KG)
- Prof. Dr. Dirk Kutscher (Hochschule Emden/Leer)
- Jörg Langkau (nicos AG)
- Florian Lauf (Fraunhofer ISST)
- Dr. Markus Leberecht (Intel Deutschland GmbH)
- Andreas Linneweber (UNITY AG)
- Sebastian Lins (Karlsruher Institut für Technologie (KIT))
- Dr. Ignacio Martin Llorente (OpenNebula Systems SL)
- Dirk Loßack (Sovereign Cloud Stack)
- Oliver Loukota (QSC AG)
- Dr. Jesus Luna Garcia (Robert Bosch GmbH)
- Maximilian Lund (Maximilian Lund GmbH)
- Tobias Mader (ExaMesh GmbH)
- Christoph Maggioni (secunet Security Networks AG)
- Berthold Maier (T-Systems International GmbH)
- Alexander Maintok (ODN OnlineDienst Nordbayern GmbH & Co. KG)
- Gebhard Marent (Capgemini Deutschland GmbH)
- Marius Marocico (Fujitsu TDS GmbH)
- Christoph Marsch (SAG Deutschland GmbH)
- Dr. Alberto P. Martí (OpenNebula Systems SL)
- Dr.-Ing. Kai Martius (secunet Security Networks AG)
- Matthias Marx (Bundesministerium für Wirtschaft und Energie)

- Nadja Menz (Fraunhofer FOKUS)
- Sven Miesikowski (Fujitsu Technology Solutions GmbH)
- Matthias Möller (BOTLabs GmbH)
- Dipl.-Ing. Lars Nagel (International Data Spaces e.V.)
- Dr. Andreas Nauerz (Robert Bosch GmbH)
- Thomas Niessen (Kompetenznetzwerk Trusted Cloud e.V.)
- Open-Xchange AG
- ORACLE Deutschland B.V. & Co. KG
- Klaus Ottradovetz (Atos SE)
- Valeri Parshin (Fujitsu TDS GmbH)
- Heinrich Pettenpohl (Fraunhofer ISST)
- Dr.-Ing. Julius Pfrommer (Fraunhofer IOSB)
- Christoph Plass (UNITY AG)
- Jens Plogsties (SysEleven GmbH)
- Xavier Poisson Gouyou Beauchamps (Hewlett-Packard Entreprise France)
- Dr. Carsten Polenz (SAP SE)
- Peter Reiner (Fujitsu Technology Solutions GmbH)
- Dr. Ronny Reinhardt (Cloud&Heat Technologies GmbH)
- Jonas Riedel (4Com GmbH & Co. KG)
- Thomas Rinck (noris network AG)
- Thies Rixen (QSC AG)
- Hannes Rollin (T-Systems International GmbH)
- Artur Romão (Decsis – Sistemas de Informação S.A.)
- Leslie Romeo (1&1 Mail&Media SE)
- Ingo Rübe (BOTLabs GmbH)
- Dr. Aly Sabri (olmogo GmbH)
- Dipl.-Ing. Marcos Sanz Grossón (DENIC eG)
- Dr. Nik Scharmann (Robert Bosch GmbH)
- Marc Schieder (DRACOON GmbH)
- Ralph Schirmeisen (Hewlett Packard Enterprise)
- Arne Schmieg (German Edge Cloud GmbH & Co. KG)
- Christian Schmitz (ownCloud GmbH)
- Alban Schmutz (OVHCloud SAS/CISPE)
- Stefan Schnaus (Fujitsu TDS GmbH)
- Volker Schnittler (VDMA e.V.)
- Marco Schuldt (Bundesministerium für Wirtschaft und Energie)
- Alexandre Seifert (vertical GmbH)
- Olivier Senot (DOCAPOSTE SAS)
- Sebastian Steinbuß (IDSA e.V.)
- Alexander Stöhr (XignSys GmbH)
- Rainer Sträter (1&1 IONOS SE)
- Olav V. Strawe (4Com GmbH & Co. KG)
- Dr. Christoph F. Strnadl (Software AG)
- Kai Stursberg (Deutsche Telekom AG)
- Prof. Dr. Ali Sunyaev (Karlsruher Institut für Technologie (KIT))

- Andreas Tamm (Arvato Systems GmbH)
- Rui Manuel Tavares (Fujitsu Technology Solutions GmbH)
- Romano Tesone (SAG Deutschland GmbH)
- Prof. Dr. Oliver Thomas (Deutsches Forschungszentrum für künstliche Intelligenz GmbH)
- Dr. Philipp Trinius (T-Systems International GmbH – Telekom Security)
- Michael Tufar (SAG Deutschland GmbH)
- Alexandra Ulbricht (Fujitsu Technology Solutions GmbH)
- Dr. Constantino Vázquez (OpenNebula Systems SL)
- Markus Vehlow (PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft)
- Alexander Vowinkel (Deloitte Consulting GmbH)
- Markus Wartha (EDASCA SCE)
- Dr. Christian Weiss (Deutsche Telekom AG)
- Andreas Weiss (EuroCloud Germany)
- Sascha Wessel (Fraunhofer AISEC)
- Dr. Sabine Wilfling (Scheer GmbH)
- Alexander Willner (Fraunhofer FOKUS)
- Dr. Dirk Woywod (Verimi GmbH)
- Dipl. -Inf. Andreas Zerfas (German Edge Cloud GmbH & Co. KG)
- Tim Zöllner (noris network AG)