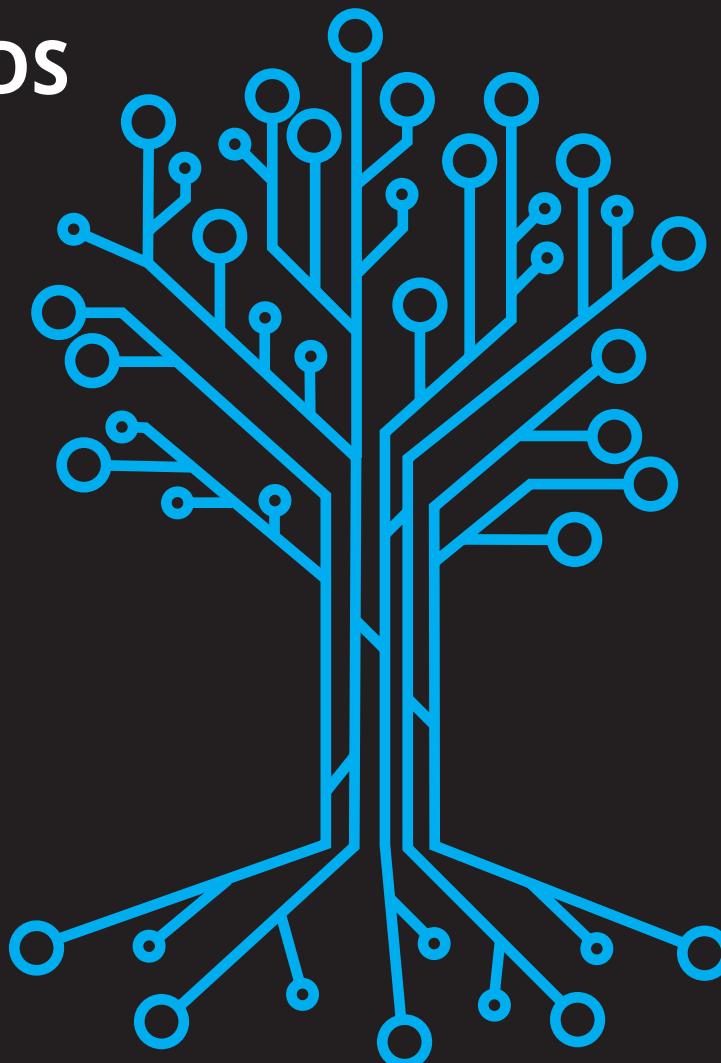


Position Paper | Version 1.0 | January 2021

GAIA-X and IDS



- Position Paper of members of the IDS Association
- Position Paper of bodies of the IDS Association
- Position Paper of the IDS Association
- White Paper of the IDS Association



Publisher

International Data Spaces Association
Anna-Louisa-Karsch-Str. 2
10178 Berlin
Germany

Copyright

International Data Spaces Association,
Dortmund 2021



Editor

Prof. Dr. Boris Otto
Fraunhofer Institute for Software and Systems
Engineering ISST

Cite as

Otto B. et al. (2021): GAIA-X and IDS.
International Data Spaces.
<https://doi.org/10.5281/zenodo.5675897>

Authors & Contributors

Prof. Dr. Boris Otto, Fraunhofer ISST
Alina Rubina, DE-CIX Management GmbH
Andreas Eitel, Fraunhofer IESE
Andreas Teuscher, SICK AG
Anna Maria Schleimer, Fraunhofer ISST
Dr. Christoph Lange, Fraunhofer FIT
Dr.-Ing. Dominik Stingl, DE-CIX Management GmbH
Evgeni Loukipoudis, DTS
Gerd Brost, Fraunhofer AISEC
Gernot Böge, FIWARE Foundation e.V.

Heinrich Pettenpohl, Fraunhofer ISST
Jörg Langkau, nicos AG
Joshua Gelhaar, Fraunhofer ISST
Koki Mitani, NTT Corporation
Marius Hupperz, Fraunhofer ISST
Monika Huber, Fraunhofer AISEC
Nils Jahnke, Fraunhofer ISST
Robin Brandstädtter, Fraunhofer IESE
Sascha Wessel, Fraunhofer AISEC
Sebastian Bader, Fraunhofer IAIS

Contributing Projects



International Data Spaces



Federal Ministry
of Education
and Research

This work has been supported by the German Federal Ministry of Education and Research (BMBF) in the context of the InDaSpacePlus project (no. 01IS17031) and by the Fraunhofer Cluster of Excellence »Cognitive Internet Technologies«.



Contents

Introduction	4
Management Summary	4
Purpose of this document	4
Motivation	5
Background	6
IDS Architecture	6
GAIA-X Architecture	8
Integration & Differences between GAIA-X and IDS.....	13
High-Level Overview	13
Digital Identities	14
Certification.....	15
Interoperability - Data / Services	17
Self-Description	19
Usage Control.....	24
Trustworthy Runtime	26
Next Steps	28
References.....	29



Introduction

Management Summary

This position paper demonstrates how elements of the International Data Spaces Reference Architecture Model fit to the GAIA-X principles and architecture elements described in the Technical Architecture whitepaper. The view is based on the June 2020 documents, which are the latest technical documents available. Also, recent architectural decisions are considered, which both cover together the areas of digital identities, certification, self-description, usage control as well as interoperability and data services as well as trustworthy runtime.

The comparison shows, that GAIA-X is not as mature as the International Data Spaces (IDS) initiative, but follows the same vision of proliferating data sovereignty and create an ecosystem of trust for data sharing. The IDS initiative and IDS Reference Architecture Model (IDS-RAM) offer various concepts and solutions that contribute to the overall vision of GAIA-X and to the concrete GAIA-X architecture demands. On the other hand, GAIA-X provides concepts that include the data storage and cloud-related elements, which can complement the IDS architecture.

The conceptual mapping results in the following high-level relationship:

- The Federated Catalogue comprises the IDS Broker, Vocabulary Provider and Information Model
- The Federation Service of Sovereign Data Exchange stems on IDS Usage Control and Clearing House
- The GAIA-X Federation Service of Identity & Trust benefits from the IDS Identity Provider and Dynamic Attribute Provisioning Service (DAPS)
- GAIA-X Nodes are aligned with IDS Connectors as gateways
- The GAIA-X Data Ecosystem is the place where IDS Data Provider and Data Consumer are conceptually located
- The IDS Service Provider, IDS App Store Provider and App Provider are located in the GAIA-X Infrastructure Ecosystem

Purpose of this document

This position paper gives a first overview of the architectures of GAIA-X and International Data Spaces. This is followed by a discussion on how the two infrastructures are or can be aligned to one infrastructure. We only focus on the alignment of IDS and GAIA-X without any discussions about other initiatives like Plattform Industrie 4.0, SWIPO (Switching Cloud Providers and Porting Data), or similar. This current paper also does not specifically address synergies with the Once-Only technical system developed by the European Commission for the public sector, which will re-use mature solutions from the CEF Building Blocks and the ISA² Core Vocabularies.

From our perspectives, these initiatives are also highly relevant and are partly linked to both, IDS and GAIA-X initiatives, but an integration would go beyond the scope of this paper.



Motivation

Driven by the conviction that we can push forward the development of a sustainable and innovative data economy in Europe, the GAIA-X project was launched in autumn 2019. Encouraged by widespread support, the development of a trustworthy and sovereign digital ecosystem for Europe remains the declared goal. Thereby, it is not geographically restricted but refers more to European values when referring to a European ecosystem. This European digital ecosystem will foster innovation and proliferate new data-driven services and applications. To this end, GAIA-X will enable interoperability and portability of infrastructure, data and services and establish a high degree of trust for users. Existing difficulties like diverse cloud-edge landscapes, legal uncertainties or technological integration issues hinder the emergence of a strong digital single market. The project is closely aligned with the European Data Strategy, which strives towards a genuine single market for data, as well as the EU Recovery Plan. In accordance to that, GAIA-X supports innovative data applications and innovation across industry sectors. By considering European values, GAIA-X is seen as a step towards technological independence of Europe. This encompasses avoiding vendor lock-in situations to foster a free market, as well as fundamental values of transparency and freedom of choice.

However, designing an infrastructure that enables digital sovereignty is only one part of GAIA-X. The other part is to enable sovereign data exchange by transferring the data to the infrastructure, but also to utilize the data for new data-driven services. A key capability for the European and International economy therefore is data sovereignty. Data owners must be able to decide, control and monitor what happens to their data, who receives it and what it is used for. This requires uniform economic and legal procedures and standards on the one hand, and on the other hand an information technology procedure to enable and exercise data sovereignty in the first place.

Currently, more than 40 use cases describe scenarios that benefit from GAIA-X and are expected to foster GAIA-X concepts and technologies in future. They capture different domains, ranging i.a. from health, finance, or mobility to public administration or agriculture – all obtaining specific needs and particularities.

In October 2015, the Fraunhofer Society initiated the International Data Spaces (IDS) project, former Industrial Data Space, funded by the German Federal Ministry of Education and Research. The IDS initiative aims at standardizing data exchange and data sharing between participants while enabling them to keep sovereignty over their own data. This endeavour is supported by the non-profit organization named International Data Spaces Association (IDSA), which is actively contributing. In 2020, the IDSA consists of 117 members from all over the world who together define the IDS standard for data sovereignty. The members of the IDSA come from different industries and provide use cases where the IDS architecture is applied in their corresponding domain, which already presents an analogy to GAIA-X.

GAIA-X is a fairly new initiative with a first high-level architecture where a demonstrator-like Minimal Viable GAIA-X is expected in the first quarter of 2021, whereas the IDS architecture is much more mature and has already been tested by several systems in science and industry. This will result in a high-level alignment between these two initiatives.



Background

The following chapter describes the architectures of the IDS and GAIA-X. First, an architecture overview is provided for both initiatives followed by an explanation of basic terms. Then, particular aspects and elements of special interest follow. Especially the fairly new technical elements of the GAIA-X architecture are explained.

IDS Architecture

Architecture Overview

Digitization is both driver and enabler of innovative business models. Key resource for enterprises to succeed in this endeavour is data. A prerequisite for smart services, innovative value propositions and automated business processes is the secure exchange and the easy combination of data within ecosystems. In this context, the International Data Spaces aim at creating a secure data space that supports enterprises of all industries and sizes in the autonomous management of data. A key capability for organizations to develop in order to be successful in the data economy is data sovereignty.¹ It can be defined as a natural person's or corporate entity's capability of being entirely self-determined regarding its data. The International Data Spaces propose an architecture for this central capability and related aspects, including requirements for secure and trusted data exchange and sharing in business ecosystems.

The IDS Reference Architecture Model (IDS-RAM) provides several elements, roles and interactions that constitute an infrastructure for sovereign data exchange (see Figure 1).²

Core Participants are **Data Owner**, **Data Provider**, **Data Consumer** and **Data User**. Here the term Data Owner is not used in a legal understanding but rather seen from a management perspective. Therefore, a Data Owner is defined as a legal entity or natural person creating data and/or executing control over it. This enables the Data Owner to define Data Usage Policies, the Payment Model, and provide access to its data. Usually, a participant acting as Data Owner automatically assumes the role of the Data Provider as well. However, there may be cases in which the Data Provider is not the Data Owner especially in the context of increasing usage of cloud providers and data centres. For example, if the data is technically managed by a different entity than the Data Owner, such as in the case of a company using an external IT service provider for data management.

¹ BMWi, GAIA-X: Driver of digital innovation in Europe, 2020:

<https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-a-pitch-towards-europe.html>

² IDSA, IDS Reference Architecture Model 3.0, 2019:

<https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

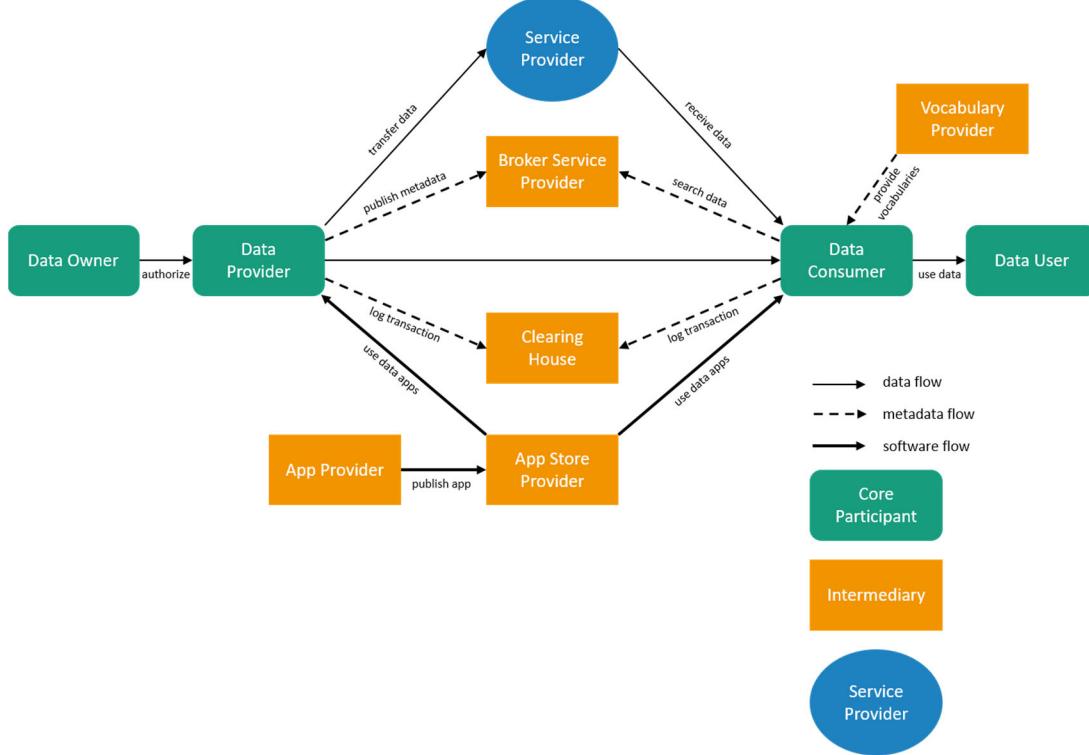


Figure 1: IDS Roles and Interactions (source: IDSA, IDS RAM 3.0)

Basic Terms

A first fundamental aspect for all core participants mentioned in Figure 1 is **certification**. Most roles in the IDS require certification of the organization that wants to assume that role. This includes certification of the technical, physical, and organizational security mechanisms the organization employs. Additionally, all components used in the ecosystem must be evaluated and certified on a technical level in order to ensure their conformance to the IDS standards as well as adequately used security mechanisms. By having an independent third party conducting the evaluation and confirming the correct implementation, the certification establishes trust in the whole ecosystem. The Certification Scheme applied is described in detail in Section 0.

The **IDS Connector** is responsible for the exchange of data, as it executes the complete data exchange process from and to the internal data resources and enterprise systems of the participating organizations.³ It is important to note that the data is transferred between the Connectors of the Data Provider and the Data Consumer (peer-to-peer network concept). The Connector architecture uses application container management technology to ensure an isolated and secure environment for individual data services.⁴ The IDS Connector, one of the International Data Spaces' core components, connects industrial data clouds, as well as

³ for a detailed explanation on Data discovery and data exchange see IDSA, IDS Reference Architecture Model 3.0, 2019, pp.36-39:
<https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

⁴ IDSA, Position Paper Usage Control in IDS 2.0, 2019:
<https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Usage-Control-in-IDS.pdf>



individual enterprise clouds, on-premises applications and individual, connected devices and therefore provides the technical access to an IDS ecosystem. It provides metadata to the IDS Broker as specified in the Connector self-description, e.g. technical interface description, authentication mechanism, exposed data sources, and associated data usage policies.⁵

Intermediaries are Broker Service Provider, Clearing House, App Store Provider, App Provider, and Vocabulary Provider. For data exchange, the Data Provider makes metadata available via the **IDS Broker**. A Data Consumer can search this metadata for a dataset that fits their requirements. If the terms and conditions of the Data Provider match the needs of the Data Consumer, data exchange can take place. For this instance, the Connector logs the data transaction and sends the data record to the **Clearing House**. Additionally, **Data Apps** can further process the exchanged data. Those Data Apps are available in an **App Store**. They are deployed within the IDS Connector to facilitate data processing workflows. To annotate and describe datasets, specific vocabularies are offered by the **Vocabulary Provider**.

The **Identity Provider** provides an authentication service for all IDS participants. It offers a service to create, maintain, manage, monitor, and validate identity information of and for participants in the IDS. This is of particular importance for the network of trust in the IDS.

Moreover, **IT companies** may provide software and/or services to the **IDS participants**. Roles subsumed under this category are Service Provider and App Provider. Service providers in the IDS can combine data from different data providers or refine individual data assets, thus creating added value for the data consumer. Another category of roles is presented by the Governance Body. This category belongs to the Certification Body and Evaluation Facilities, which are in charge of the certification of participants and core technical components (e.g. Connector).

GAIA-X Architecture

Architecture Overview

According to the vision and objectives of the architecture, the core architecture principles include **openness** and **transparency**, **interoperability**, **federation** as well as **authenticity** and **trust**. The following technical guidelines enforce these principles and assure compliance with the GAIA-X vision:

- Security-by-design
- Privacy-by-design
- Enabling federation, distribution and decentralisation
- User-friendliness and simplicity
- Machine-processability
- Semantic representation

The GAIA-X Ecosystem is formed by an **Infrastructure Ecosystem plus a Data Ecosystem**, both connected via **Federation services** while the whole architecture bases upon Policy Rules and an Architecture of Standards. Both follow the idea of a shared economy where you can share your data and services while applying policies and maintaining sovereignty over them. The two ecosystems cannot be viewed separately. Within the Infrastructure Ecosystem

⁵ Fraunhofer IDS Software: www.dataspaces.fraunhofer.de/software

infrastructure services are provided, connected or consumed, while the Data Ecosystems deal with data as the main business asset. Similar to the IDS, ecosystem participants are classified into the general roles Provider and Consumer. According to the activity, an entity can have both roles at the same time. Figure 2 provides a high-level architecture overview. To realize this architecture, GAIA-X aims at leveraging existing standards as well as open technologies and concepts. By combining existing solutions **GAIA-X acts as orchestrator and integrator**. It is neither an additional hyperscaler nor obtains an own central data storage.

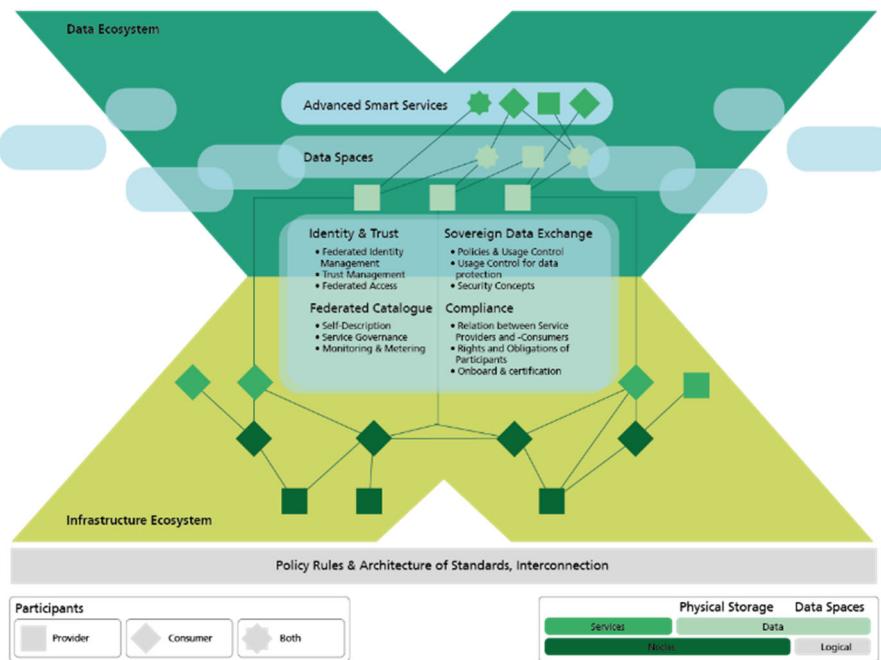


Figure 2: GAIA-X Architecture (own adaption based on BMWI 2020, GAIA-X Technical Architecture)

Basic Terms

This section introduces the main assets of GAIA-X, namely Nodes, Services, Service Instances, and Data Assets.

A **Node** is a general computational resource or infrastructure element, which may range from an edge resource to a virtual machine, a container, a data centre or any other generic infrastructure building block that services can be deployed on. Nodes are placed in the GAIA-X Infrastructure Ecosystem.

In the GAIA-X language, **Services** describe a **cloud offering** including all kinds of cloud services. In GAIA-X, Services are offered by a **Service Provider**. If a service is realized on a GAIA-X **Node**, it is called a **Service Instance**. Service Instances can run on one or more nodes. Further, Services can be combined with each other, e.g., a data service on a platform, enabling the creation of service cascades. During all Service executions, GAIA-X enables interoperability. Thus, **Services become portable from one Node to another**.

The term **Data Asset** describes a data set, which is provided to consumers via GAIA-X Services and made available or hosted on GAIA-X Nodes. These Data Assets can be searched and

consumed by GAIA-X participants. They can also be hosted privately. Similar to Services, Data Assets can be leveraged in combination with each other and form data spaces according to the federated character of the ecosystem.

A **GAIA-X Participant** is typically a business organization participating in the ecosystem, but can also be a natural or any form of a legal person. The participating entity obtains the role of a provider, consumer or both, depending on the respective business case. Each Asset has an associated **GAIA-X Provider** belonging to the GAIA-X ecosystem so that no provisions from outside without self-descriptions are allowed. In addition to these core roles, further ones exist. Examples are Service Provider, Service Instance Provider, or Node Provider.

To express their properties and characteristics, Participants and Assets use obligatory GAIA-X **Self-Descriptions**. Every element of GAIA-X has a Self-Description. This contains structured, searchable metadata about concepts such as data owners and usage policies. Providers of Assets themselves are responsible for the creation of their respective Self-Descriptions. Self-Descriptions are expressed using a graph data structure. They contain mandatory attributes that are predefined by the GAIA-X entity according to the type of Asset or Participant as well as optional attributes. To testify a claimed attribute or certification, portions of the Self-Description are being signed by trusted parties. The creation and check of the respective Self-Description will be an essential part of each organization's and asset's onboarding process. To its facilitation, a tool will be made available. Furthermore, the option of hierarchical Self-Descriptions will enable Providers to inherit parts of their Self-Description to their Assets. Overall, Self-Descriptions establish trust and facilitate the decision-making process.

On a technical level, Self-Descriptions serve different functionalities: They represent the foundation to search and select assets in catalogues and are as well used to apply and monitor usage policies. Furthermore, contract negotiation can be conducted on the basis of Self-Descriptions.

Federation services

Federation services are the core of GAIA-X as they interconnect the Infrastructure and Data Ecosystem. They comprise on the one hand infrastructure services, but on the other hand also organisational support functions. They include Identity and Trust Services, Compliance Services, Federated Catalogues and Sovereign Data Exchange Services.

The discovery of assets will take place by means of the **Federated Catalogue**. Therefore, different instances of the **Federated Catalogue** can exist. For instance, Data Assets need proper **Self-Description** to be found by data consumers. Therefore, an open and transparent query algorithm is implemented to satisfy consumer needs and to objectively find the best fitting offerings in the tangle of registered assets. This makes Catalogues the main building block for the publication and discovery of Self-Descriptions of Data Assets and participants. It is important to note, that GAIA-X Data Connectors are part of the Federated Catalogue.

In addition, **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. In addition to that, metering offers access to performance indicators and consumption statistics. Monitoring capabilities as well as standard metering interfaces will be made available as a part of the Self-Description functionality.

The category of **Identity & Trust** features methods that ensure the Participants' identities can be verified and trust towards their capabilities and assets can be created. A central method is represented by the **Federated Identity** model. It contributes to a trustful environment by several means. In particular, federated identity management makes identities operable between different domains by connecting several national and international identity providers. Already existing identities can be handed over by businesses that are regarded as trustworthy entities. The federated identity model incorporates widely accepted practices and processes as well as general and domain-specific policies.

For the diverse Services and Nodes offered within the GAIA-X ecosystem, three different assurance levels will be introduced. These levels describe the conformity of a Participant, Service or Node to information security and data protection requirements. Whereas the basic level has to be fulfilled by every Participant, substantial and high assurance is needed for Services and Nodes that support mission-critical or share and store sensitive data, respectively.

Definitions to ensure **Compliance** are established for the relation between **Service Provider** and **Service Consumer**, as well as rights and obligations for participants and onboarding and certification procedures. First, the relation between Service Provider and Consumer is framed in a Legal Context which is not necessarily explicitly represented in a technical system. One part of the Legal Context is the Service Context, which includes Policies as well as Metering and Billing of Service consumption. The GAIA-X Technical Architecture paper defines Policies as a set of assertions that restricts the behaviour and usage of an Asset. In a concrete Service Usage Session, a Provider's Service instance interacts with a Consumer's Service Client, a technical system controlled by the Consumer. Here, Self-Descriptions verify each one's identity and also serve to match each one's Policies: This means in particular Provider Policies, describing usage restrictions, and Consumer Policies, restricting the attributes of assets to be consumed. The Technical Architecture paper further provides a sum-up of general Rights and Obligations of GAIA-X Participants.

To enable and ensure a natural or legal person's ability to decide exclusively how his data are to be used, **Sovereign Data Exchange** services are established by GAIA-X. A prerequisite is interoperability on the metadata level, as it enables self-determined decision-making regarding the use and processing of his data. A key component of data sovereignty is the enforcement of **Usage Policies**, so-called Usage Control. Policies describe the terms and conditions under which data assets can be used on the consumer side. Enforcement of these Policies allows control of the Provider's data after leaving his system boundaries. Another technical mean closely connected to Usage Control is the ability of decentral and auditable logging. In this logging, the term describes a business-related logging to document business transactions. It permits undertaking organizational or legal measures to ensure conformance to Usage Policies where technical enforcement is not possible.



Policy Rules, Architecture of Standards & Interconnection

To ensure high-level data protection, security, transparency and portability within the GAIA-X ecosystem, a framework of **Policy Rules** is being developed. They describe common ground rules and principles for collaboration and participation in GAIA-X. All Participants accept the rules as a prerequisite to join the ecosystem and also the offered Services have to adhere to them. Most of the Policy Rules are based on the European regulatory frameworks and driven by the focus on data sovereignty and self-control over critical information. According to the division in two ecosystems, namely Data and Infrastructure Ecosystem, two sets of rules are present.

The use of standardized data models and interaction patterns is important to enabling interoperability between nodes, user-friendly services, exchangeability of Service Providers and data exchange between different instances in the Infrastructure Ecosystem. As a variety of standards already exist, the most suitable ones to set up a sovereign data infrastructure in Europe are selected and integrated into an **Architecture of Standards**. These standards can be regulatory, technical or industry-specific. Within GAIA-X, the Data Ecosystem and the Infrastructure Ecosystem have to be combined to enable a seamless exchange of data and services in a federated cloud architecture.⁶

Such a federated architecture is unimaginable without an underlying interconnected network infrastructure. In this regard, Interconnection and Networking represent the main building blocks to connect and federate the different entities of the Infrastructure Ecosystem with each other. In order to search for and choose the appropriate type of **interconnection** and networking, they are modelled as services with a machine-readable Self-Description. Based on this description, GAIA-X participants are able to seek for and choose the appropriate interconnection and networking services according to their needs. These building blocks will enable the formation of a federated and interconnected GAIA-X networking infrastructure.

⁶ BMWI, GAIA-X: Technical Architecture, 2020:
https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=2

Integration & Differences between GAIA-X and IDS

High-Level Overview

The combined architecture of GAIA-X and IDS supports and enables data spaces and builds advanced smart services in industry verticals. GAIA-X focuses on sovereign cloud services and cloud infrastructure, while IDS focuses on data and data sovereignty. The interaction of GAIA-X and IDS has three main tasks: self-sovereign data storage, trustworthy data usage and interoperable data exchange. This way, GAIA-X is developed in accordance with the European Data Strategy and supports smart data applications and innovations across industry sectors. For this purpose, GAIA-X and IDS complement each other to ensure cloud and data sovereignty for end-to-end data value chains in federated ecosystems.

Figure 3 presents a mapping of IDS components into the GAIA-X architecture. The Data Provider and Data Consumer are mapped into the GAIA-X Data Ecosystem, while the App Store Provider, App Provider and Service Provider are rather located in the GAIA-X Infrastructure Ecosystem.

The IDS Connectors can be integrated in the GAIA-X Nodes, as they work as secure gateways. It is important to note, that Connectors do not restrict to the GAIA-X Data Ecosystem, but reach down the whole stack including the GAIA-X Infrastructure Ecosystem for security reasons.

The four Federation services are also congruent to various IDS concepts: A key element is the GAIA-X Federated Catalogue, which leverages the IDS Broker, Vocabulary Provider and Information Model. The Federation Service of Sovereign Data Exchange is represented by the IDS Clearing House and Usage Control concept. Further, the GAIA-X Federation services of Identity & Trust and Certification can take advantage of the IDS Identity Provider and IDS Certification Body.

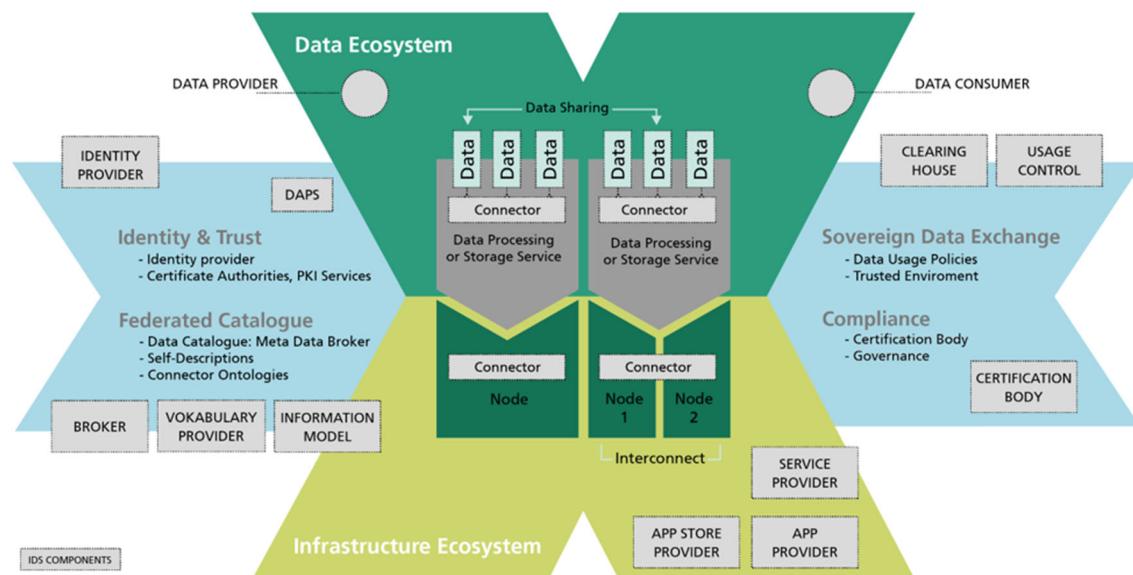


Figure 3 Mapping of IDS Components into the GAIA-X Architecture (source: GAIA-X initiative)

Digital Identities

The IDS identity concept provides means to handle **dynamically changing attributes without the need for certificate revocation and reissuance**. The identity concept for devices is a pluggable and modular concept, building on top of a traditional PKI foundation. Dynamic attributes provided by the Dynamic Attribute Provisioning Service (DAPS). Authorization Services for specific use cases are also supported.

Identity certificates can be created for devices and services. The certification and evaluation processes call for signatures of software artefacts, created by individuals representing their function and organization. Figure 4 gives an overview about the Identity concept in the IDS with the usage of X.509 certificates for connectors. Personal identities are planned to be integrated in the future.

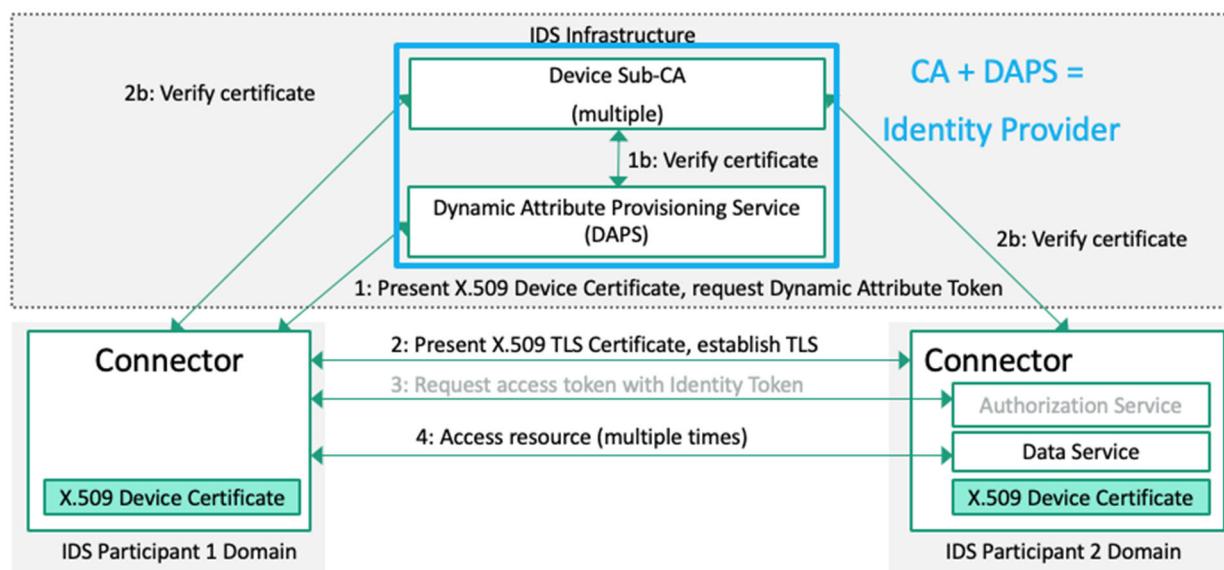


Figure 4 IDS Identity Concept for dynamic identity attributes (source: IDSA 2019, IDS RAM 3.0)

IDS identity management is designed to create trust chains that support the creation, evaluation and acceptance of software artefacts by creating individual signatures after each step (publication and evaluation stages). The concept is designed with flexibility in mind: Device Certification Authorities (CAs), which are responsible for issuing, validating and revoking digital certificates and identities, are supported by either using a central infrastructure CA or by using company and vendor specific CAs. eIDAS support for users is also part of the concepts, incorporating the possibility of introducing Trust Service Providers into the scheme.⁷

IDS and GAIA-X both envision trust relationships across company boundaries, enabling complex service and data value chains. Both rely on a strong trust model. Where IDS components focus on Connectors as gateways for Edge- and cloud applications, GAIA-X is

⁷ European Commission, Trust Services and Electronic identification: <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

Service- and Node-oriented, calling for identity and trust schemes that support assurance levels, status tracking and certification approaches.

IDS and GAIA-X both rely on multiple assurance levels: IDS Connectors are based on the Security Profiles Base, Trusted and Trusted+. Trusted relies on multiple security layers such as hardware trust anchors and Trusted Execution Environments. Pushing even further, Trusted+ supports protection from unauthorized changes on the Connectors. This maps to the assurance profiles used in GAIA-X (see next section for details on assurance levels).

IDS rely on X.509 certificates for organizational, personal and technical identities (Connector identities). Connector identities are enriched with dynamic identity claims based on OAuth2. GAIA-X also relies on identity claims, using Decentralized Identifiers and Verifiable Credentials. These are container formats and credential verification protocol blueprints which can be harmonized with the IDS approach. IDS support the verification of identity claims (depending on the trust level) based on technical means (such as remote integrity verification for higher trust levels). These means can be integrated into Verifiable Credentials using custom proof mechanisms. Both approaches call for a federated identity system by allowing the integration of existing organizational identity providers into a harmonized identity system.⁸

Certification

In addition to the establishment of trustworthy digital identities for the participants in the ecosystem, the organizations in the IDS must ensure that their operational environment and their management processes fulfil a certain level of security. Likewise, GAIA-X Nodes and Services must be operated in a reliable manner. The companies' trustworthiness as well as the compliance of GAIA-X Nodes and Services with defined functional and security requirements must be verifiable on a technical level. Such proofs of their trustworthiness are used in advance to the transfer of data between different services as well as before providing GAIA-X Services with (potentially sensitive) data. In addition, reliable verification techniques are used as basis for continuous monitoring.⁹

In a comparable manner, the IDS offer certification for operational environments of the participating companies as well as for the technical components utilized for data exchange and enforcement of usage control policies. For both types of certification, the IDS specified a respective matrix of possible certification levels based on:

- Three security profiles with an increasing list of requirements for each security level / profile (see Figure 5)
- Three assurance levels with an increasing depth of the evaluation conducted for each level (see Figure 6)

⁸ IDSA, IDS Reference Architecture Model 3.0, 2020:

<https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

⁹ IDSA, IDS Certification explained, 2019

<https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-IDS-Certification-Explained.pdf>



	Self- Assessment	Management System	Control Framework
Entry Level	✓	✓	
Member Level		✓	✓
Central Level		✓	✓

Figure 5 Assurance Level (source: IDSA 2019, IDS Certification Explained)



	Checklist Approach	Concept Review	High Assurance Evaluation
Base Security Profile	✓	✓	
Trust Security Profile		✓	✓
Trust+ Security Profile		✓	✓

Figure 6 Security Profiles and Assurance Level (source: IDSA 2019, IDS Certification Explained)

The different security profiles map to the three assurance levels, which are currently specified in GAIA-X: *Basic*, *substantial*, and *high*.

Additionally, GAIA-X and IDS share common goals: Data sovereignty, interoperability, the reusing of established standards as well as providing a secure and trustworthy data ecosystem. As these objectives form the basis for the necessary requirements, GAIA-X can substantially benefit from the work done in the IDS certification in the past years to reduce costs and effort. With the IDS-Ready label, which has already been issued, for instance, to the so-called Data Intelligence Hub (DIH) connector of T-Systems as well as the Trusted Supplier Connector (TSC) of the German Edge Cloud, first evaluations of concepts for technical components exist that implement the named shared goals.

In particular, the following assets from the IDS can be reused for GAIA-X:

- Certification criteria for data sovereignty in IDS components and for IDS participants
- DIN SPEC 27070: a standard with requirements for security gateways which was established in consultation with many industrial partners (ISO adoption planned)
- Procedures and tooling for implementing the certification in a technical verifiable format (using code signatures of trusted third parties)¹⁰

IDS and GAIA-X both have the goal to provide open source implementations of each necessary core component. The reuse of functionalities required for both an IDS Connector and a GAIA-X Node will provide useful synergies for all involved parties. The result should also include a certification for this reference implementation, which can be reused in products addressing both the IDS-Community and GAIA-X. The same holds true for the development of tools to verify conformance to the standards and security of the components.

¹⁰ DIN SPEC 27070 <https://www.din.de/de/wdc-beuth:din21:319111044>

Interoperability - Data / Services

The intended seamless exchange of data and services across systems, networks and organizations requires a shared understanding of data exchange and interaction patterns (1), data formats (2), the meaning of information data descriptions (3) and the process workflows (4) driving them. Furthermore, the self-sovereign approach of both the IDS and GAIA-X also requires the exchange of intended and unintended usage declarations (5). This understanding is necessarily not only required for humans, but the semantic meanings have to be accessible for technical components, participating in the data exchange or proving central infrastructure. With the rich IDS Information Model based on the Semantic Web and the RDF specifications, the IDS describe all these facets of shared knowledge at a single source, both understandable for machines and users. This will be discussed in further detail in Section 0 on Self-Description below.

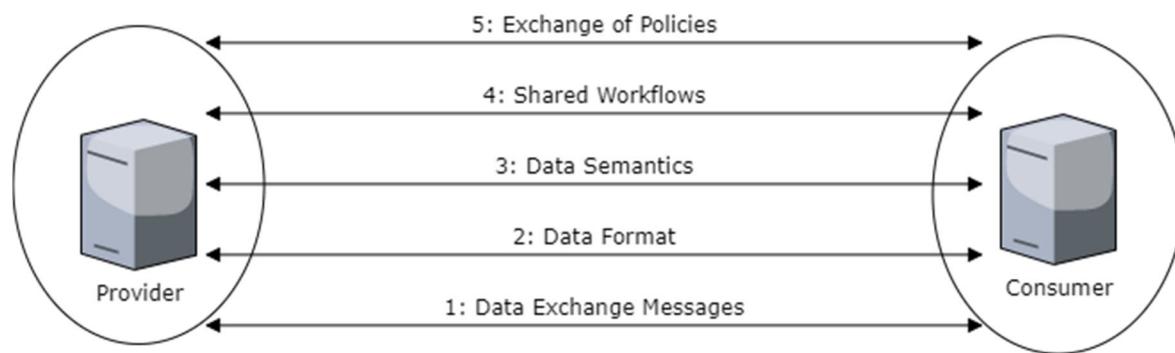


Figure 7 Interoperability Stack (own visualization)

Data Exchange and Interactions

Both GAIA-X and the IDS currently develop a REST API description. The IDS promote the principles originally presented in the Linked Data Platform (LDP) specification, a W3C Recommendation since 2015. The thereby integrated interaction sequences directly support the core advantages of REST interactions with semantically annotated data while enabling a transparent mapping of READ and WRITE operations in decentralized networks. The IDS further extend the LDP Recommendation by introducing further security and accountability features as well as a mapping to the rich message model of the IDS. Via a draft Architecture Decision Record on "REST as the Interface Technology for Federation Services", GAIA-X is already committed to REST interactions as the primary means of interaction in GAIA-X. This can easily be extended towards the design principles as developed for IDS interactions, thereby integrating discoverability by HATEOAS, content negotiation, strict resource-orientation and a scalable model for responsibilities and access management in distributed architectures like the Web. While GAIA-X aims also for the integration of Human User Interfaces for the leveraging of these APIs, the focus of the International Data Spaces remains on automated data exchange. For application domains with higher trust requirements, IDS offers the IDSCP, a protocol which enables the creating of a secure tunnel bound to system integrity verification and remote attestation. These mechanisms will be supported for gateways as well as cloud-based infrastructure, based on Trusted Execution Environments (TEEs). These concepts will be merged into GAIA use cases with higher trust requirements.



Data Format

Similar to the REST approach, both the IDS and GAIA-X promote the usage of JSON as the central standard, in particular the semantically self-describing JSON-LD, as detailed below in Section 0. This widely accepted and well-supported syntax allows the efficient transport of any kind of structured information. The obvious advantages, the rich tool support and the widespread usage in the area of web services, reduce the hurdles for serializing, exchanging and parsing data objects. Consequently, this requirement is out of the box fulfilled by both approaches in the same way, though the current status might change in the future. While the IDS allow other data serialization formats to be exchanged, GAIA-X needs still to specify all accepted standards. Shared data descriptions in order to unambiguously exchange information, and to prevent misunderstandings or data loss, also the intended meaning of exchanged data objects, is crucial; cf. the Section 0 on Self-Description. The semantics of data exchanged is given by vocabularies (in this context also, synonymously, called "ontologies" or "schemas"). In addition to the general-purpose, foundational role of the IDS Information Model and, similarly, the emerging GAIA-X Self-Description ontology, the operators of domain-specific data and service spaces driven by IDS or GAIA-X technology need to agree on additional domain-specific vocabularies. Over their entire lifecycle, these vocabularies will be managed by an IDS Vocabulary Provider and, respectively, the GAIA-X Federated Catalogue.

Shared Workflows and Standardized Processes

The core requirement for any higher-level interaction are shared Identity Management mechanisms, as outlined in Chapter 0. In addition to that, several infrastructure components promote information validation and input for the processes, like Data-Catalogues and Participant-Catalogues together with Identity Validation. Building on that, each involved component of a distributed ecosystem needs to understand the fundamental processes to establish a business process, execute its operations and successfully terminate it afterwards. The Process Layer of the IDS Reference Architecture Model and the IDS Usage Policy Negotiation sequence are examples of such complex processes, which combine several interactions and requests into meaningful workflows.

Similar demands appear in GAIA-X, for instance in order to register and search for suitable services at a Federated Catalogue. Such workflows, also regarding a life cycle model of digital entities, have been defined already for the IDS Broker and form obvious collaboration possibilities between the IDS and GAIA-X. In contrast however, not aligning the processes imposes the risk of conflicts breaking business cases, even though a syntactic exchange of data might have happened successfully.

Policies and the Exchange of Intentions

The previous four layers enable the basic technical communication between components. Self-sovereign business models however require a further understanding about *what* is actually intended and *which* permissions each participant has received. In addition to the productive data, the components need to be enabled to also exchange the requirements and obligations imposed by the provisioning and consumption of data assets.

The IDS Usage Control Language paves the way to express such statements, share it with potential business partners and implement them in enforceable configurations.

Instances of this language, called IDS Contracts, represent legally binding agreements, which can be interpreted automatically and natively interconnected with the additionally supplied metadata, for instance as part of the Self-Descriptions of both GAIA-X and IDS assets and services. Thereby, unambiguous descriptions enable the formulation and implementation of arbitrarily complex business requirements in transparent and therefore trustworthy manners.¹¹

Self-Description

In line with its top-level Architecture Guidelines #5 “Machine-Processability” and #6 “Semantic representation”, GAIA-X envisages Self-Descriptions for all Assets and all Participants. The same holds for the IDS – the main difference is in the different scope of assets, as will be detailed in the subsection “Subjects of Self-Description” below, after having discussed the purpose of Self-Description. A dedicated subsection covers the common approach to the conceptualization and implementation of Self-Description in GAIA-X and IDS. We finally address the topic of trust in Self-Descriptions, where GAIA-X so far goes beyond the IDS.

Purpose and General Characteristics of Self-Descriptions

The GAIA-X Technical Architecture mentions the following purposes of Self-Descriptions, which are generally in line with the IDS-RAM.

- Enabling consumers to select offers (e.g., of services) based on their requirements, and, similarly, empowering Participants in their decision-making process, e.g., when discovering Assets in a Catalogue
- Enabling exchange, sharing and brokerage of data between GAIA-X Services, and between GAIA-X Services and non-GAIA-X Services.
- 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; expressive semantics, uniquely defined by a defined schema vocabulary – same as in the IDS, as discussed in Section 0.
- Navigable and uniquely referenceable from anywhere, in a decentralized fashion, where Self-Descriptions referring to other Self-Descriptions form a graph with typed relations. – This is, in principle, possible in the IDS as well, thanks to the common Linked Data foundation, but not yet explicitly realized in the IDS architecture. The IDS enable “navigation” through self-descriptions rather in specific defined scenarios. For example, descriptions of Data Assets are sent from the Data Provider’s Connector to a Broker and can then be retrieved by potential Data Consumers.

¹¹ W3C, Linked Data Platform: <https://www.w3.org/TR/ldp/>

- Accompanied by statements of proof (e.g. certificates and signatures), making them trustworthy by providing cryptographically secure verifiable information – not yet addressed in the IDS; see the discussion in Section 0.

Subjects of Self-Description

Figure 8 shows the types of Assets in GAIA-X and their relations. Of the GAIA-X Assets, introduced in Section 0, only Data Assets are directly comparable to the IDS in the narrow sense. IDS Data Apps have in common with GAIA-X Services that they process data, but whereas Data Apps are deployed in the small, restricted environment of the IDS Connector of, e.g., a Data Provider or Data Consumer, Services are deployed on Nodes connected to the whole cloud.

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

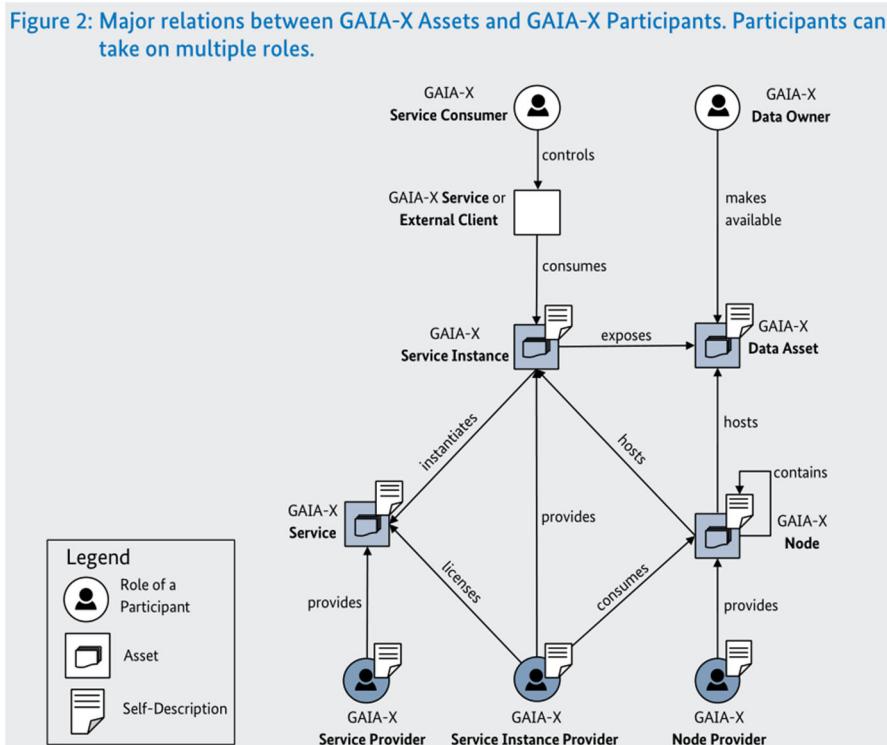


Figure 8: Top-level Self-Description Ontology (source: BMWI 2020, GAIA-X Technical Architecture)

In the IDS, self-description explicitly also applies to the components of the architecture as introduced in Section 0, e.g., Connectors, whereas the Self-Description of GAIA-X Federation services has so far only been addressed in an implicit way. IDS also require messages to self-describe in their headers. GAIA-X so far stipulates the “machine-readability” of all further artefacts such as messages, which is a weaker requirement and yet has to be elaborated towards full Self-Description.¹²

¹² Sebastian Bader, Jaroslav Pullmann, Christian Mader, Sebastian Tramp, Christoph Quix, Andreas W. Müller, Haydar Akyürek, Matthias Böckmann, Benedikt T. Imbusch, Johannes Lipp, Sandra Geisler, Christoph Lange. The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content. International Semantic Web Conference (ISWC) 2020.

GAIA-X and IDS have in common the Self-Description of Participants. In analogy to the different types of Assets, GAIA-X has a broader supply of Participant roles, including, e.g., the Node Provider.

The IDS Information Model takes a data-centric perspective. Everything that it covers can be seen as a “concern” affecting the exchange of Digital Resource; cf. the Concern Hexagon of the IDS-RAM (Figure 9).

Similarly, the Self-Description of a GAIA-X Data Asset 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. Thus, a Data Asset can be specified with own specific requirements with regard to Security and Data Protection as well as other administrative requirements, e.g., data lifecycle.

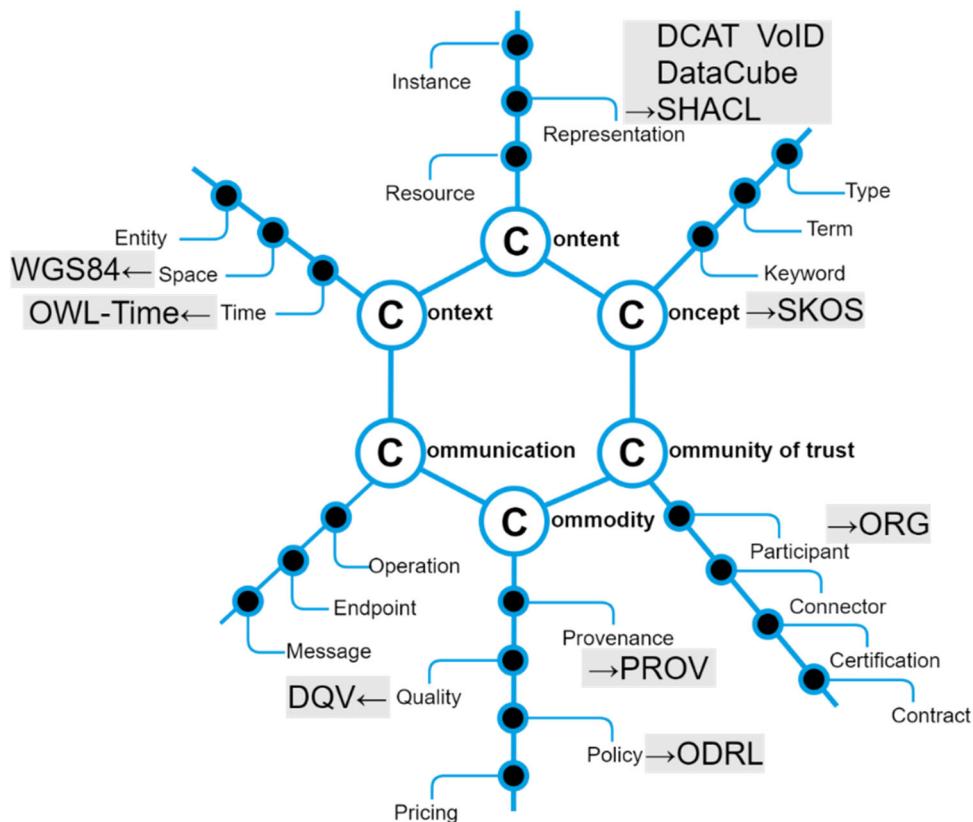


Figure 9: Concerns of Exchanging Digital Resources (source: IDSA 2019, IDS RAM 3.0)

Conceptualization and Implementation of Self-Description

The GAIA-X Technical Architecture provides the conceptual top-level ontology of self-descriptions (see Figure 8 above). Another diagram, cited here as Figure 10 provides further details; an even more detailed meta-model is being worked on, so far internally.

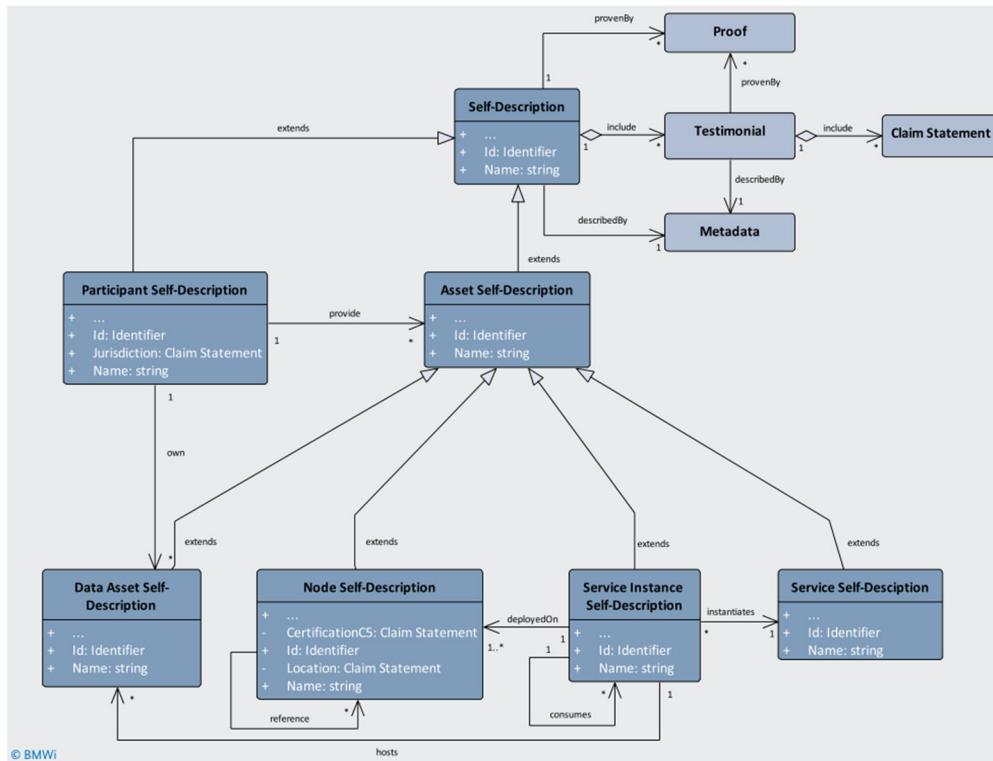


Figure 10 Schematic inheritance relations and properties for the top-level GAIA-X Self-Descriptions (source: BMWI 2020, GAIA-X: Technical Architecture)

Similarly, the IDS-RAM introduces the Information Model on three different layers, as summarized in Table 1 below.

IDS Information Model	GAIA-X Self-Description model
Conceptual layer: text and UML diagrams in the IDS-RAM	Text and diagrams in the GAIA-X Technical Architecture; meta-model
Declarative layer: ontology, validation shapes, queries	Ontology, validation shapes, queries
Programmatic layer: library ready to use in programming languages	No counterpart yet

Table 1: Layers of the GAIA-X Self-Description model and the IDS Information Model

The formalization and implementation of the schema of GAIA-X Self-Descriptions as an RDF/OWL ontology is work in progress. Top-down, the figures shown above translate into definitions of ontology terms in a straightforward way, e.g. (in the Turtle serialization of RDF):

```

gax:hosts a owl:ObjectProperty ;
rdfs:domain gax:Node ;
rdfs:range gax:ServiceInstance .

```

Via an Architecture Decision Record (ADR), it has been agreed that GAIA-X Self-Descriptions shall be encoded in the JSON-LD serialization of RDF. This is in line with common practice for IDS self-descriptions and message headers. In any case, conversion to other serializations such as RDF/XML or Turtle is possible using off-the-shelf tools.

Bottom-up, the GAIA-X community is currently collecting the terminology and knowledge that should be covered by the Self-Descriptions of various assets. For those subjects of Self-Description that GAIA-X has in common with the IDS, i.e., Data Assets and Participants, we consider the IDS Information Model well suited. While an in-depth discussion of GAIA-X Participants has yielded the requirement to cover multiple attributes beyond the limited scope of the IDS Information Model, and while an in-depth discussion of GAIA-X requirements for Data Assets is only beginning, the IDS Information Model has been realized to be by reusing multiple ontologies (cf. Figure 9) for its core concerns, and to ensure an easy integration of domain specific vocabularies to address requirements of applications that go beyond the core concerns of the Information Model itself¹³.

From a meta-modelling perspective, the GAIA-X community has raised certain requirements that go beyond the IDS Information Model. While the IDS Information Model is a straightforward RDFS ontology with limited use of OWL features, uses SHACL for validation purposes and makes use of SPARQL queries to retrieve self-descriptions, e.g., from a Broker, GAIA-X aims at a hierarchical organization of information, e.g., that one Node represents “a pan-European Node Provider that is structured into country regions, which are themselves structured into data centre locations, racks and individual servers, which themselves are exposed as GAIA-X Nodes.” It is a subject of ongoing discussions whether or how, e.g., redundant storage and synchronization problems in such a hierarchy can be avoided by an inheritance mechanism that propagates properties of nodes through the hierarchy.

From an operational perspective, GAIA-X envisages future “query algorithms on top of the Self-Description Graph”, including complex consistency checks that make sure, e.g., that “a Service Instance cannot depend on other Service Instances that are deployed on Nodes in a foreign jurisdiction”. While such use cases have not yet been considered for the IDS, it is the common Semantic Web and Linked Data foundation that enables the look-up of definitions and connected information on the fly while at the same time formulating machine-processable formal logic and extensive encoded knowledge in the form of ontologies. Mature specifications such as the LDP Recommendation mentioned in Section 0 and RFC 7231 standardize the underlying negotiation steps and are already a vital part of today’s Web.

GAIA-X itself currently still lacks the required rich semantic models, opening the opportunity of synergies based on the gained insights during the IDS Information Model developments and at the same time enabling the IDS to efficiently enrich its interactions classes with the competence brought together in the GAIA-X community.

Trust in Self-Descriptions

GAIA-X goes beyond the IDS in notion of trust in Self-Descriptions. In the IDS-RAM, trust in a Participant is established based on a multi-layered approach: The Participant has to pass a certification as a prerequisite for being admitted to the ecosystem of a particular data space (“static trust”). Certification also has to be undertaken for each type of IDS Connector. For both, different trust levels are defined. Participants can host multiple IDS Connector

¹³ This mechanism will be explained in the forthcoming version 4.0 of the IDS RAM and is also explained in Bader et al. (2020).

instances of different trust levels. For identity management, see section 0. IDS self-descriptions issued by a connector are *implicitly* assumed to be trustable. Depending on the trust profile, a set of the attributes can be explicitly verified. The identity of the participant is verified by the Identity Provider that issued the Connector certificates. The trust profile for higher trust levels can be verified using remote attestation of the software stack. Various identity attributes can be verified using the Dynamic Attribute Provisioning Service (DAPS), which is similarly envisaged in GAIA-X, and continuous Dynamic Trust Monitoring.

While the Identity and Certification mechanisms of GAIA-X build on similar foundations as those of the IDS, as discussed in Sections 0 and 0, there is an additional mechanism to establish trust in Self-Descriptions. While, like in the IDS, the Providers of a GAIA-X Asset are responsible for the *creation* of the respective Self-Description, trusted parties can establish trust by cryptographically *signing* sets of claim statements within Self-Descriptions, which they have verified.^{14,15}

Usage Control

Usage Control is an extension to traditional access control and supports data sovereignty by providing concepts to respect data usage restrictions and obligations after access to data has been granted. In the GAIA-X Technical Architecture paper, the IDS Usage Control concept is explicitly named as suitable approach.

Within the IDS, there are two main approaches to implement data sovereignty with data usage control: First, the specification of data usage restrictions and obligations as policies. Second, the technical enforcement of these specified policies. These approaches can be easily aligned to the demanded concepts for GAIA-X named "Specification of Usage Policies" and "Enforcement of Usage Policies".

Similar to GAIA-X, the IDS-RAM differentiates between technology-independent, human-readable policies that create a common understanding of data usage restrictions and obligations, and technology-dependent, machine-readable policies able to be directly processed by technologies enforcing data usage restrictions and obligations in a system. By choosing such an approach, the IDS prevent vendor lock-in, ensures interoperability and enables an open market for data sovereignty technologies.

The IDS offer currently fourteen main policy classes that are supported by the Information Model, further eight will be published soon. These IDS policy classes can be refined and transformed to technology-dependent, machine-readable policies and obtain an ensured relation to legally binding formulations. This may be, for example, a legal base such as the European judicial area.

Moreover, the IDS initiative shows the technical feasibility by offering a web-based policy editor supporting the specification and transformation of these fourteen policy classes and the enforcement by different technical implementations.

¹⁴ BMWI, GAIA-X: Technical Architecture, 2020:
https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=2

¹⁵ IDSA, IDS Reference Architecture Model 3.0, 2020:
<https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

Summarized, the IDS approach to support policy specification, including a technical toolchain and the maintenance in the information model, seems to be very similar to the demanded concepts in GAIA-X for the “Specification of Usage Policies”.

Regarding the “Enforcement of Usage Policies”, the IDS integrates usage control capabilities into their Connector implementations. In GAIA-X, this usage control capabilities can be integrated into GAIA-X Services.

It is important to note that the IDS differentiate between usage control capabilities at Data Provider side and usage control capabilities at Data Consumer side. For each side the usage control integration is solved in different ways: At Provider Side, a routing pattern controls and enforces usage restrictions and obligations on data flows. Contrary at the Consumer Side, an interceptor pattern ensures the control of the data flow. Another dimension to mention is that data usage restrictions and obligations can demand different mechanisms for enforcement. For example, the concepts for offering monitoring and notification capabilities differ from those about interactions with storage endpoints. The latter is very important when using external storages that are controlled by the usage control technology (i.e. the Connector in IDS) in order to obey the provided policies. For further details, we refer to the IDSA Position Paper about Usage Control in the IDS.

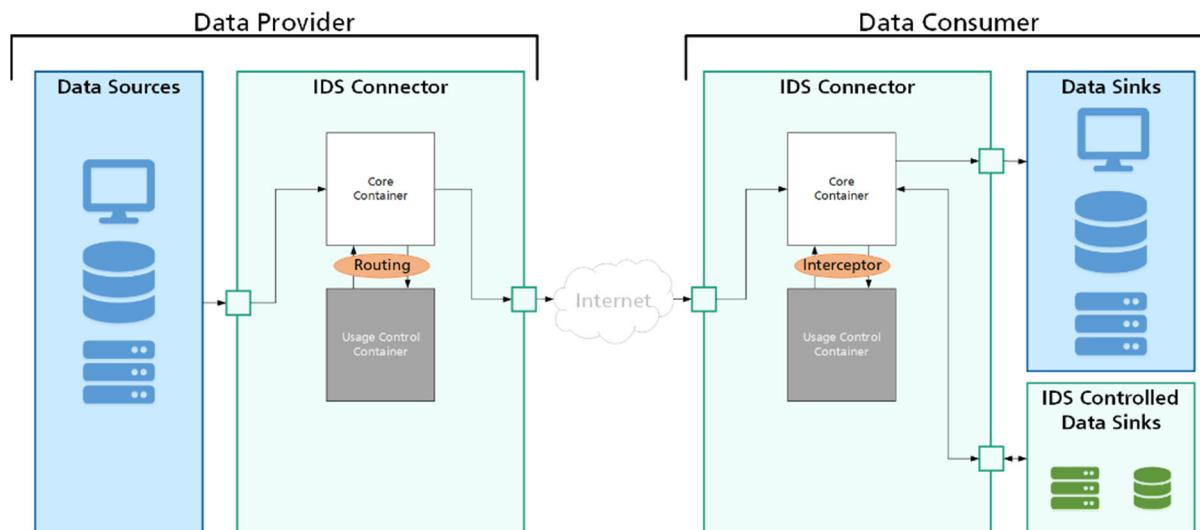


Figure 11 Usage Control in IDS (own visualization)

Finally, the IDS differentiate between data usage control and data provenance tracking. The former serves as proactive enforcement of usage restrictions and obligations at runtime, the latter serves as retrospective recording of data flows and usages to support, for instance, data traceability or auditing. To conclude, the demanded concepts of GAIA-X “Enforcement of Usage Policies” seem to be very closely aligned to the IDS usage control enforcement.

All usage restrictions and obligations should be enforced by technical measures, which also holds for GAIA-X. It is important to understand that the above mentioned fourteen classes of data usage restrictions and obligations are expressed as technology-independent policies. In cases where the technical enforcement cannot be guaranteed by the connector, the Data Provider may decide that organizational and legal measures are sufficient instead. Nevertheless, to technically implement a trustworthy usage control, it must be based on a

sound trust model and valid security requirements. IDS concepts enable this by defining trust profiles for connector implementations.^{16 17 18}

Trustworthy Runtime

The IDS as well as GAIA-X provide the possibility to extend their functionality by executing additional software (apps or services) to process data. For that purpose, IDS Connectors support the usage of IDS Apps while the GAIA-X Nodes can be used to run Service instances. While the wording is different, the technical implementation is quite similar: In both cases, the runtime provides an environment for a group of isolated processes with restricted I/O using Linux system calls. For compatibility the following aspects need to be standardized:

- What interfaces (API) does the runtime offer for apps or services?
- What security requirements must the technical implementation of the runtime fulfil?

API for the apps or services

The main purpose of the runtime is the execution of apps or services for processing data. Furthermore, it must support the following functionalities:

- Communication between its own apps or services and those on other trustworthy runtimes in the IDS or GAIA-X.
- Communication with external systems that provide, access or extract the data processed in the apps or services.
- Persistent storage of data.

In general, these functionalities must be available for apps or services on all systems in the IDS and GAIA-X, independent of the utilized hardware and implementation of the runtime. In other words, the trustworthy runtime should provide an abstraction layer with clearly defined APIs that can be used by all apps or services. In favour of the interoperability between systems, these APIs should be consistent for both IDS and GAIA-X to enable apps and services to be executable in both environments.

Security requirements for the runtime

In both cases, IDS and GAIA-X, data is considered to be a valuable asset and must be protected.

Therefore, IDS Connectors always implement a base set of security requirements. Security measures in the base profile include features for identity and access management, system integrity and data confidentiality. They are based on ISO/IEC 62443-4-2 and complemented with additional IDS-specific requirements as well as requirements for the development processes. For more advanced trust profiles, the IDS additionally require strict isolation of

¹⁶ BMWI, GAIA-X: Technical Architecture, 2020:
https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=2

¹⁷ IDSA, Usage Control in the International Data Spaces, 2019:
<https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Usage-Control-in-IDS.pdf>

¹⁸ IDSA, IDS Reference Architecture Model 3.0, 2020:
<https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

services, a reduced attack surface and support for (hardware) trust anchors. These requirements are the basis for the technical enforcement of usage control policies which is also a specified requirement for those connectors.

As explained in section 3.2, in the IDS the correct implementation of all these security requirements is verified during the evaluation of an independent third-party. The runtime's task in this context is the verification of the software signatures that result from a successful certification process as well as providing the required information for the remote attestation to communication partners. The reuse of those concepts and requirements is also of benefit for GAIA-X.

Different possibilities for implementing the runtime

A trustworthy runtime must implement all functionalities to fulfil the security requirements and to provide the API to the apps or services. In the IDS ecosystem, different types of devices must provide a trustworthy runtime. This includes embedded devices, edge devices, servers and cloud infrastructures. GAIA-X has the same scope. In the following, we describe two common concepts as they are used in the IDS:

In the first example the operator of the Connector has full control over the device. Typically, the system is secured by a secure boot process using a Dynamic Root of Trust for Measurement (DRTM) and code signatures for all parts of the Trusted Computing Base (TCB). This includes the boot loader, a Linux kernel and a base system image with common system services. Additionally, a hardware trust anchor including a secure key storage is typically utilized.

In the second example, the Connector is executed on a server or in a cloud infrastructure, where the operator of the Connector wants to execute its applications without giving the cloud provider access to the processed data (Confidential Computing). For this purpose, a Trusted Execution Environment (TEE) based on Intel SGX or AMD SEV can be used to protect the processed data.

Both concepts can equivalently be used in GAIA-X to securely run Services on a GAIA-X Node.¹⁹

¹⁹ BMWI, GAIA-X: Technical Architecture, 2020: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=2



Next Steps

Over the next months, a main event in the GAIA-X context is the formal establishment of the GAIA-X Foundation, where IDSA members will be formally established as members in various boards and committees.

The recent GAIA-X summit with its lively contributions and the great interest from the political, public and technology expert side proves the relevance of the initiative. The goals and next steps will be pursued vigorously, and concrete steps will be taken to meet the commitments made at the KickOff in June 2020. For example, the GAIA-X Federation services project was finally launched in November 2020 and is concerned with the specification and implementation of the first version of the Federation services. Representatives of the IDS initiative are involved in this Federation services project in order to contribute their existing expertise on sovereign data exchange and the IDS architecture. An alpha version of GAIA-X Federation services is expected to be available as open source solution in the third quarter of 2021. In order to create more transparency about IDS solutions and to support implementations, the technical specification of IDS-RAM elements called IDS-G will grow in the near future and be enriched with new content. In addition, the IDSA Rulebook will provide a description of the processes within the IDSA, including e.g. operational aspects, certification procedures or legal aspects. Furthermore, aspects of traceability, monitoring and metering as well as the IDS Clearing House are not yet pronounced sufficiently in the discussion of GAIA-X and IDS, but represent a part for subsequent activities to this paper. Also, the lifecycles of different elements are to be considered.

In the near future, the GAIA-X AISBL will be opened to new members as Day2 entries. In addition, a technical summit, the GAIA-X Conference, will provide an insight into the technical side of GAIA-X and will go into details. The new edition of the technical architecture document, which provides a basis for all technical considerations and is of great value for the elaboration of a technical adaptation to other initiatives and ecosystems, is scheduled to be published in March 2021. In addition, the Architecture of Standards document will also be published at that time. These documents will provide the basis for further joint development of the IDS initiative and GAIA-X to work towards the shared vision of sovereign digital ecosystems.

Until then, first architectural decisions are discussed recently and fixed to refine the existing Technical Architecture paper. Meanwhile, as the GAIA-X initiative evolves, the IDS concepts are further introduced and proliferated in the GAIA-X community.

As GAIA-X gets more and more concrete over time, the IDS-RAM adds up to the GAIA-X architecture by providing existing solutions, which fulfils the claim of GAIA-X to be an architecture of existing standards and to leverage existing technologies and concepts. Nevertheless, GAIA-X also presents an opportunity for IDS to connect to a broad community and share the common vision and goals of a sovereign data ecosystem, which may also stimulate the development of IDS components and opens up new perspectives.

References

Sebastian Bader, Jaroslav Pullmann, Christian Mader, Sebastian Tramp, Christoph Quix, Andreas W. Müller, Haydar Akyürek, Matthias Böckmann, Benedikt T. Imbusch, Johannes Lipp, Sandra Geisler, Christoph Lange. **The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content.** International Semantic Web Conference (ISWC) 2020.

BMW, 2020, **GAIA-X: Driver of digital innovation in Europe:** <https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-a-pitch-towards-europe.html>

BMW, 2020, **GAIA-X: Technical Architecture:** https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=2

DIN SPEC 27070, 2020, Anforderungen und Referenzarchitektur eines Security Gateways zum Austausch von Industriedaten und Diensten: <https://www.din.de/de/wdc-beuth:din21:319111044>

European Commission, 2014, **Trust Services and Electronic identification:** <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

European Commission, 2020: **The European Data Strategy:** https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

Fraunhofer, 2020, **International Data Spaces Software:** <https://www.dataspaces.fraunhofer.de/de/software.html>

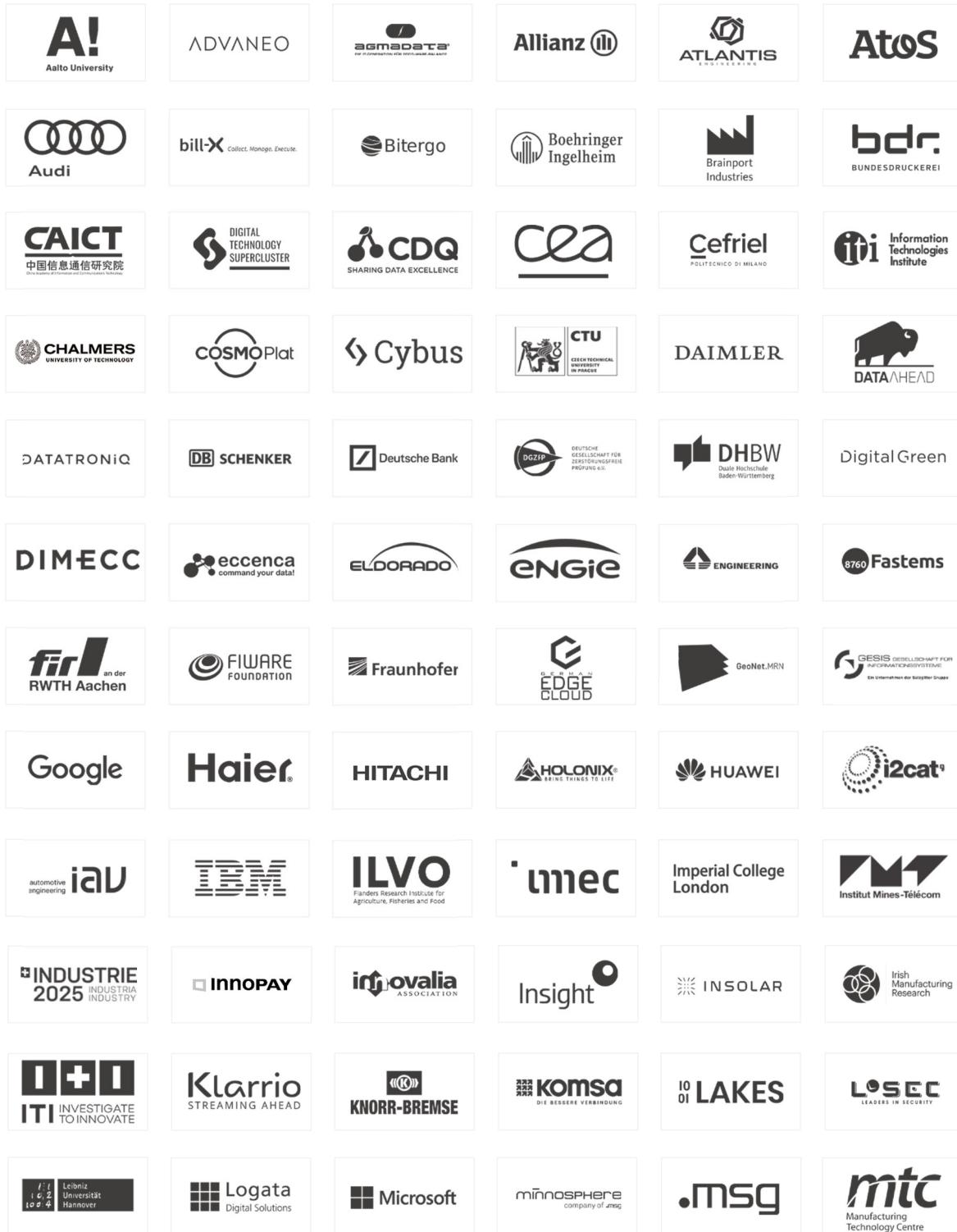
IDSA, 2019, **IDS Certification explained:** <https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-IDS-Certification-Explained.pdf>

IDSA, 2020, **IDS Reference Architecture Model 3.0:** <https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf>

IDSA, 2019, **Position Paper Usage Control in IDS 2.0:** <https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Usage-Control-in-IDS.pdf>

W3C, 2015, **Linked Data Platform:** <https://www.w3.org/TR/ldp/>

OUR MEMBERS





OVERVIEW PUBLICATIONS



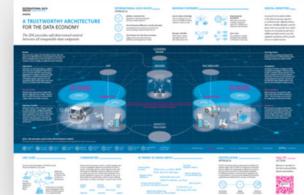
Reference
Architecture Model



Executive
Summary



Image Brochure



Infographic



Use Case
Brochures



Study on Data Exchange



Position Paper
Implementing
the European
Data Strategy



Position Paper
GDPR Requi-
ments and Rec-
ommendations



Position Paper
Usage Control
in the IDS



Position Paper
IDS Certifica-
tion Explained



White Paper
Certification



Sharing data while
keeping data
ownership



Magazine Data Spaces_Now!

For these and further downloads: www.internationaldataspaces.org/info-package

Code available at: <https://github.com/industrial-data-space>

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

 [@ids_association](https://twitter.com/ids_association)

 [international-data-spaces-association](https://www.linkedin.com/company/international-data-spaces-association/)