INTERNATIONAL DATA SPACES ASSOCIATION

INTERNATIONAL DATA SPACES
FACT SHEET AND CORE STATEMENTS

Version 1.0 | August 2019

STRATEGIC POSITIONING

- Objective: The objective of the International Data Spaces Association (IDSA) is to establish a standard for data sovereignty – for the trustworthy, self-determined exchange of data.
- Values: The specification of the IDSA forms the basis for data ecosystems and marketplaces based on European values, i.e. data protection and security, equality of opportunities, through a federated design, through ensuring data sovereignty for the data originator and through trust between the participants.
- International Data Spaces Association: The IDSA is a charitable, not-for-profit organization. All members have the same rights to use the results. The adoption of the IDS idea in the market takes place in three stages:
  1) Research to solve previously unresolved questions (Fraunhofer, TNO, vtt, etc.);
  2) Consensus building on architecture, implementation options and standardization in the Association's committees;
  3) Transfer of concepts from the association's work into marketable products and services by companies from the association and outside.

  IDSA is currently on the threshold from 2) to 3).
- International: IDS is an international initiative. The IDSA has 100 members from 19 countries (European Union plus Brazil, Canada, China, India, Japan, United States) and formal cooperation with international initiatives (Platform Industrie 4.0, IIC, IVI, DTA, RRI, OPC-F, Fiware, DMA, iShare).
- Data sovereignty: With the concept of data sovereignty, IDS makes an important contribution to digital infrastructures and thus provides an answer to market-inhibiting effects of data economics in general, especially for the Industrial IoT, for AI and any kind of Smart Service Scenarios. IDS provides the ability to describe, trade and protect the central object of these ecosystems: the asset data. There is currently no global standard for this.
- IDS and European Union: IDS is part of the strategy of the European Commission on the Strategic Value Chain of the Industrial IoT as well as of the "Digitizing European Industry (DEI)" strategy of the European Commission.
- IDS and GAIA: The preliminary work of the IDS is of added value for GAIA and should definitely be taken up, as it directly contributes to GAIA's goals and thus significantly shortens the time to market for GAIA. On the way to a flourishing data economy, however, many challenges still need to be consistently addressed by GAIA.
- IDS and AI: With the concept of data sovereignty, IDS provides the basis for successful artificial intelligence by making considerably more data sources accessible.

GENERAL CONCEPT

- IDS provides a reference architecture, a formal standard and reference implementations including the sample code.
- IDS is a concept analogous to the internet based on peer-to-peer communication, but not a platform.
- Internal/external: IDS addresses ecosystems and corporate networks. Use cases within a factory or firewall do not require IDS.
- Certification: The certification concept confirms the conformity of components (connectors) and organizations to the IDS architecture by independent organizations (PwC, TÜV, Fraunhofer). This ensures that the organizations have taken all necessary measures for an IDS-compliant operating environment and also use components that have been implemented according to the connector variant.

CONNECTOR AND IMPLEMENTATION

- IDS connector: The IDS connector acts as a gateway. It can be implemented in different ways depending on the scenario: on microcontrollers, sensors, mobile devices, on servers, in the cloud. Due to the container architecture, the IDS connector also allows trusted execution of apps – those that can sovereignly process data from different sources. These software services will not run in an ERP system behind the firewall, but on cloud platforms, i.e. "in the center" of ecosystems. The connector is therefore a suitable execution component for Amazon Web Services (AWS), Data Intelligence Hub (DIH), SAP HANA, etc., because it enables the platforms to offer a secure environment in which data sovereignty is

guaranteed. Domain-specific application profiles enable embedding in specialist domains with different requirements (see DIN SPEC 27070).

- Connector variants: Companies can choose between four connector variants, depending on the usage scenario and scope of the protection requirements: Basefree, Base, Trusted, Trust+. The "base" profile meets basic security requirements for communication across company boundaries. A connector that has been certified according to the "trust" profile provides additional security features such as strict isolation of the service containers and mutual verification of integrity. A "trust+" profile connector even provides protection against manipulation by administrators.
- Implementation and products: Companies develop market-ready solutions (commercial and non-commercial) and make them available to the market through their own business models. The product must be certified to be interoperable with other IDS connectors. IDSA is a not-for-profit organization and has no intention to make profit.
- Plugfest and developers community: All these things are implemented in the "plugfest", where all developers (research institutions and companies) meet every 3 months at the "IDS Lab" in Dortmund. There are currently implementations of connector variants from 15 companies and research institutions as well as from the services broker, appstore, clearing house, identity management and vocabulary provider. There is a development roadmap, which will be implemented by the developers community during the plugfests. Usable code is available on the association's internal collaboration platform (only accessible to association members) as well as parts of it in git repositories of association members.

CONTENT CONCEPT

- Semantics: IDS standardizes the semantics of data exchange. IDS provides the semantics for the IDS architecture in the shape of an information model, it describes, for example, what a broker, a connector, data goods, data givers are, etc. IDS also provides the semantics for the IDS architecture in the form of an information model. In addition, IDS suggests semantics for data usage conditions (data may be used, read, three times; data may not be forwarded, but only for a fee, etc.). IDS does not define technical or domain-specific semantics. So IDS does not say which features describe a screwing robot etc. or what an "industry 4.0 thing" looks like – this is done by the asset administration shell (AAS), whose instantiated data can then be provided with terms of use via IDS before it is exchanged via an IDS connector.
- IDS and EDI: IDS does not replace electronic data interchange (EDI). EDIFACT messages for invoices, delivery schedules, etc. will still be available in many years. But EDI does not standardize terms of use.
- IDS and standardized terms of use: No standard realizes that yet. IDSA currently specifies 14 classes for terms of use, which are also transferred to the World Wide Web Consortium via the working group on Open Digital Rights Language (ODRL).
- Data ecosystems: IDS is made for ecosystems because this is where innovation takes place. From the perspective of an ecosystem member, ecosystems need their own data, data from "friends and family" (familiar, long-standing, etc.) and context data (weather, traffic, etc.), often public data.
- Policy enforcement: Not only to describe data sovereignty in a declarative way and thus to make it interpretable for a computer (which is already an important step), but to be able to technically enforce data sovereignty (enforcement), is a central point of the whole IDS initiative. IDSA pursues various technology development strands (which already existed before IDS was established and which are independent concepts in themselves), including distributed usage control, data provenance tracking and sticky policies.
- IDS and cloud: For the integration of IDS components into a modern cloud platform such as DIH, AWS, etc., we need an architecture image that, as a reference model, shows typical components (including the connector, see above)

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund | Germany

phone: +49 231 9743 619
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association