INTERNATIONAL DATA SPACES ASSOCIATION

International Data Spaces

Enabling Data Economy

Why

Data sovereignty: Assigning binding usage restrictions to data; establishing a concept and components for a secure and trusted data infrastructure

The International Data Spaces Association (IDSA) has defined a reference architecture and a formal standard to be used for creating and operating virtual data spaces. The IDS Architecture is based on commonly accepted data governance models facilitating secure exchange and easy linkage of data within business ecosystems.

The IDS Architecture ensures digital sovereignty for data owners making data available for being exchanged or shared. It thereby constitutes the basis for developing and offering smart services and for establishing innovative business processes.

The IDS initiative aims at creating secure and trusted data spaces, in which companies of any size and from any industry can manage their data assets in a sovereign fashion. It addresses companies and other organizations from across Europe and beyond. IDSA already counts over 130 member organizations from more than twenty countries.

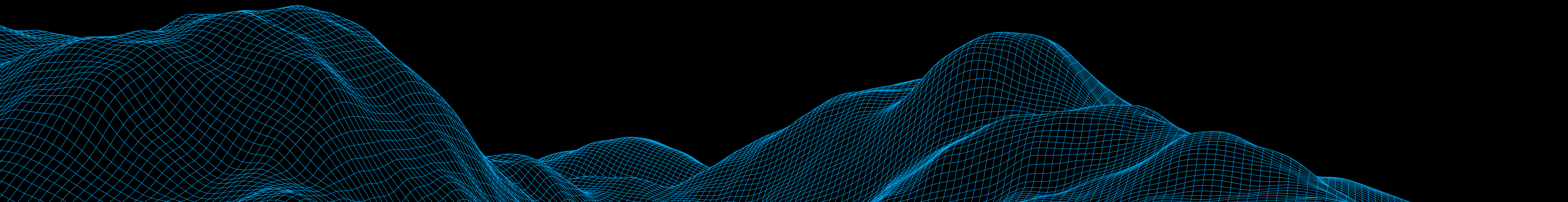
Data is the raw material for innovation. This is particularly true for three major areas that are of paramount importance in today’s digitalized world: artificial intelligence (AI), the internet of things (IoT), and big data. For data to unfold its full potential, it must be made available in cross-company, cross-industry business ecosystems.

Data value chains range from capturing data by means of sensors to preprocessing, storing, and transferring data to eventually data analysis, data processing, and data usage. The existence of data value chains is a necessary precondition for achieving innovation within business ecosystems.

Data sovereignty in IDS presupposes metadata attached to data, which unambiguously defines data usage policies at each level of the data value chain. Enforcing data sovereignty requires an appropriate technical infrastructure that facilitates contractual agreements on the use of data, such as allowing (or disallowing) the processing, linkage or analysis of data by data users, or allowing (or disallowing) third parties access to data. If need be, data sovereignty is ensured also within third parties’ digital infrastructures (e.g. networks, clouds, or software components).

IDS Connector – the gateway software component of a technology made in Europe

To incentivize data sharing among organizations and individuals across countries, a trustworthy technology is needed. This technology must ensure data sovereignty across different industries and on a non-competitive basis by means of appropriate digital infrastructure components and a standard, interoperable format.



The IDS initiative has developed a software architecture that ensures data sovereignty by facilitating the secure exchange of data between trusted parties. Certified participants are granted access to the data ecosystem, in which they can attach usage policies to their data before they make it available to other participants. This is made possible by a dedicated software component, the IDS Connector, which can be installed on a server, in a cloud, on an IoT device, on a smartphone. The IDS Connector can act as a gateway for data and services and is in addition a trusted environment for the execution of individual software components.

This way, data is generated decentrally, before it can be exchanged based on the IDS architectural concepts, if necessary stored in any kind of cloud (public, private, etc.), and processed in line with data usage policies specified. The IDS Connector uses containerization technology ensuring "trusted execution"; i.e. data inside the container is protected against unauthorized access and manipulation, and can be used only as agreed upon by the parties involved.

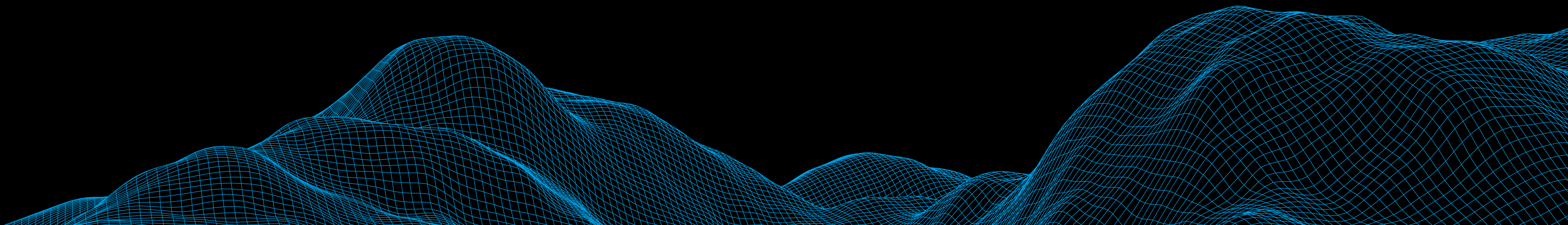
Using a soft infrastructure to enforce data sovereignty

A soft infrastructure constitutes the basis for ensuring data sovereignty in the first place. Such an infrastructure must be equipped with 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 IDS features (such as a metadata-broker service provider or functions for data quality assessment), that make a data ecosystem based on data sovereignty valuable for its users. Therefore, the overall goal of IDSA is to design and develop a secure and trusted digital infrastructure that relies on basic European values.

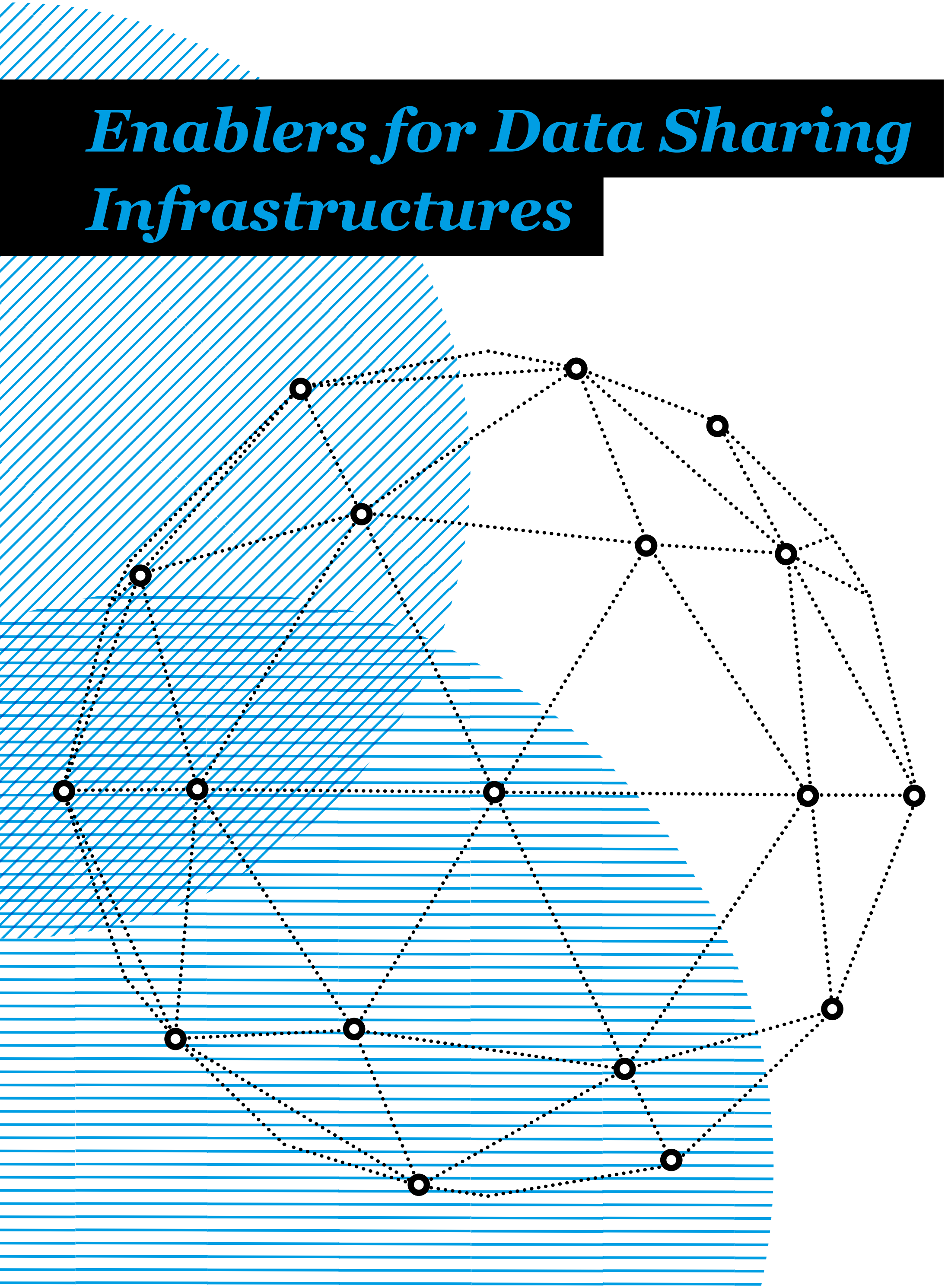
Digital platforms as data ecosystems

Whether we speak of business, politics, the media, or society – digital platforms have become an indispensable element in today's digitalized world. These platforms provide access to products, services, digital content, information, and data for everybody. When it comes to bringing supply and demand together as efficiently as possible, digital platforms clearly outmatch traditional business models. They have evolved from technical instruments to complex ecosystems. Digital platforms can create new markets, and stimulate existing ones. Across highly fragmented markets, they can bring together people or companies who otherwise would never have gotten in contact with one another. In short: Digital platforms bear enormous potential and countless opportunities.

Digital platforms; applications in the fields of AI, IoT, or big data; projects such as GAIA-X or AI4EU – all these application areas and endeavors are inconceivable without IDS. IDS will significantly contribute to their success. IDS is an open standard for facilitating secure and trusted data sharing to connect those platforms in an accepted and standardized manner that is guided by the principles of data sovereignty. IDS should be integrated as an inherent component in future architecture models of the data economy.



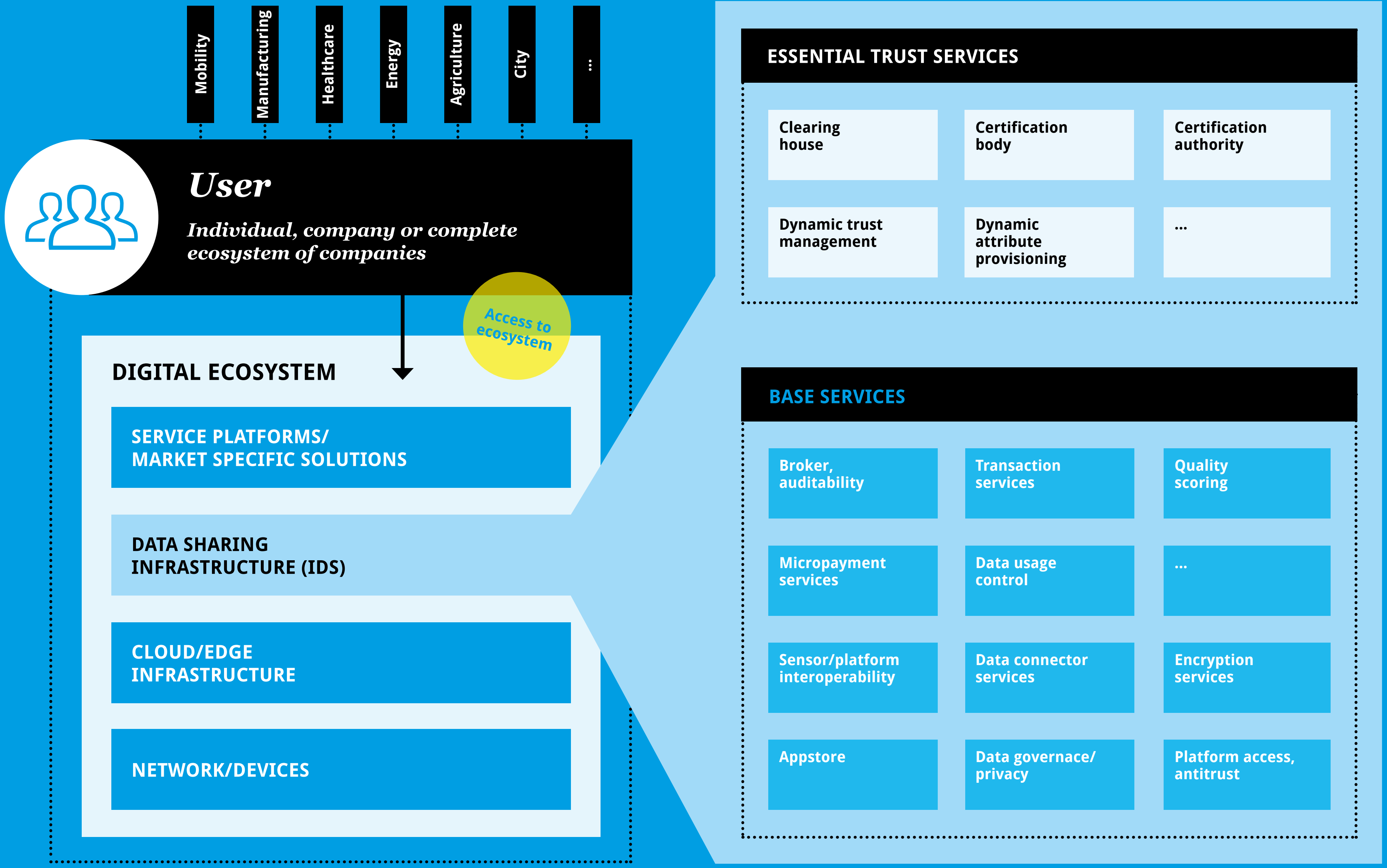
Enablers for Data Sharing Infrastructures



With the IDS Architecture, the International Data Spaces Association is setting a standard for data sharing on a trustworthy and self-determined basis – a standard for data sovereignty.

The IDS standard is critical for establishing data ecosystems and data marketplaces. The standard guarantees data security and data protection for all parties involved, establishes mutual trust among them, ensures a level playing field by means of a jointly developed and commonly accepted design, and enforces data sovereignty for all data owners. It enables trading data on the basis of ethical principles and common European values.

The IDS standard is an enabler of markets to unfold. To leverage the full value adding potential of data, data must be describable and tradeable with the help of a global, interoperable standard. Such a standard has not been in place so far. IDS is such a global, interoperable standard. IDSA counts over 130 member organizations from 22 countries all across the world. These organizations are both private enterprises and not-for-profit research institutes. They have formed industry-specific communities and cross-industry working groups, in which they have developed information models and governance models constituting the basis of the IDS Architecture.



Mobility

Manufacturing

Healthcare

Energy

Agriculture

City

...

User

Individual, company or complete ecosystem of companies

Access to ecosystem

DIGITAL ECOSYSTEM

SERVICE PLATFORMS/ MARKET SPECIFIC SOLUTIONS

DATA SHARING INFRASTRUCTURE (IDS)

CLOUD/EDGE INFRASTRUCTURE

NETWORK/DEVICES

ESSENTIAL TRUST SERVICES

Clearing house	Certification body	Certification authority
Dynamic trust management	Dynamic attribute provisioning	...

BASE SERVICES

Broker, auditability	Transaction services	Quality scoring
Micropayment services	Data usage control	...
Sensor/platform interoperability	Data connector services	Encryption services
Appstore	Data governace/ privacy	Platform access, antitrust

Evolution

An initiative resulting in a formal standard

Combined with a supranational, standardized cloud system, IDS, being an international standard for data sovereignty, would create a key element for a Europe-wide digital infrastructure. This digital infrastructure must be built up now.

The IDS Architecture and the formal norm DIN SPEC 27070 are ready to use. All necessary development and testing activities have been finalized.

The IDS initiative was brought to life by business, politics, and research in a joint effort. The goal of this initiative – to design, develop, test and establish a reference architecture for creating a secure data space and facilitating secure and trustworthy data exchange – has been accomplished. The IDS Reference Architecture Model (IDS-RAM) is based on findings gained from extensive benchmarking and requirements analyses. Research and development activities were mainly conducted in Fraunhofer-led research projects funded by the German Federal Ministry of Education and Research, in application projects that were funded by the German Federal Ministry for Economic Affairs and Energy and in research projects funded by the European Commission. Over fifty use cases have been implemented by companies from different industries, from which a few products have resulted already.

IDSA collects and bundles the interests and requirements of its member organizations from business and research. To identify, analyze and evaluate the various kinds of requirements to be met by the IDS reference architecture, IDSA members have established cross-industry working groups as well as industry-specific communities. These efforts have led to “IDS_ready“, the certification scheme granting also companies outside IDSA access to IDS. IDS_ready certified participants and components thereby are entitled to take part in secure, IDS-based data value chain processes.

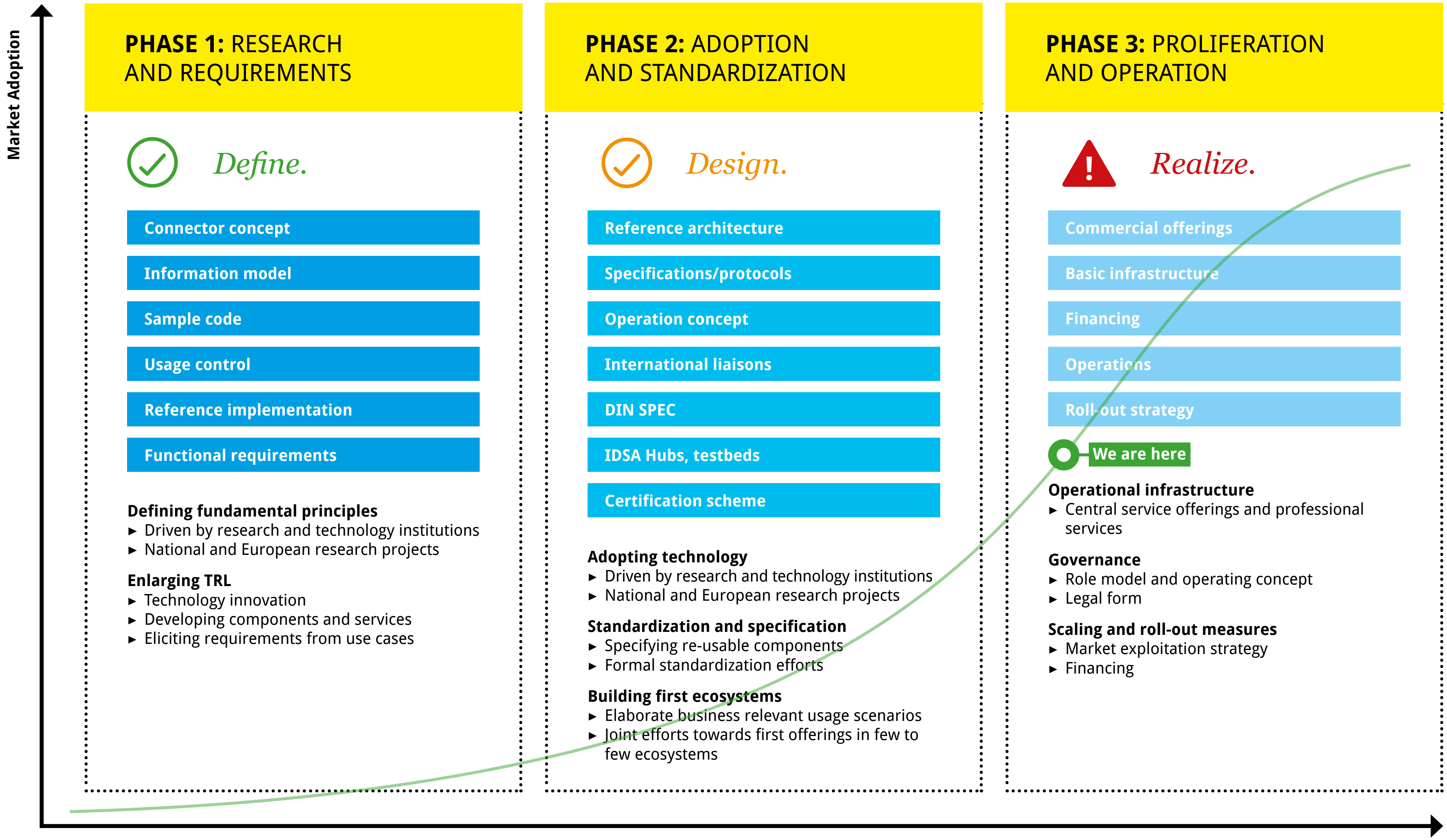
Meanwhile, parts of the current version of the IDS reference architecture (version 3.0) have become a formal norm: DIN SPEC 27070. IDS reference instantiations and sample code is available for software developers and can be tested within testbeds. Official IDSA Hubs have been established in seven countries, promoting the idea of standardization and adoption of IDS. Many companies and multipliers are working on concepts for operating secure and trustworthy infrastructures for data exchange.

IDSA reaches out globally. Member organizations come from all across the world. IDSA collaborates closely with cognate initiatives and associations (see box).
To make the IDS Architecture and the IDS standard central elements of a European digitalization strategy, IDSA contributes to a number of R&D projects funded by the European Commission.

Liaisons and cognate initiatives:

- Big Data Value Association
- Data Market Austria
- Data Trading Alliance
- eCl@ss
- Fiware Foundation
- Industrial Internet Consortium
- Industrial Value Chain Initiative
- iShare
- OPC Foundation
- Plattform Industrie 4.0
- Robot Revolution Initiative

Achievements and future challenges



PHASE 1: RESEARCH AND REQUIREMENTS

✓ *Define.*

- Connector concept
- Information model
- Sample code
- Usage control
- Reference implementation
- Functional requirements

Defining fundamental principles
- Driven by research and technology institutions
- National and European research projects

Enlarging TRL
- Technology innovation
- Developing components and services
- Eliciting requirements from use cases

PHASE 2: ADOPTION AND STANDARDIZATION

✓ *Design.*

- Reference architecture
- Specifications/protocols
- Operation concept
- International liaisons
- DIN SPEC
- IDSA Hubs, testbeds
- Certification scheme

Adopting technology
- Driven by research and technology institutions
- National and European research projects

Standardization and specification
- Specifying re-usable components
- Formal standardization efforts

Building first ecosystems
- Elaborate business relevant usage scenarios
- Joint efforts towards first offerings in few to few ecosystems

PHASE 3: PROLIFERATION AND OPERATION

⚠ *Realize.*

- Commercial offerings
- Basic infrastructure
- Financing
- Operations
- Roll-out strategy

Operational infrastructure
- Central service offerings and professional services

Governance
- Role model and operating concept
- Legal form

Scaling and roll-out measures
- Market exploitation strategy
- Financing

Facts and Statements

Strategic Positioning

- **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, but also 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.

- **Objective:** The International Data Spaces is establishing a standard for data sovereignty – for the trustworthy, self-determined exchange of data.

- **Values:** The specification of the International Data Spaces Association 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:** IDSA is an international initiative. The IDSA has 130+ members from 20+ countries (European Union plus Brazil, Canada, China, India, Japan, United States) and formal cooperation with international initiatives (Plattform 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 strategy of the Digitizing European Industry (DEI).

- **IDS and GAIA-X:** The preliminary work of the IDS is of added value for GAIA-X and has been taken up as direct contribution to GAIA-X's goals and will significantly shorten the time to market for GAIA-X. On the way to a flourishing data economy, however, many challenges still need to be consistently addressed by GAIA-X.

- **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 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 micro-controllers, sensors, mobile devices, on servers, in the cloud. Due to the container architecture, the IDS Connector also allows trusted execution of apps – those that sovereignly analyze 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), Digital Innovation Hubs (DIH), SAP HANA, etc., because it enables the platforms to offer a secure environment in which data sovereignty is maintained. 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 administration tray, 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. IDS 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 groups:** 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 that, as a reference model, shows typical components (including the connector, see above).

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

HEAD OFFICE:
International Data Spaces Association
Emil-Figge-Str. 80
44227 Dortmund
Germany

Phone: +49 (0) 231 70096 501
info@internationaldataspaces.org

@ids_assosiation

international-data-spaces-association

www.internationaldataspaces.org