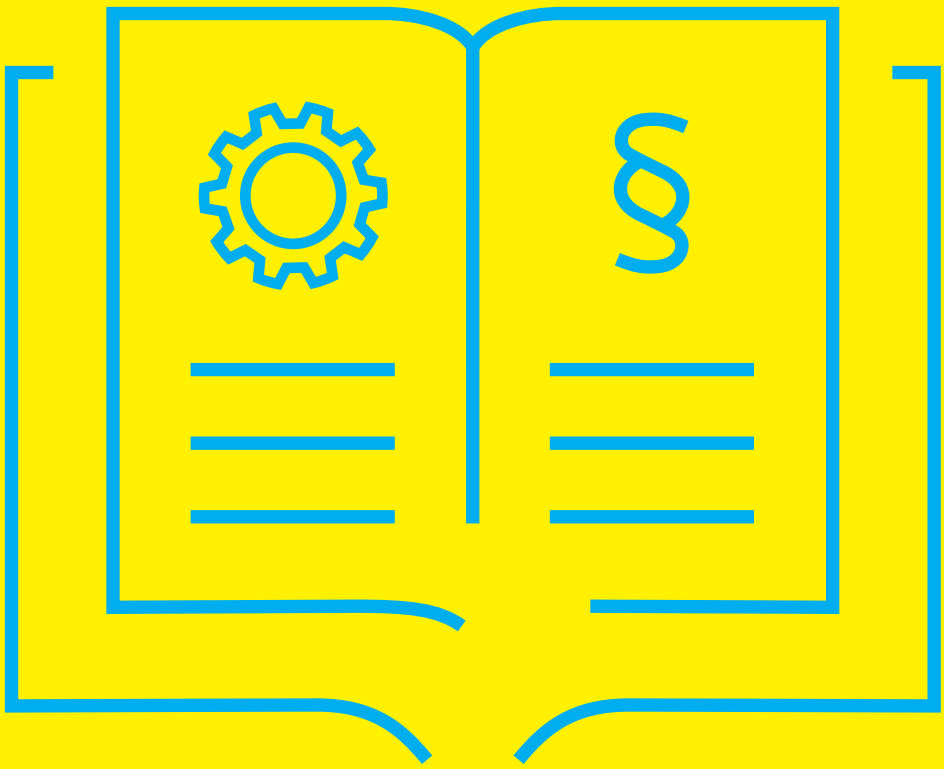
INTERNATIONAL DATA SPACES ASSOCIATION

White Paper | Version 1.0 | December 2020

IDSA Rule Book



- ○ 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

Editor

Sebastian Steinbuss
International Data Spaces Association

Authors & Contributors

Alberto Berreteaga Barbero, Tecnalia
Alexander Duisberg, Bird&Bird
André Nemat, idigiT
Andreas Hoffmann, Fraunhofer FOKUS
Andrea Panzer-Heemeier, Arqis
Angelo Marguglio, Engineering
Anne Immonen, VTT
Aram Wiencke, German Edge Cloud
Bernd Fondermann, German Edge Cloud
Bernt Corneliussen, Orbiter
Charlotte Duicuing, KU Leuven
Christoph Schlueter Langdon, Deutsche Telekom AG Constantin Abate, T-Systems
Cristina Brandtstetter, FIWARE
Dan Negrea, SICK
Daniel Hommen, Orbiter
Dennis Oliver Kubitza, Fraunhofer IAIS
Denys Shportenko, SQS
Emre Bayamlioglu, KU Leuven
Erkuden Rios, Tecnalia
Felix Beckwermert, Atos Germany
Gabriele de Luca, Engineering
Gerd Brost, Fraunhofer AISEC
Gernot Boege, FIWARE
Guillermo Amat, ITI
Hannes Bauer, Orbiter
Heinrich Pettenpohl, Fraunhofer ISST
Ibon Arechalde, Tecnalia
Ilkka Niskanen, VTT
Jani Koskinen, Sitra
Jesús Alonso, Innovalia
Jörg Langkau, nicos AG
Jose I. Hormaeche, Energy Cluster
Joshua Gelhaar, Fraunhofer ISST
Julie Baloup, KU Leuven
Kari Hiekkanen, Sitra
Karsten Schweichhart, Deutsche Telekom AG
Klaus Ottradovetz, Atos Germany
Luis Usatorre, Tecnalia

Cite as

Steinbuss S., Ottradovetz K., Langkau J., Punter M. et al. (2021) IDSA Rule Book. International Data Spaces Association.
https://doi.org/10.5281/zenodo.5658294

Maarten Kollenstart, TNO
Marc Torrent, Eurecat
Mario Wolf, SICK
Marion Jost, Fraunhofer FOKUS
Marius Schmidt, German Edge Cloud
Marko Turpeinen, 1001 Lakes
Markus Ketterl, MSG
Marnix Vermaas, Visma Connect/iSHARE
Marta Castro, Tecnalia
Martin Böhmer, Fraunhofer IML
Matthias Böckmann, Fraunhofer IAIS
Matthias Rebmann, SICK
Matthijs Punter, TNO
Meri Seistola, Sitra
Michael Fritz, Fraunhofer ZV
Mike de Roode, TNO
Mikko Sierla, Vastuu Group
Monika Huber, Fraunhofer AISEC
Murua Bela Cortu, Tecnalia
Naiara Elejalde Innovalia
Olivier Wasmeier, SICK
Olli Pitkanen, 1001 Lakes
Pekka Mäkelä, Sitra
Peter Sorowka, Cybus
Philip Kempermann, Heuking
Richard Stevens, IDC
Sarah Becker, idigiT
Sascha Hackel, Fraunhofer FOKUS
Sebastian Bader, Fraunhofer IAIS
Sebastian Steinbuss, IDSA
Sebastian Fandrich, SICK
Simon Dalmolen, TNO
Thomas Krebs, Deutsche Telekom AG
Till Riedel, KIT TECO
Tobias Neufeld, Arqis
Ulrich Ahle, FIWARE
Werner Jost, T-Systems
Xabier Yurrebaso Asua, Tecnalia
Olatz Mediavilla, SQS

Table of Content

List of figures

1 Introduction

1.1 Who should read this rule book?

It is all about data. If your business has anything to do with generating or exchanging data or building/using data-driven ecosystems and business models, you should be thinking about data sovereignty. This book is for you.

This rulebook addresses:

- Peer-to-peer data sharing
- Data sharing ecosystems
- Data marketplaces
- Data-driven platforms
- Data-driven business models
- GAIA-X participants

1.2 Goals and scope

1.2.1 Goals of the IDSA

The IDSA aims to unlock the data economy of the future by providing the blueprint for secure, self-determined data exchange among trusted partners. This is what's referred to as "data sovereignty," and it is vitally important, in light of the fact that data access and exchange are rapidly becoming critical success factors for both companies and entire economies.

Until now, companies have held vast amounts of valuable data that they have been unable to control, share or monetize on their own terms. The IDSA has defined a reference architecture and a set of agreements that can be used to create virtual data spaces which establish trust among partners and a basis for innovative, new business models, products and services.

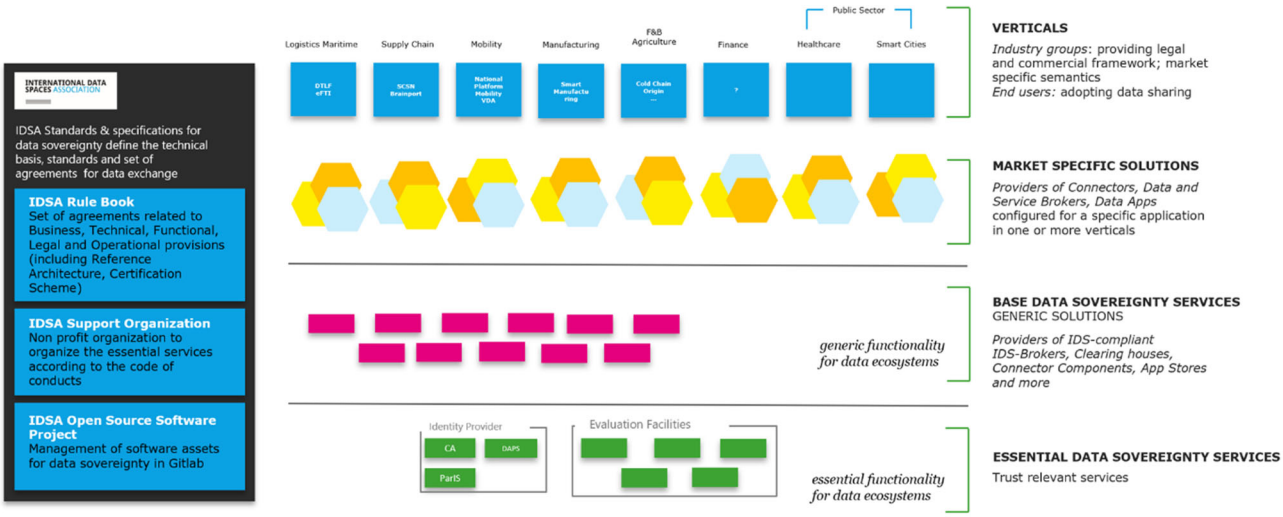


Figure 1 Overview IDS enabled ecosystems

The IDS protocol is based on commonly accepted data governance models so that it can facilitate secure data exchange and easy linkage across disparate systems, industries and geographies.

1.2.2 The purpose and scope of the rule book

In order for the future data economy to function smoothly and deliver on its value proposition, all players need to abide by a common governance framework that specifies the functional, technical, operational and legal agreements that structure their roles and interactions within and across the various parts of the ecosystem. This book outlines that framework.

By following these rules and guidance, all players can work together to reach our shared goal of unlocking the full value of the global data economy. For the purposes of this book, the key roles in the IDS ecosystem are as follows:

1. **The IDSA Support Organization**: Responsible for maintaining the rule book and for supporting its application. The IDSA support organization helps coordinate key processes and as general governance instance a foundation for the realization of internal structures and interfaces to other parties.

2. **The essential service providers**: Responsible for providing the essential services needed by all participants. They build the source of common agreements.

3. **All users of IDS:** Users will need guidance on how to proceed within this framework to realize use cases on the foundation of a trustworthy infrastructure and governance.

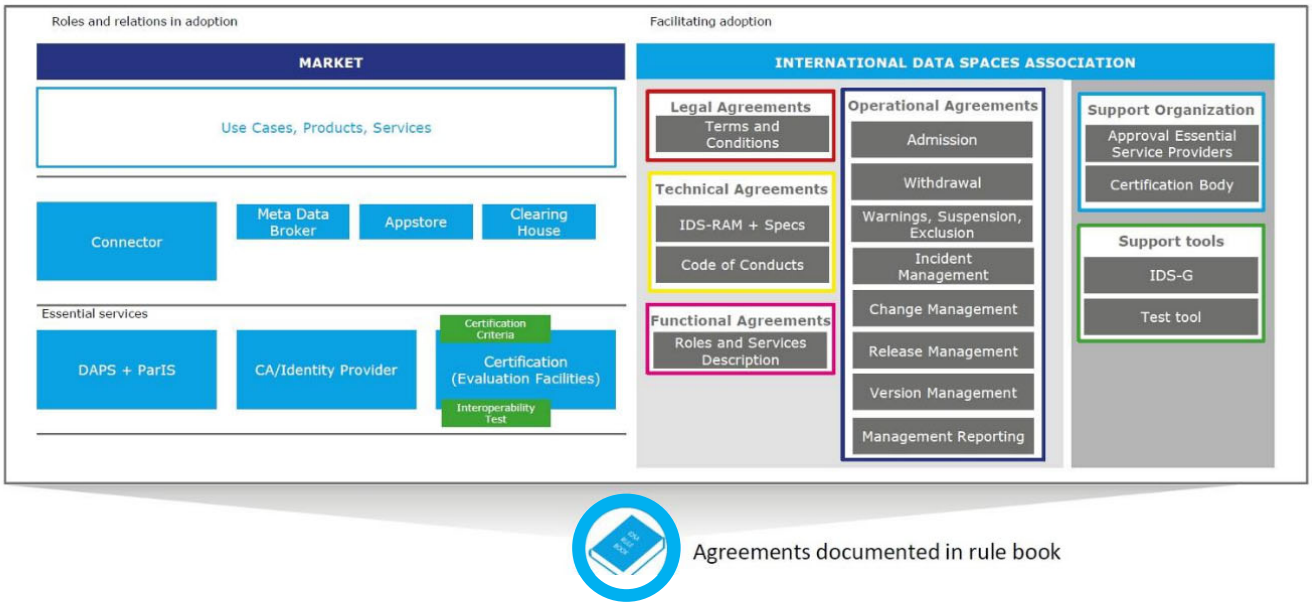


Figure 2 Overview Rule Book scope and goals

1.2.2.1 Scope in detail

The IDSA rule book defines structures and processes for implementing the IDS-Reference Architecture Model in the real world. This includes putting essential services in place as well as defining key processes, such as admission and withdrawal of participants.

Our approach to data sovereignty is not industry specific. It is applicable to all sectors. Therefore, sector-specific rules are not described in this book. All of these rules and guidelines can be applied in and across all industries and sectors. IDS is a horizontal approach, enabling data sovereignty to propagate throughout the digital economy.

This document covers:

1. **Functional agreements**: Guidance on functionality of common services as well as definition, processes and services of dedicated roles

2. **Technical agreements**: Everything you need to know to implement or use a technical artefact of the IDSA world.

4. **Operational agreements**: Everything you need to know to run and collaborate (technically) within data sovereignty services.

5. **Legal agreements**: The legal agreements governing data exchange are a critical success factor, so this has been an important focus: what legal environment is valid, what legal boundaries can be set, and what laws provide the right framework to benefit the data economy. This book provides guidance on on how organizations may define the rules and legal agreements for trustworthy collaboration.

6**. Commercial assumptions:** This rule book enables several different business models, rather than favoring one particular one. Commercial agreements are not part of the rule book, but we make some commercial assumptions regarding essential services (low profit), base services (enabling functionality, and higher-profit services on top of that. Commercial agreements will be discussed separately.

7. **Liaisons agreements**: The IDS-based data sovereignty community naturally collaborates with other ecosystems like ENX or certifications in automotive, Plattform Industrie4.0, GAIA-X etc. Liaisons agreements are about guiding principles guard-railing for these collaborations. IDSA provides processes and measures to actively contribute to liaisons and to provide value for the IDSA Liaison partners.

1.3 How to use IDS Competitive Advantage with Data Sovereignty

It is possible now to implement IDS based frameworks, services and offerings and start using the benefits of trusted data sovereignty for your business or your own offerings. The way you do this depends on the role you are going to play in the dedicated, data-driven continuum.

Overall, there are some rules and guidelines in common:

- Life cycle is defined: There is a common definition on life cycle agreements for IDS based assets, e.g., the IDS standards and services. See section “Operational Agreements, Life Cycle”.

- Processes: There are some common definitions of necessary processes for development, certification, onboarding, operation, usage and the like. See section "Operational Agreements. Processes"

Typical roles anticipated in an IDS based data driven continuum are described in more detail in a following chapter. Included are data provider and data owner, data consumer, data user, meta data broker, software, service and app provider, appstore provider, and basic roles like ID provider, certification provider, clearing house and vocabulary provider.

Furthermore, there will be some papers on examples of use cases and business models addressing the different roles.

In summary, using IDS and utilizing data sovereignty as competitive advantage for your own business is quite easy, because everything is ready to go. The guiding web site https://www.internationaldataspaces.org provides all information, and a friendly hotline (SupportOffice@internationaldatspaces.org) is here to help you with any questions.

1.4 Guiding principles

The following guiding principles led the team in structuring the complete IDS ecosystem, it´s roles and this rule book.

- Don't reinvent the wheel.
- Integrate into existing systems.
- Integrate or use existing standards.
- Be industry-agnostic, and applicable in all verticals as horizontal standard.
- Be easily usable and applicable by individual companies and initiatives/ecosystems.
- Overall: Create an open global standard for data sovereignty:
  Open standard generally implies: 1) free to use for everyone (although in some sectors this is interpreted in different ways), 2) an open process through which everyone can participate, 3) transparent decision-making (preferably by consensus or otherwise through a pre-defined structure).

1.5 Glossary

The IDSA rule book is considered normative and is therefore compliant with RFC 2119. The general IDSA glossary can be found on IDS-G.[1]

1.6 Do you want to know more?

Throughout this rule book, you will find references to different IDS and IDSA elements that you may want to know more about. Remember that you can always find additional information about these elements, and much more, at other sources provided by IDSA:

- The IDSA website (https://www.internationaldataspaces.org) website aims to provide visitors with an easy way to learn about the International Data Spaces Association. It is the reflection of what we do, who we are and what International Data Spaces stand for. Use cases illustrate the possibilities of the data economy and outline the added value created by the IDS standard. The download center gives

[1] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary

access to the IDS Reference Architecture, papers and studies, scientific publications and marketing materials. We are constantly updating our content with news and blog articles, events and with our regularly published magazine DATA SPACES NOW.

- The IDSA Jive collaboration platform (https://industrialdataspace.jiveon.com) is the collaboration platform for IDSA members, where you can find details from the IDSA Working Groups and Task Forces. IDSA members can get access to jive via the IDSA Homepage [https://industrialdataspace.jiveon.com/].
- The IDSA GitHub repositories (https://github.com/International-Data-Spaces-Association) see also section 3.4

2 Functional agreements

Functional agreements define the rights and duties for the different roles played by various parties in the IDS. Next to the basic and technical role-definition in the Reference Architecture Model, further assignments must be made to operationalize the IDS. This includes defining essential services needed to operate a data space and base services that are not mandatory but required from a data space perspective to enable the required functional aspects. Enabling essential services is crucial for the IDS and it includes administrative tasks, as described in section 4.2.1. These tasks will be conducted in one or more support organizations as described in the remainder of this section.

The IDS-RAM[2] defines a role model in the business perspective section to describe the fundamental mechanics of a data space. Each role that a participant can assume in the IDS is described in detail, together with the basic tasks assigned to it. The majority of roles require certification of the organization that wants to assume that role, including certification of the technical, physical, and organizational security mechanisms the organization employs. Certification of organizations that want to participate in International Data Spaces is considered a fundamental threshold to establish trust among all participants (especially with regard to roles that are crucial for the overall functioning of such as the broker service provider, the app store, the identity provider, or the clearing house). The certification scheme applied in the participant evaluation process is described in detail in Section 4.2.

There are four categories of roles:

- Category 1: Core Participant
- Category 2: Intermediary
- Category 3: Software / Service Provider
- Category 4: Governance Body

[2] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#ids-reference-architecture-model

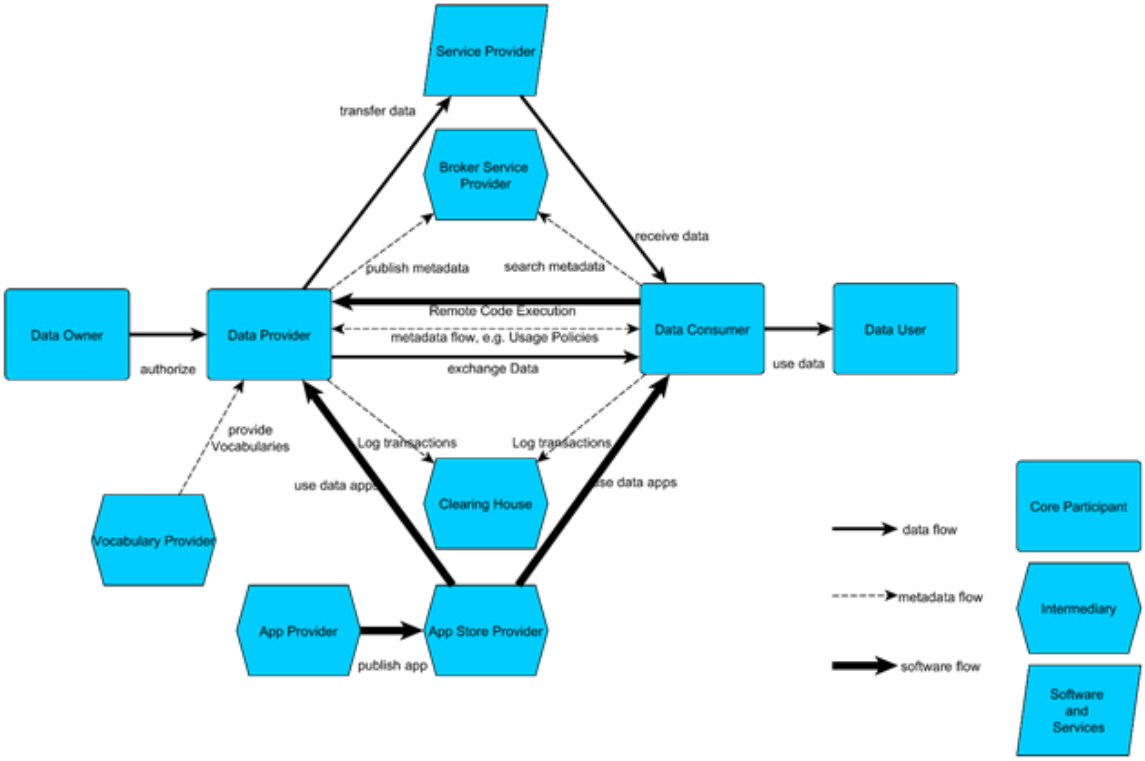


Figure 3 Role model as described in IDS-RAM

While the IDS-RAM defines the existence of an identity provider and states its technical relevance, the rule book reflects the operational aspects of the identity provider as essential services.

2.1 Essential services

2.1.1 Archetypal framework conditions

In the reference architecture, IDSA has defined archetypal roles (in the sense of a generally applicable standard) for data ecosystems that follow the value propositions of international Data Spaces of trust, data sovereignty and enforcement of terms of use for data (see IDS RAM).

2.1.2 Essential Services

Some of these roles are essential for the fulfilment of the value proposition:

- Certification Body (CB)
- Certification Authority (CA) (provisioning of X.509 certificates)
- Dynamic Attribute Provisioning Service (DAPS) (OAuth compatible)
- Participant Information System (ParIS)
- Dynamic Trust Management (DTM) (former Security Operation Center)

These roles must be operated and controlled in operational terms under the rules of procedure defined by the IDSA. There is a make-or-buy option for each of these roles, i.e.

they can be operated by the IDSA or tendered to one or more service providers. Until further notice, a service center as part of the office will be responsible for coordination. In the medium term, the service center is to be transferred to a separate corporate body for the professional maintenance of operations – for the time being named as "IDSA Support Organization". This option is desired and should be realized from the very beginning.

Further roles are important but not essential for the success and growth of data ecosystems - these include the app store, vocabulary provider and clearing house. It is not the IDSA's task to fill these roles or to give them a business structure. This is left to the market. The IDSA is active as a non-profit association on a pre-competitive basis. Nevertheless, the IDSA sees it as its task to stimulate data ecosystems based on IDS.

2.1.3 Base Services

While essential roles in the IDS are required to provide trust in the ecosystem, others are required to improve usability of the system as a whole and raise the added value of the ecosystem. These roles are described as base services and should be enabled by key participants of the ecosystem. The following service are considered to be base services:

- IDS meta-data broker (rudimentary broker-functionality according to reference architecture)
- Clearing house (decentralized logging capabilities, according to IDS-RAM)
- App store (according to IDS-RAM)

2.1.4 Connectors

The success of trusted data ecosystems also requires the provision of IDS connectors as a central component for secure and trusted data exchange. To this end, companies must develop commercial and non-commercial offerings in this direction and offer them to the market (i.e., variants of the four IDS Connector profiles defined in the reference architecture as open source, as a product or as an as-a-service offering). The IDSA supports the development of this offer by providing sample code, reference implementations, testbeds including test services for interoperability testing, technical specifications, a starter kit and a co-creation platform in the form of a developer community. Companies that want to offer software based on the IDS Reference Architecture or services according to the role definition of the IDS Reference Architecture must be members of the IDSA.

The IDSA advocates a market-based approach, international competition and diversity of offerings, especially with regard to the ability to fit in with companies of all sizes (from SMEs to international corporations).

2.2 IDSA Support Organization (IDSA-SO)

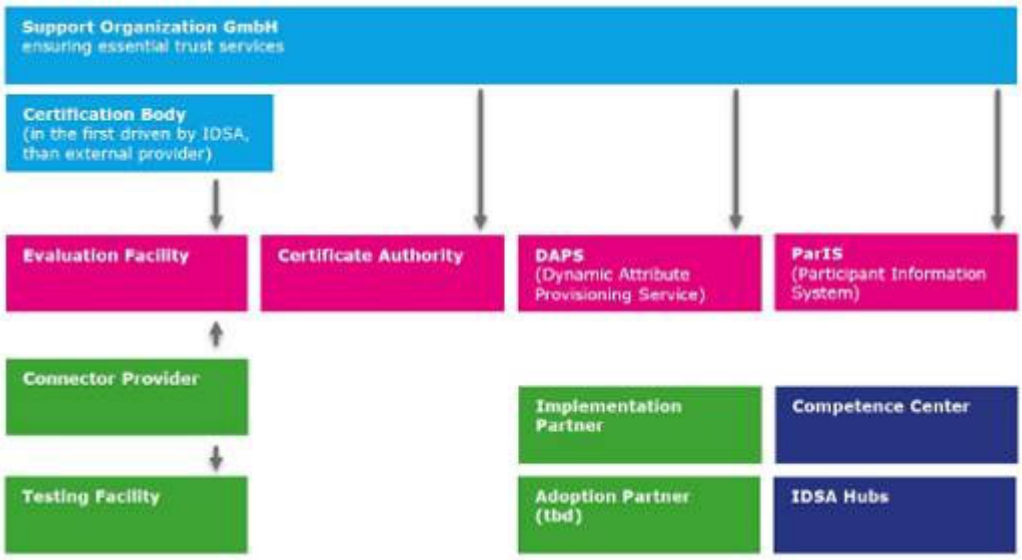


Figure 4 Structure of the IDSA Support Organization

IDSA SO is the entity securing trust in IDS solutions. This entity is responsible for coordinating the essential services which will be provided by several provider companies which perform their service according to the IDS rule book and the right there provided rules of procedure. This contains these services:

Certificate Authority:

To secure the flow of data between entities, the parties in the digital ecosystem must be able to identify and authenticate themselves. Identity verification and secure digital storage of identity parameters are part of the essential services that will be provided. ID certificates secure the digital communication.

Evaluation Facilities (for components and organizations) and SW testing:

Certification of companies and connectors will be conducted by evaluation facilities. These will also provide consultancy and pre-defined test procedures for SW prior to certification. Only certified organizations and connectors can take part in the IDS ecosystem. The criteria are defined in DIN SPEC 27070 and in the criteria catalogue of IDSA.

DAPS (Dynamic Attribute Provisioning Service), **ParIS** (Participant Information Service):

Efficient management of certificates and metadata, streamlining the process and reducing cost through use of a dynamic attribute provisioning system.

Enabling Services:

The IDSA Support Organization provides a connection to other services that enable participants to enter a Data Space, if required. These are services by **Implementation Partners** and **Adoption Partners**, as well as Open Source or

commercial offerings for connectors, core components or testing facilities for own developments.

IDSA SO will organize these processes according whereby it ensures the provisioning and SLA of the essential services provided by companies from the market.

The governance framework including the functional, technical, operational, and legal agreements for the interaction of the IDSA SO with the essential services providers are defined in the IDS rule book.

2.2.1 Tasks, business processes and resources for the IDSA Support Organization

The IDSA SO has the core working fields:

- Organizing essential services
- Acting as Certification Body

Essential service provider management

The IDSA SO has to conduct the following tasks for Essential Service Provider Management:

- Manage rules of procedure
- Perform RfQ
- Selection of providers
- Assignment of providers
- Onboarding, Offboarding of providers (see Figure 5)
- Billing
- Contact point for general support, first level support remains the duty of service providers, including evaluators.

The essential services can indiscriminatory be provided by any company accepting the rules of procedure and SLAs.

Certification body

The IDSA SO will take over the role of the certification body for the IDSA. The business processes to be performed are depicted in the Figure 5.

This includes the following processes for “technical onboarding of participants”:

- IDSA SO takes over the role as the official certification body
- IDSA SO receives and assesses evaluation report for components
- IDSA SO receives and assesses evaluation report for organizations
- IDSA SO evaluates the provisioning of digital certificates for components and organizations by the CA according to the evaluation results and agrees to the provisioning in case of a positive evaluation
- IDSA SO registers components and organizations in DAPS
- IDSA SO updates ParIS

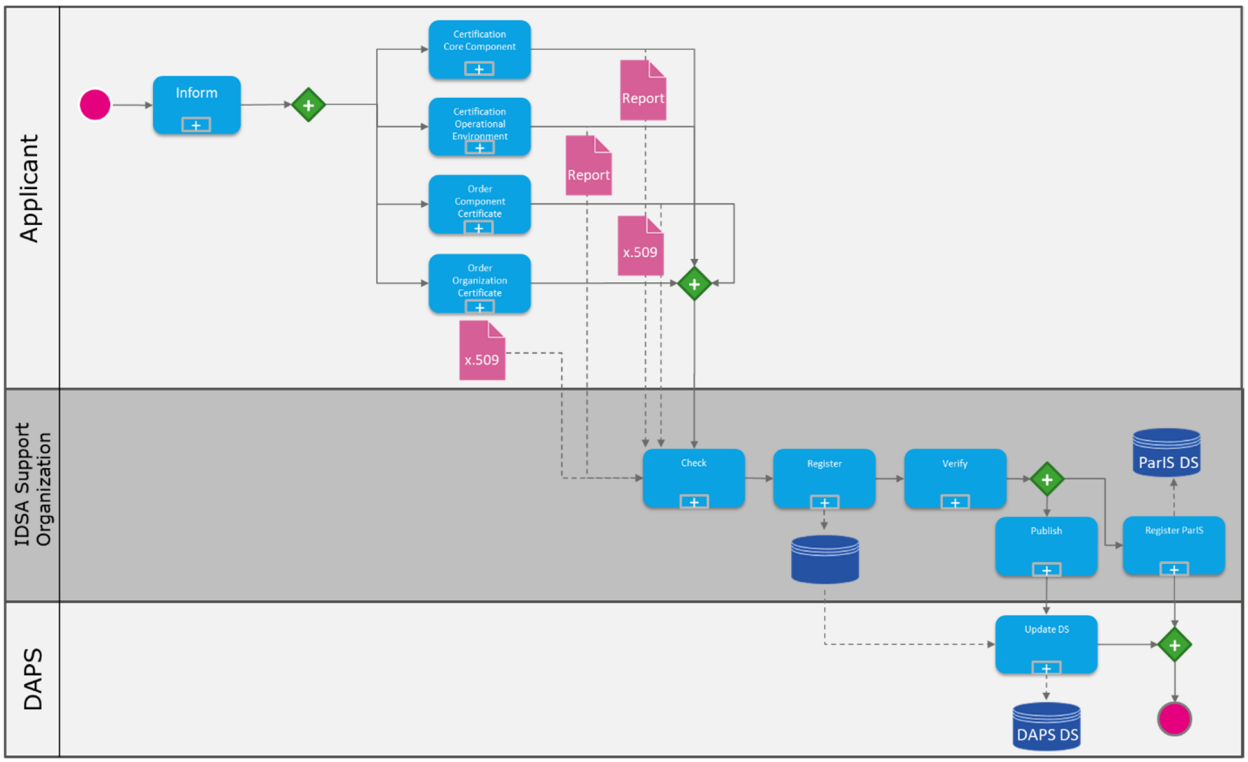


Figure 5 General onboarding flow in IDSA Support Organization

This includes the following processes for "technical onboarding of participants":

- IDSA SO takes over the role as the official certification body
- IDSA SO receives and assesses evaluation report for components
- IDSA SO receives and assesses evaluation report for organizations
- IDSA SO evaluates the provisioning of digital certificates for components and organizations by the CA according to the evaluation results and agrees to the provisioning in case of a positive evaluation
- IDSA SO registers components and organizations in DAPS

IDSA SO updates ParIS

2.3 Additional roles

Additional roles that are not Essential Services nor Base Service also need further definition of for operationalization.

2.3.1 Service Providers

Currently no further specification available.

2.3.2 Certification Body

The duties of the Certification body on operational level are as described in the section of the IDSA Support Organization (IDSA Support Organization (IDSA-SO) on page 14) and the Certification Scheme[3].

The Certification Body approves evaluators for the IDSA Certification Scheme. This includes the following activities:

- Provides application form for the approval of Evaluation Facilities
- Checks applications for completeness and consistency (formal checking)
- Informs applicant about incompleteness of the application
- Informs applicant about incompleteness of the application
- Maintains a database for all companies applying for becoming an Evaluation Facility (considering GDPR and other guidelines)
- Stores all documents of the application (considering GDPR and other guidelines)
- Organizes Audit to evaluate the applying Evaluation Facility
- Determines the group of evaluators to be interviewed
- Arranges and schedules the audit
- Conducts the audit on three to four areas
    - Quality Management System
    - Security Management System
    - Competence of the Evaluators
    - Equipment and its handling (area of application: component certification)
- Prepares the audit findings in a preliminary report
- Discusses the preliminary report in a final discussion
- Points out eventual corrective measures & (eventually) root cause analysis

Based on the approval process the Certification Body provides an audit report to the applicant. The audit report will be stored by the Certification Body. The audit report states the rejection or the approval of the evaluation facility. In case of rejection the applicant will be informed. An approved evaluation facility will receive an evaluation facility identifier by the Certification Body and an approval statement.

During the evaluation of applicants by the evaluation body, the Certification Body will provide process support and witness the evaluations. It will review the evaluation report and provide certificates.

[3] https://www.internationaldataspaces.org/wp-content/uploads/2020/01/IDSA-Strategy-paper-certification-scheme-V.2.pdf

2.3.3 Evaluation Facilities

Refer to the IDS Certification Scheme[4], Approval for evaluators and IDS-ready link on IDSA Homepage[5].

2.3.4 Metadata Broker

Refer to IDS-RAM and IDS Meta Data Broker Specification (see IDS Specifications on page 21)

2.3.5 Clearing House

Refer to IDS_RAM and IDS Clearing House Specification 1.0(link).

2.3.6 App Store

Will not be part of the Version 1.0 of this document as the required specification are still missing.

2.3.7 Interactions

The interactions between the different roles in the IDS are described in the IDS-RAM. This Rule Book describes additionally the interactions with the IDSA-SO in the following section Administrative Processes 29.

[4] https://www.internationaldataspaces.org/wp-content/uploads/2020/01/IDSA-Strategy-paper-certification-scheme-V.2.pdf
[5] https://www.internationaldataspaces.org

3 Technical agreements

3.1 IDS Reference Architecture Model

Data Exchange and Data Sharing are essential for Data-Driven Business-Ecosystems, as well as the need for Data Sovereignty. The International Data Spaces Reference Architecture Model (IDS-RAM[6]) defines fundamental concepts for Data Sovereignty, Data Sharing and Data Exchange. Focusing on the generalization of concepts, functionality, and overall processes involved in the creation of a secure "network of trusted data", the IDS-RAM resides at a higher abstraction level than common architecture models of concrete software solutions do. The document provides an overview supplemented by dedicated architecture specifications defining the individual components of the International Data Spaces

The model is made up of five layers: The Business Layer specifies and categorizes the different roles which the participants of the International Data Space can assume, and it specifies the main activities and interactions connected with each of these roles. The Functional Layer defines the functional requirements of the International Data Spaces, plus the concrete features to be derived from these. The Process Layer specifies the interactions taking place between the different components of the International Data Spaces; it provides a dynamic view of the Reference Architecture Model. The Information Layer defines a conceptual model which makes use of linked-data principles for describing both the static and the dynamic aspects of the International Data Spaces's constituents. The System Layer is concerned with the decomposition of the logical software components, considering aspects such as integration, configuration, deployment, and extensibility of these components.

In addition, the Reference Architecture Model comprises three perspectives that need to be implemented across all five layers: Security, Certification, and Governance. The Security Perspective defines the common security measures for the International Data Spaces and the concepts for Data Usage Control. The Certification Perspective describes the IDS Certification scheme as a foundation for every interaction in the IDS. The Governance Perspective describes the Responsibilities of the Roles in the IDS.

3.2 IDS Certification Criteria

Certification is one perspective in the IDS-RAM. The IDS Certification approach is described in detail in the IDS Certification Scheme[7]. Additionally, the following documents describe the certification approach in detail:

- Certification Criteria for Core Components (Connector[8]; Broker[9])

[6] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary#ids-reference-architecture-model
[7] https://www.internationaldataspaces.org/wp-content/uploads/2020/01/IDSA-Strategy-paper-certification-scheme-V.2.pdf
[8] https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Components-Connector.pdf
[9] https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Components-Broker-1.pdf

- Certification Criteria for Operational Environment[10]
- Rules of Procedure[11]
- Approval Scheme for Evaluators[12]

3.3 Interoperability Test

Evaluation facilities for components will be conducting the evaluations that ensure a correct implementation of the IDS specifications as well as an adequate level of security in the components. Ensuring a comparable quality of all evaluations is necessary to make the certification with its different security and assurance levels reliable. This includes in particular:

- All evaluation facilities conduct transparent and equivalent conformance tests in the „IDS Reference Testbed“ based on the regulations from the WG Certification and the specifications approved by the IDSA Technical Steering Committee.
- All evaluation facilities assess the fulfillment of the security requirements listed in the IDS criteria catalog in a comparable way.
- The evaluation facilities only advise the issuing of a certificate if both, conformance and security tests, have been passed without issues.
- To ensure the capability of evaluation facilities to conduct the evaluations according to the specifications, the certification body has to assess the competence of the evaluation facilities before approving them.

Ensuring the Interoperability between the components is one important aspect of the evaluation. The Interoperability tests are currently under development[13].

3.4 IDS-G

IDS-G[14] is intended to provide specifications and further documentation by the IDSA to the public. While the Reference Architecture Model and other documents are available via the IDSA Homepage IDS-G focuses on documentation and specifications for developing and testing IDS based solutions. This includes technical documentation and interface descriptions. IDS-G's master branch is stable therefore the reliable foundation for the development and maintenance of IDS-based solutions. It is maintained under the umbrella of the IDSA Technical Steering Committee.

Additionally, IDS-G provides access to the IDSA Open Source projects. Today the following Open Source projects are available:

- IDS Information Model[15]

[10] https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Operational-Environments.pdf
[11] https://industrialdataspace.jiveon.com/docs/DOC-2507
[12] https://industrialdataspace.jiveon.com/docs/DOC-1911
[13] https://industrialdataspace.jiveon.com/community/workinggroups/certification/content
[14] https://github.com/International-Data-Spaces-Association/IDS-G
[15] https://github.com/International-Data-Spaces-Association/InformationModel

More Open Source projects will be set up by the IDSA Technical Steering Committee in the future.

3.5 IDS Specifications

IDSA provides multiple specifications that sum up under the IDSA Reference Architecture Model. The different specifications are aligned in the IDSA Roadmap that is maintained by the IDSA Technical Steering Committee. A release as described in section 4.2.2 therefore contains a set of documents and specifications.

The current specifications are listed below:

System	Document	Status
Connector	**Architecture**	
	https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf see chapter 3.5.1	final (April 2019) Official
	Core Component Certification https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Components-Connector.pdf	Version 2.0 Official
	Operational Environment Certification https://www.internationaldataspaces.org/wp-content/uploads/2020/10/IDSA-White-Paper-Criteria-Catalogue-Operational-Environments.pdf	
	APIs	
	Communication Guide https://industrialdataspace.jiveon.com/docs/DOC-3062	Version1.0 Official
	Handshake https://industrialdataspace.jiveon.com/docs/DOC-1817	
	Usage Control between Connectors https://industrialdataspace.jiveon.com/docs/DOC-2292	
		Version1.1 informative

System	Document	Status
		Version 1.0 Informative
		Work in progress
Usage Control	**General** https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-Position-Paper-Usage-Control-in-IDS.pdf **Policy Language in detail** https://industrialdataspace.jiveon.com/docs/DOC-2264	final (11-2019) informative work in progress informative
Information model	**Information model on Github** http://ids.semantic-interoperability.org/ https://github.com/International-Data-Spaces-Association/InformationModel	V4.0 official
Identity Provider	**DAPS & CA** https://github.com/International-Data-Spaces-Association/IDS-G	Work in Progress informative
Broker	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-White-Paper-Specification-IDS-Meta-Data-Broker.pdf	Version 2.1 official

System	Document	Status
App Store & Data Apps	https://industrialdataspace.jiveon.com/docs/DOC-2604	work in progress informative
Clearing House	https://www.internationaldataspaces.org/wp-content/uploads/2020/09/IDSA-White-Paper-Specification-IDS-Clearing-House.pdf	Version 1.0 official
Certification	Certification Scheme https://industrialdataspace.jiveon.com/external-link.jspa?url=https%3A%2F%2Fwww.internationaldataspaces.org%2Fwp-content%2Fuploads%2F2020%2F01%2FIDSA-Strategy-paper-certification-scheme-V.2.pdf	official
	Rules of Procedure https://industrialdataspace.jiveon.com/docs/DOC-2507	official
	Approval Scheme https://industrialdataspace.jiveon.com/docs/DOC-1911	official
	Requirements for evaluators https://industrialdataspace.jiveon.com/docs/DOC-3213	official

The specifications are the foundation for the IDS and will be evaluated during the certification process.

3.5.1 Dynamic Attribute Provisioning Service (DAPS)

The DAPS[16] specification is available on IDS-G[17]. It includes the specification of the DAPS interfaces as well as the definition of the Dynamic Attribute Token DAT. The DAPS issues Dynamic Attribute Tokens (DATs) to verify dynamic attributes of Participants[18] or Connectors[19].

For the time being DAPS is limited to single instances that are not federated or synchronized with other DAPS instances. This is subject of active work in IDSA.

[16] https://github.com/International-Data-Spaces-Association/IDS-G/blob/master/glossary/README.md#dynamic-attribute-provisioning-service
[17] https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/core/DAPS
[18] https://github.com/International-Data-Spaces-Association/IDS-G/blob/master/glossary/README.md#participant
[19] https://github.com/International-Data-Spaces-Association/IDS-G/blob/master/glossary/README.md#connector

4 Operational agreements

4.1 Governance body

4.1.1 IDSA Support Organization IDSA-SO

Today, the IDSA Support Organization is conducted as an activity in the IDSA Head Office to support the following processes:

Functional Support:

- Onboarding
- Offboarding
- Contact point for general support, first level support remains the duty of service providers, including evaluators.
- Provide general information on IDS, IDSA and on the process support
- Find service providers and/or provide a list of known and approved service providers
- Onboarding and offboarding of essential service providers
- Approval of Evaluators
- Act as Certification Body
- Enabling the essential services:
- CA
- DAPS
- ParIS

The following are not the duties of the IDSA Support Organization:

- Lobbying / Stakeholder Management is done by IDSA HO and IDSA members
- Financing

4.1.2 Bodies of the IDSA

The Bodies of the International Data Spaces Association are described in the IDSA Organizational Handbook and in the statues of the IDSA[20]. An overview is provided in the figure below.

[20] https://www.internationaldataspaces.org/wp-content/uploads/2020/06/IDSA-Statutes-2020.pdf

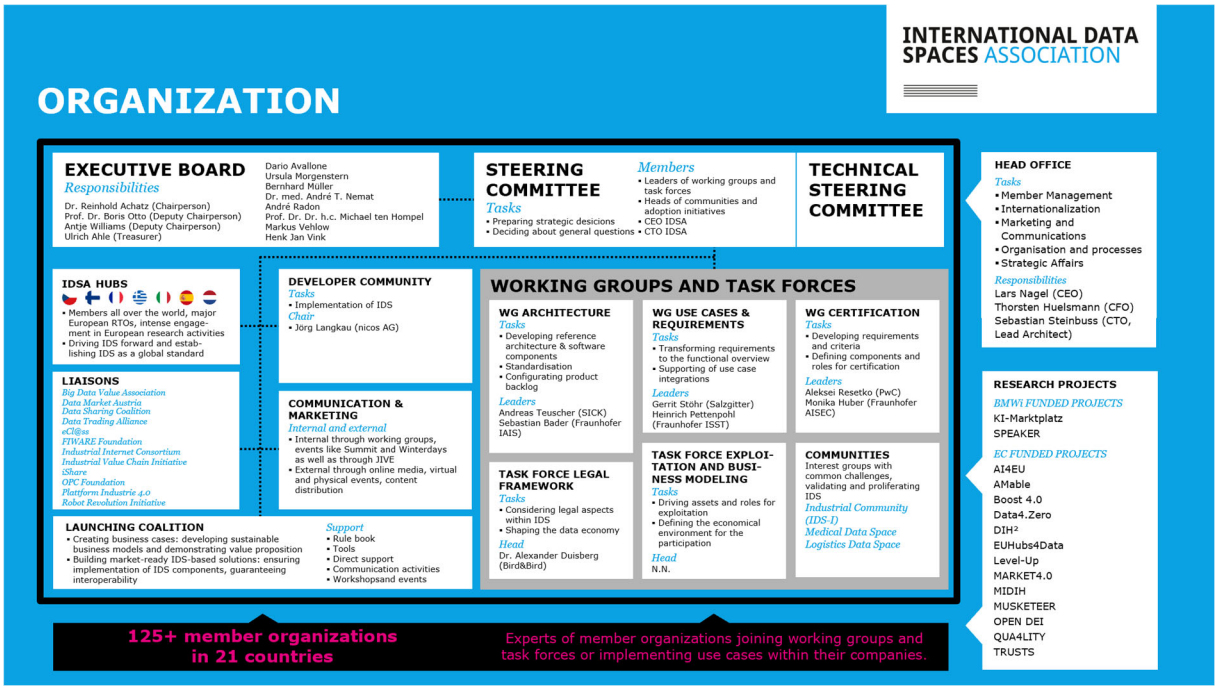


Figure 6 Organigram of the IDSA

4.1.2.1 Executive Board

The Tasks of the Executive Board are describes in the IDSA Statues (IDSA Statutes) §10:

1.The Executive Board is responsible for managing the business activities of the Association. It consists of up to twelve honorary members of the Executive Board:

- the chairman of the Executive Board who may use the title of "President"
- two deputy chairmen of the Executive Board
- the treasurer (who is simultaneously the secretary, unless a managing director is
- appointed to act in this capacity)
- up to eight further members of the Executive Board

2. The members of the Executive Board must be employees at a reasonable hierarchical level within the respective member's organization.

3. Up to eleven members of the Executive Board shall be elected in separate ballots by the General Meeting by a simple majority of the members present or represented at the meeting.

4.1.2.2 Steering Committee

1.The IDSA Steering Committee consists of:

- the Chairs and Co-Chairs of the Working Groups
- the Chairs and Co-Chairs of the Task Forces

- 2 elected representatives of the IDSA Communities
- 2 elected representatives of the IDSA adoption initiatives
- The managing directors of the IDSA Head Office
- one representative from the Fraunhofer as major research partner
- the IDSA Lead Architect

2. The Steering Committee is organized by the IDSA Lead Architect.

3. Every member of the IDSA Steering committee can vote on ballots in the Steering Committee.

4. The Steering Committee:

- decides on topics, that can not be decided in Working Groups and Task Forces
- decides on topics, that concern more than one Working Group or Task Force
- Approves Recommendations in the maturity state Proposed Recommendations (RAM, Certification Scheme, Specifications)
- Prepares decision memos for the managing board
- can be consulted by the Working Group and Task Forces
- Approves the Release Plan of the IDSA (Technical release Plan)
- Responsible (decides on) for the Strategic and organizational Goals and scoping

Working Mode

The IDSA Steering Committee meets on a quarterly basis.

Physical meetings shall be conducted twice a year.

4.1.2.3 IDS Technical Steering Committee

The technical and standardization activities need steering and alignment between the various activities. The IDSA Steering Committee has a broader perspective. Therefore, the IDSA Technical Steering Committee (IDSA-TSC) governs the relevant public projects on IDS-G and technical publications/standards.

1. The IDSA Technical Steering Committee shall prepare the Open Source activities of IDSA.

Composition

Startup Period: During the first six (6) months after launch, the TSC voting members shall consist of the Head of the IDSA Developers Community, the Lead Architect of IDSA, the Head of IDSA Standardization, the head of Working Group Certification, Head of TF Business Relevance.

Steady State: After the Startup Period, there shall be a nomination and election period for electing Contributors or Maintainers to the TSC. The TSC voting members shall consist of eleven (11) elected Contributors or Maintainers.

The technical Working Groups (Architecture and Certification) shall elect each one (1) voting Maintainer, the Task Force Business Relevance shall elect one (1) voting Maintainer, the Developers Community shall elect one (1) voting Maintainer. Seven (7) voting Contributors shall be elected by the IDS-TSC.

The TSC shall approve the process and timing for nominations and elections held on an annual basis.

2. IDS-TSC projects generally will involve Maintainers and Contributors:

- Contributors: anyone in the technical community that contributes code, documentation, or other technical artifacts to the IDSA.
- Maintainers: Contributors who have the ability to commit code and contributions to IDSA's main branch, e.g., IDS-G. A Contributor may become a Maintainer by majority approval of the existing Maintainers.

3. Participation in IDSA through becoming a Contributor and/or Maintainer is open to anyone from an IDSA member company.

4. The IDS-TSC may:

- establish workflows and procedures for the submission, approval, and closure or archiving of projects,
- establish criteria and processes for the promotion of Contributors to Maintainer status, and
- amend, adjust and refine the roles of Contributors and Maintainers listed in Section 2.2., create new roles and publicly document responsibilities and expectations for such roles, as it sees fit.

5. The TSC shall elect a TSC Chair.

6. Responsibilities: The IDS-TSC is responsible for:

- coordinating the technical direction of IDSA
- approving project proposals (including, but not limited to, incubation, deprecation, and changes to a project's charter or scope) in accordance with a project lifecycle document to be developed, approved, and maintained by the IDS-TSC
- designating Top Level Projects as part of the IDSA Open Source activities and maintain the IDSA Release Plan
- creating sub-committees to focus on cross-project technical issues or opportunities
- establishing community norms, workflows or policies for releases
- discussing, seeking consensus, and where necessary, voting on technical matters relating to the code base that affect multiple projects; and
- establishing election processes for Maintainers or other leadership roles in the technical community that are not within the scope of any single project

4.1.2.4 Working Groups (including Task Forces)

The majority of the work of the IDSA is done in the IDSA Working Groups and Task Forces. A Working Group is an ongoing major workstream in the IDSA, while a Task Force works on a major workstream with a defined end and a tangible deliverable at the end.

Working Groups Use Cases & Requirements (suspended)

The Working Group Use Case and Requirements focuses on the development of Use Cases and the methodological support. Therefor it sets up the Use Case Advisory Board and organizes a Use Case Conference.
Chairs: Heinrich Pettenpohl (Fraunhofer ISST), Gerrit Stöhr (gesis)

Working Group Architecture

The Working Group Architecture is organized in a matrix with 4 main working streams:

1. IDS-RAM development
2. Developers Community
3. Standardization and Liaisons
4. New Topics

Relevant topics are organized orthogonally to the working streams as Sub Working Groups

Chairs: Andreas Teuscher (Sick AG), Sebastian Bader (Fraunhofer IAIS)

Working Group Certification

The Working Group Certification focuses on three Working Streams:

1. Development of Criteria Catalogs for Participants and Core Components
2. Maintenance of Criteria Catalogs for Participants and Core Components
3. Definition and Maintenance of the Certification Process

Chairs: Aleksei Resetko (PwC), Monika Huber (Fraunhofer AISEC)

Task Force Legal Framework

The Task Force Legal Framework focuses on

Consultation of Working Groups and Task Forces for legal aspects
Description of Legal Framework for the IDS
Finding and describing missing legal aspects

Chair: Alexander Duisberg

Task Force Business Relevance and Ecosystem Building

Missing Mission Statement
Chairs: Missing

4.1.2.4.1 Working Mode for Working Groups and Task Forces

Member companies of the IDSA can send staff with appropriate experience and knowledge as members of the Working Groups and Task Forces.

Chair and Co-Chair of the Working Groups and Task Forces

The Working Groups elect a chair and co-chair. A simple majority of the attendees is required for the election. The Working Groups should elect the chair and the co-chair for a three-year period.

Chair and Co-Chair for Task Forces are named by the Managing Board or the Steering Committee.

The Chair and the Co-Chair organize the work in the Working Groups.

The Chair and the Co-Chair of the Working Groups and Task Forces are member of the IDSA Steering Committee.

It is recommended that the chair of the working group is set by an enterprise and the co-chair by academia.

4.1.2.5 Responsibilities of the IDSA Head Office

The IDSA Head Office supports the Working Groups in organizational aspects.

Communication within the Working Group, with IDSA members, that are not in the Working Group and external organization of meetings and events.

4.1.2.6 Confidentiality

The meetings of the Working Groups|Task Forces| and Communities are not public. Only members of the IDSA may participate in the meetings.

Invited guests are allowed to participate in the meetings.

4.2 Operational Processes

4.2.1 Administrative Processes

4.2.1.1 Admission (current term in IDSA onboarding)

The goal of the onboarding processes is to structurally connect new organizations to the IDSA . There are four types of onboarding processes which are described below.

1. **Onboarding of evaluation facilities** which can certify IDS-based solutions. The evaluation facilities should be compliant with the strict rules and

regulations as defined in the certification criteria. The evaluation facilities have to become an IDSA member. See section Approval of evaluators on page 39.

2. **Onboarding of service providers** which offer (commercial) services based on IDS. These services are certified by one of the IDS evaluation facilities. The service providers should become an IDSA member. See section Admission (current term in IDSA onboarding)on page 29.

3. **Onboarding of end-users** which use the services offered by service providers. The onboarding process of users is structured according to the corresponding service provider. Therefore, these processes are not part of this Rule Book. The end-users therefore have no direct relation to the IDSA. The end-users can, but do not have to, become an IDSA member.

4. **Onboarding of IDSA members** who want to contribute to IDSA. This is not part of the Rule Book, but additional information can be found at https://www.internationaldataspaces.org.

4.2.1.1.1 Admission of service providers

The Support Organization (as described above) is meant to be the **first** Support Organization, but **not** the **only** one. Meaning the processes from the first service organization can be implemented several times, but they have to be **federated**. The federation is not specified yet and there is work to be done.

The IDSA Onboarding process is depicted in the following picture. While the applicant has to set up some things before entering the Data Space, the Support Organization helps by informing the participant and guides through the different activities. In the following the different activities are described.

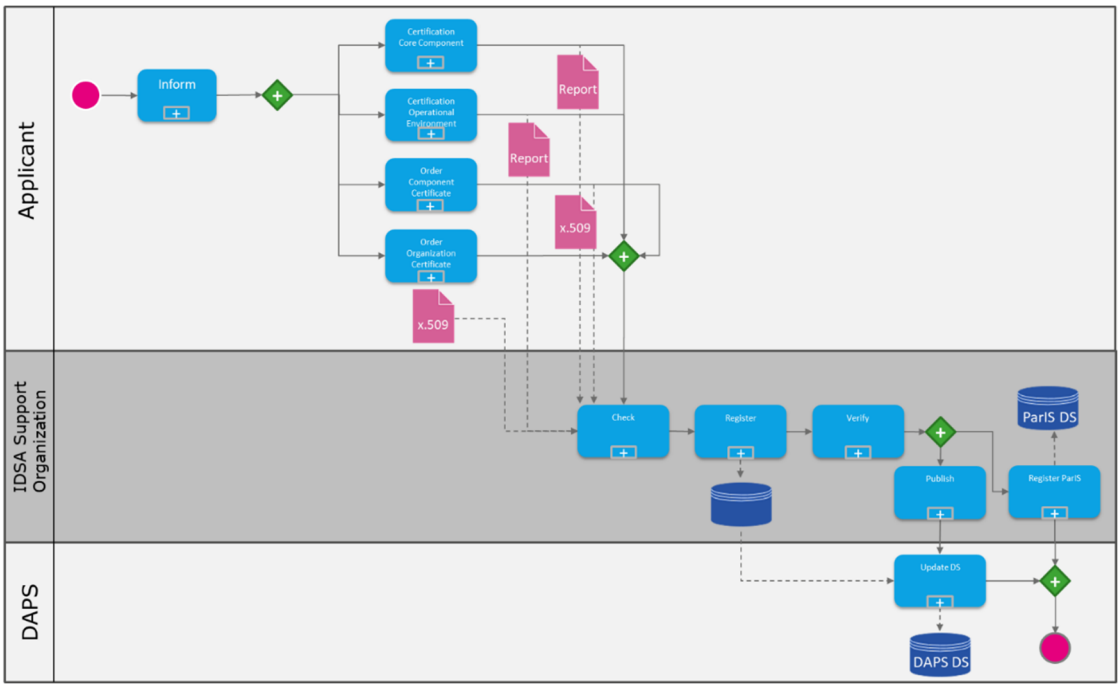


Figure 7 Overview onboarding process

Step: Inform

Responsible: Participant

Precondition: None

Postcondition: Certification can be started and X.509 Certificates can be set up

Short description:

Gather required information and plan IDS Set Up

Long Description:

The participant of the IDS needs to understand and implement the IDS concepts as described in chapter 3 of the IDSA rule book including the following documents:

- IDS Reference Architecture
- IDS Certification Scheme

Related Documents:

- IDS Starter Kit

Step: Certification of Core Component

Responsible: Participant

Precondition: Information and Planning done

Postcondition: Certification Report available

Short description:

See White Paper Certification

Long Description:

See White Paper Certification and subsequent documents

Related Documents:

Step: Certification of Operational Environment

Responsible: Participant

Precondition: Information and Planning done

Postcondition: Certification Report available

Short description:

See White Paper Certification

Long Description:

See White Paper Certification and subsequent documents

Related Documents:

Step: Set Up X.509 Certificate

Responsible: Participant

Precondition: Information and Planning done

Postcondition: Connector Certificate (X.509!) available

Short description:

Definition of CA Policies in progress.

Long Description:

Definition of CA Policies in progress.

Related Documents:

Step: Check

Responsible: Support Organization

Precondition: Certification is done and X.509 available

Postcondition: Start registration

Short description:

Check documents and artifacts provided by the participant

Long Description:

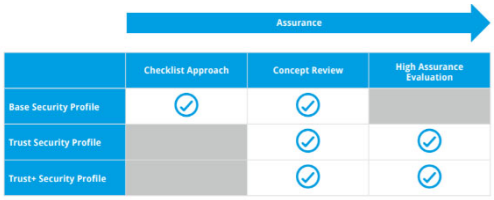
The IDSA Support Organization acts as Certification Body as described in Synopsis: Rules of Procedure for the Certification of IDS Participants and IDS Core Components [was: Verfahrensordnung für die Zertifizierung von IDS-Teilnehmern und IDS-Kernkomponenten] §2.

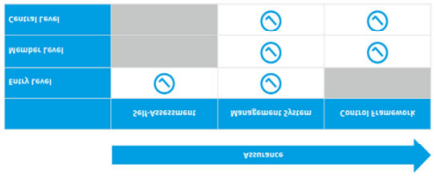
The Evaluation of the Core Component and the Operational Environment has to be checked according to the Rules of Procedure for the IDS Certification.

The content of the Certificate is described in Synopsis: Rules of Procedure for the Certification of IDS Participants and IDS Core Components [was: Verfahrensordnung für die Zertifizierung von IDS-Teilnehmern und IDS-Kernkomponenten] §5.1 No. 2-6

See following tables for mapping.

Related Documents:

The paragraph in Rules of Procedure	Text	Rule Book Specifications
§5.1.2.a	the applicant, if applicable as a short designation;	Complete name of the applicant company including the legal form (String)
§5.1.2.b	the object of certification, if applicable as a short designation;	Identifier of the Operational Environment or Component (String)
§5.1.2.c	the certification body;	identifier of the Certification Body as described in (To be defined where?)
§5.1.2.d	the designation of the authoritative version of the IDS certification criteria, if applicable as a short designation;	Version number and data of the Criteria Catalogue (for Core Component of Operational Environment) and Rules of Procedure IDSA Certification Criteria for Core Components|Operational Environment Version: N.n.n Date: YYYY-MM-DD Rules of Procedure Version N.n.n YYYY-MM-DD
§5.1.2.e	the designation of the applied rules and regulations of the certification body;	The Certification Level as described in IDSA Whitepaper Certification for 1. Core Component  Base Security Profile| Trust Security Profile | Trust+ Security Profile Checklist Approach|Concept Review|High Assurance Evaluation

The paragraph in Rules of Procedure	Text	Rule Book Specifications
		2. Operation Environment  Entry Level | Member Level | Central Level Self Assessment | Management System | Control Framework
§5.1.2.f	a unique certificate number;	See §5.2.2 No.6
§5.1.2.g	the period of validity of the certificate	Valid from YYYY-MM-DD until YYYY-MM-DD (full day each; starts at 0:00 ends at 24:00)
§5.1.2.h	an appendix containing the information pursuant to para. 3	see §5.2.2 No.3
§5.1.2.i	the IDS test mark.	See Appendix B

The paragraph in Rules of Procedure	Text	Rule Book Specifications
§5.1.3.a	the description of the object of certification;	Textual description of the object of certification, not more than 1000 characters (String)
§5.1.3.b	the unique designation of the applicant;	Full name of the company including (main) address and the EORI Number (Economic Operators' Registration and Identification)

§5.1.3.c	the unique designation of the certification;	IDS Certification|IDSC
§5.1.3.d	the designation of these procedural rules as the authoritative procedural basis;	Rules of Procedure for the Certification of IDS Participants and IDS Core Components Version 1.0
§5.1.3.e	the designation of the applied rules and regulations of the certification body;	
§5.1.3.f	the unambiguous designation of the test report and the testing laboratory;	
§5.1.3.g	the exact designation of the authoritative version of the IDS;	
§5.1.3.h	the test results.	

Step: Register

Responsible: Support Organization

Precondition: documents and artifacts provided by the participant are checked

Postcondition: Registration done

Short description:

Create a record including the information from the check action and information with regard to the Connector Certificate (public key)

Long Description:

Create a record at DAPS and ParIS (details are work in progress) and activate participant in IDS

Related Documents:

Step: Verify

Responsible: Support Organization

Precondition: participant registered

Postcondition: participant can use data space

Short description:

Verification of the information with DAPS and Participant.

Long Description:

The verification is not specified, yet.

Related Documents:

Step: Update DAPS

Responsible: DAPS/IDSA-SO

Precondition: Participant registered

Postcondition: Participant can use data space

Short description:

Create a participant record at DAPS.

Long Description:

Work in progress.

Related Documents:

Step: Update ParIS

Responsible: ParIS/IDSA-SO

Precondition: participant registered

Postcondition: Participant information available at ParIS

Short description:

Create a record at ParIS

Long Description:

Work in progress.

Related Documents:

Step: Publish Participant

Responsible: IDSA-SO

Precondition: Participant registered and verified

Postcondition: Participant information published

Short description:

If and how additional information will be published is still to be decided.

Long Description:

Work in progress.

Related Documents:

4.2.1.2 Certification

4.2.1.2.1 Approval of evaluators

The process for the approval of IDS evaluation facilities is described in the Approval Scheme for Evaluation Facilities.

The process consists of three main phases for the approval (Preparation phase, Audit phase, Approval phase) and two additional phases for the renewal of the approval and the suspension/restriction/withdrawal of the approval.

Please note that, as already mentioned in the (Roles section) the role of Certification Body is temporarily taken on by IDSA, which will hire some external experts to be able to carry out the audit on the compliancy of the evaluation facilities.

A flowchart of all the phases of the process is available in Jive[21] and it is reported below.

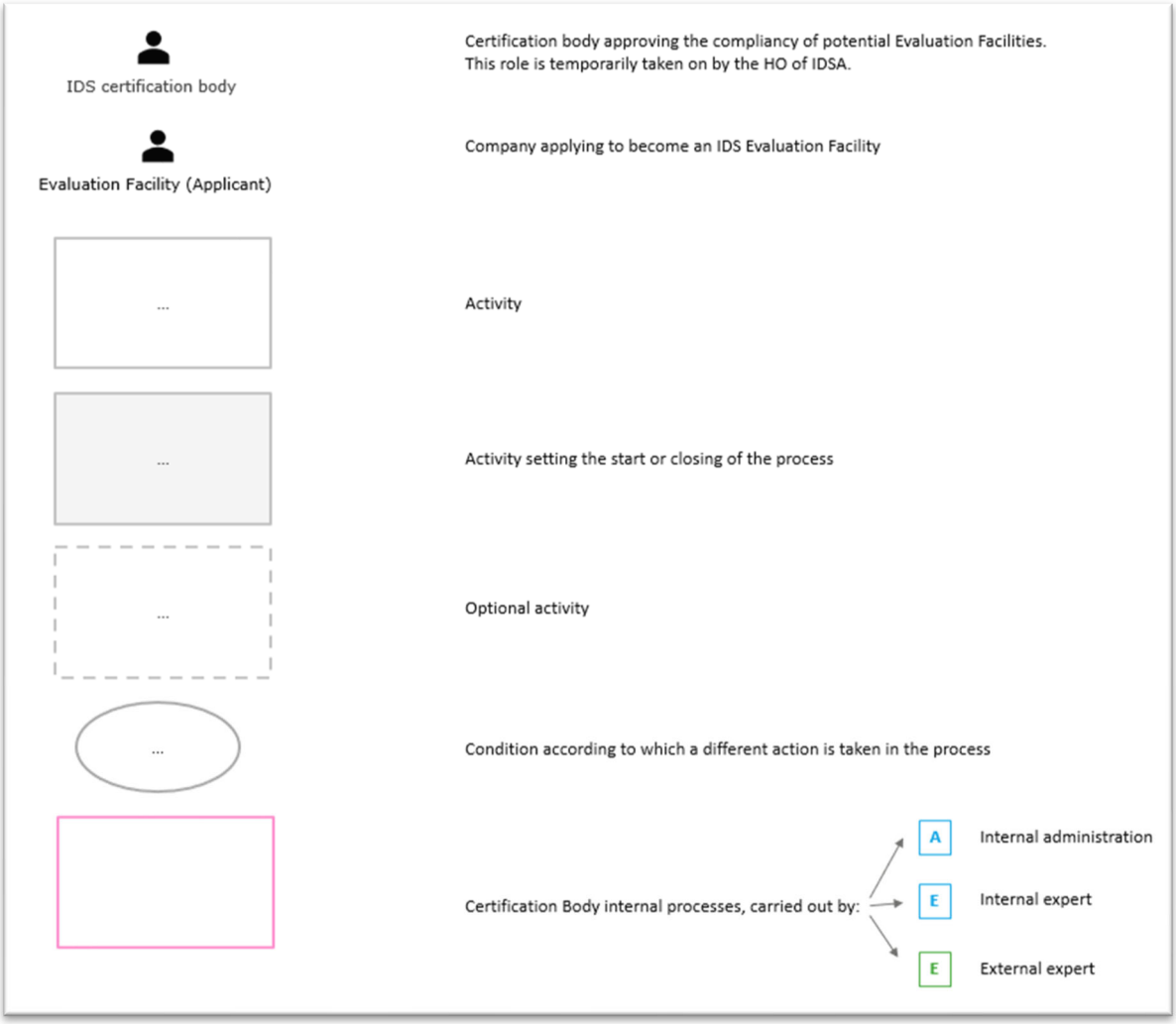


Figure 8 Legend, used symbols in the flow charts for the Certification Body

[21] https://industrialdataspace.jiveon.com/docs/DOC-3273

PREPARATION PHASE

The preparation phase consists of the initial activities to start the approval process: the certification body uploads all the necessary documentation on its website, the evaluation facility submits the formal application to become an IDS evaluation facility and the certification body checks that the application and related attachments are fine.

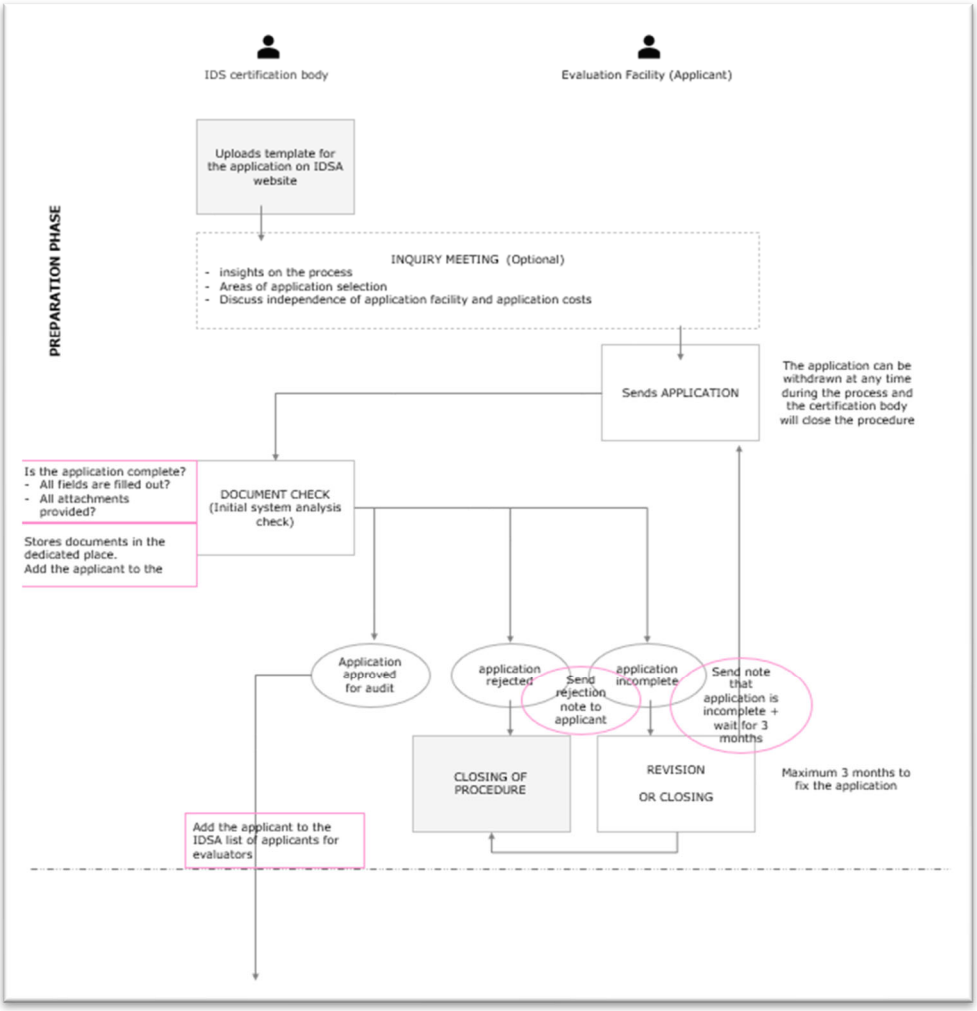


Figure 9 Flow chart Certification Body preparation phase

AUDIT PHASE

Once the application is accepted, the certification body provides the applicant with an audit plan and schedules the audit. The aim of the audit is to check that the requirements are implemented and effective and it is carried out via 3 or 4 assessments, depending on the area of application.

After the assessments are completed the certification body prepares a preliminary report, which will be discussed in a meeting with the applicant.

The phase closes after the discussion with the audit is assessed as successful or unsuccessful. In this second case the applicant can decide to plan some corrective

measures, and in this case the Approval Phase does not follow immediately, because ad additional audit might be needed afterwards.

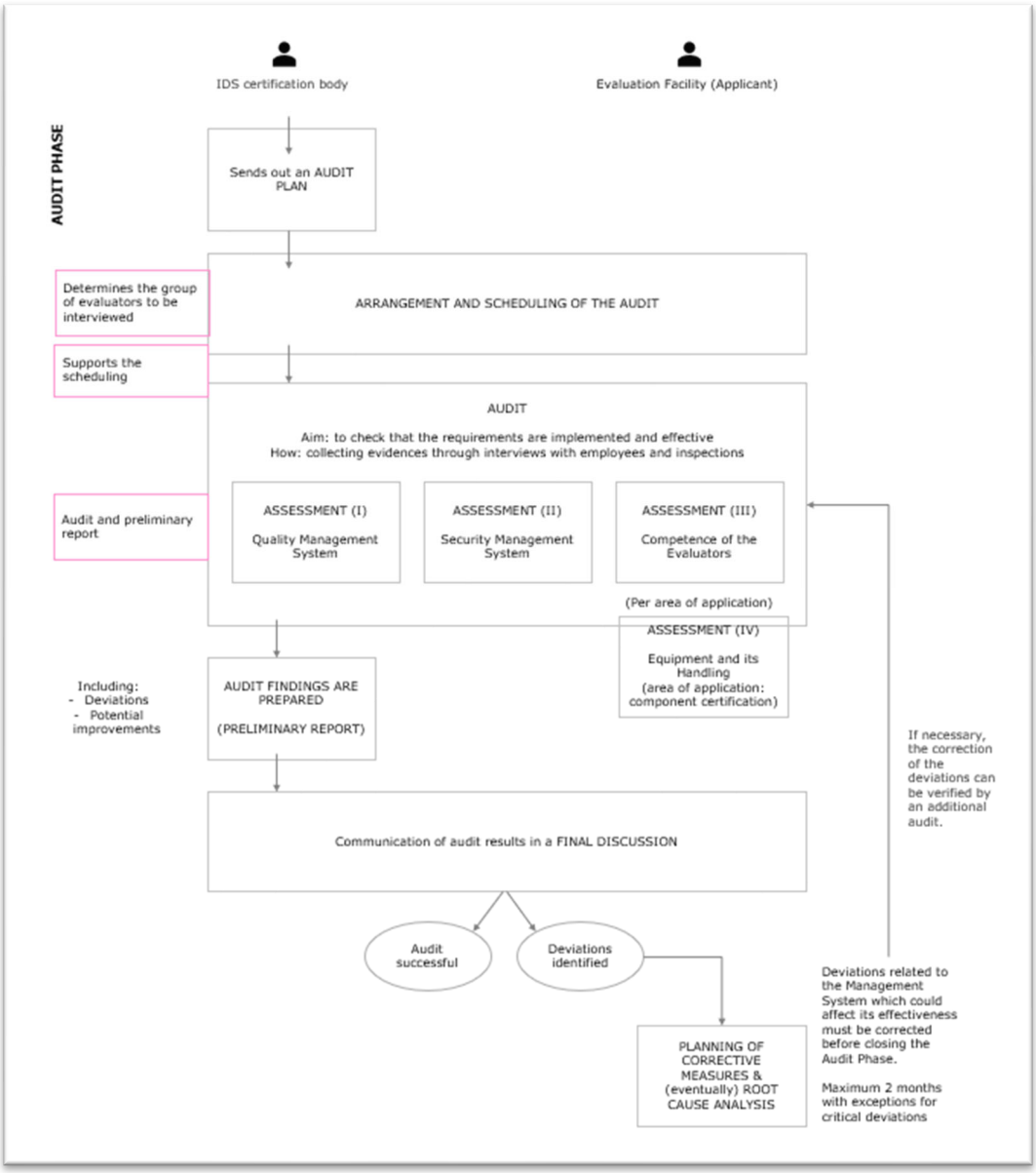


Figure 10 Flow chart Certification Body audit phase

APPROVAL PHASE

During the Approval Phase the application is formally approved or rejected.

Rejected applicants receive a formal communication of rejection. Corrective measures can be implemented, or objections can be carried out (within one month).

The approved applicants receive an official certificate from the certification body, which is valid for 2 years. They are now approved evaluation facilities and can start do evaluations

for IDS components and/or operational environments. Before the certificate expires after two years, they have to undergo the renewal for approval described in the next paragraph.

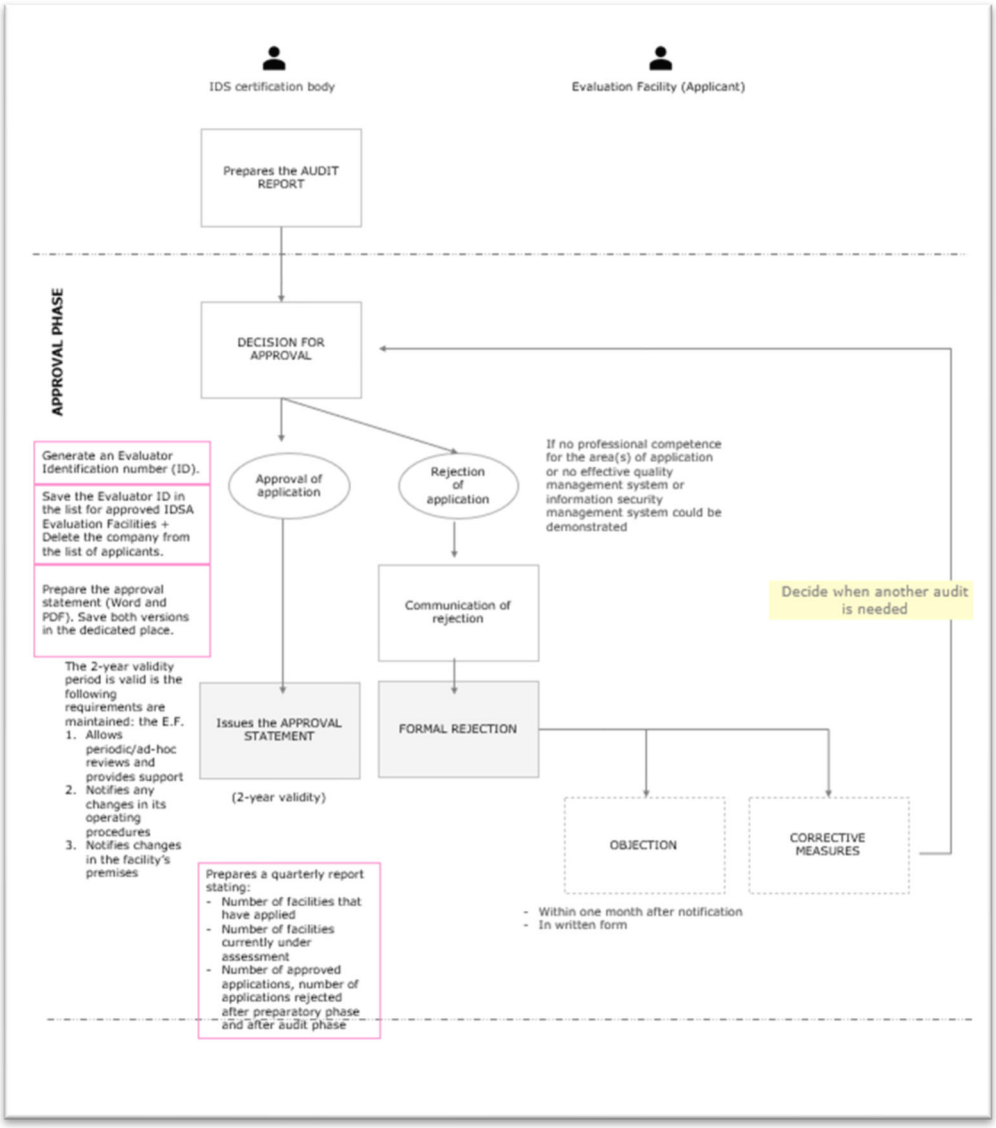


Figure 11 Flow chart Certification Body approval phase

RENEWAL PHASE

Five months before expiry of the certificate, the approved evaluation facility must formally request the renewal of approval. A new audit is then organized, which focuses on the changes that the evaluation facility underwent in the last two years.

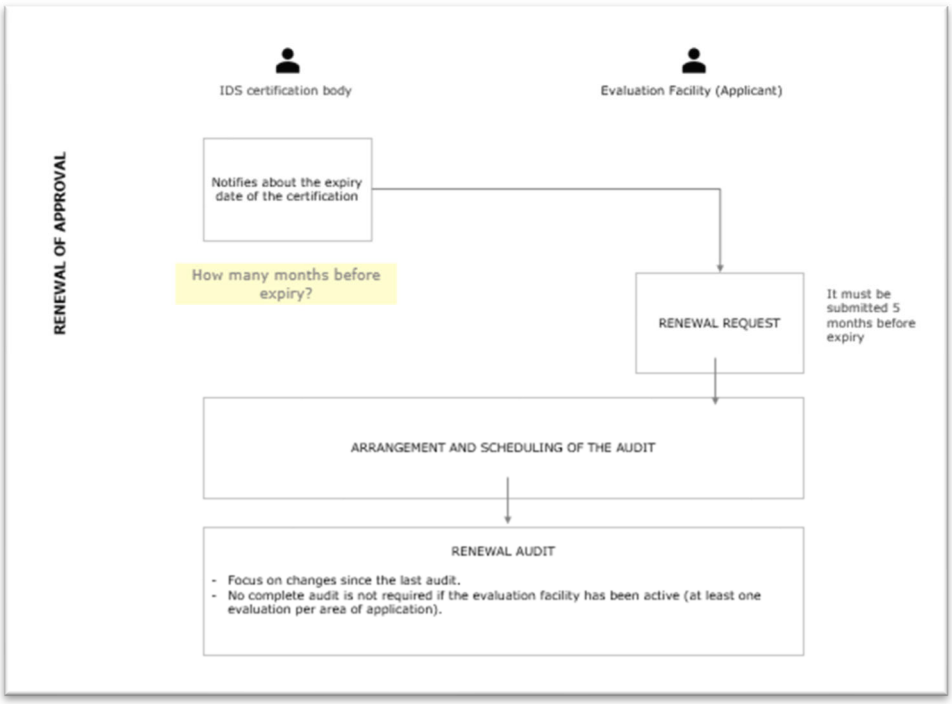


Figure 12 Flow chart Certification Body renewal phase

SUSPENSION/RESTRICTION/WITHDRAWAL

The Suspension/restriction/withdrawal of the approval can be triggered by either the evaluation facility itself or from the IDS certification body in case there are reasons to believe that the evaluation facility does not meet the IDS requirements anymore.

Suspension is a temporary state that is needed to consider the withdrawal of the evaluation facility or the restriction of its area of application.

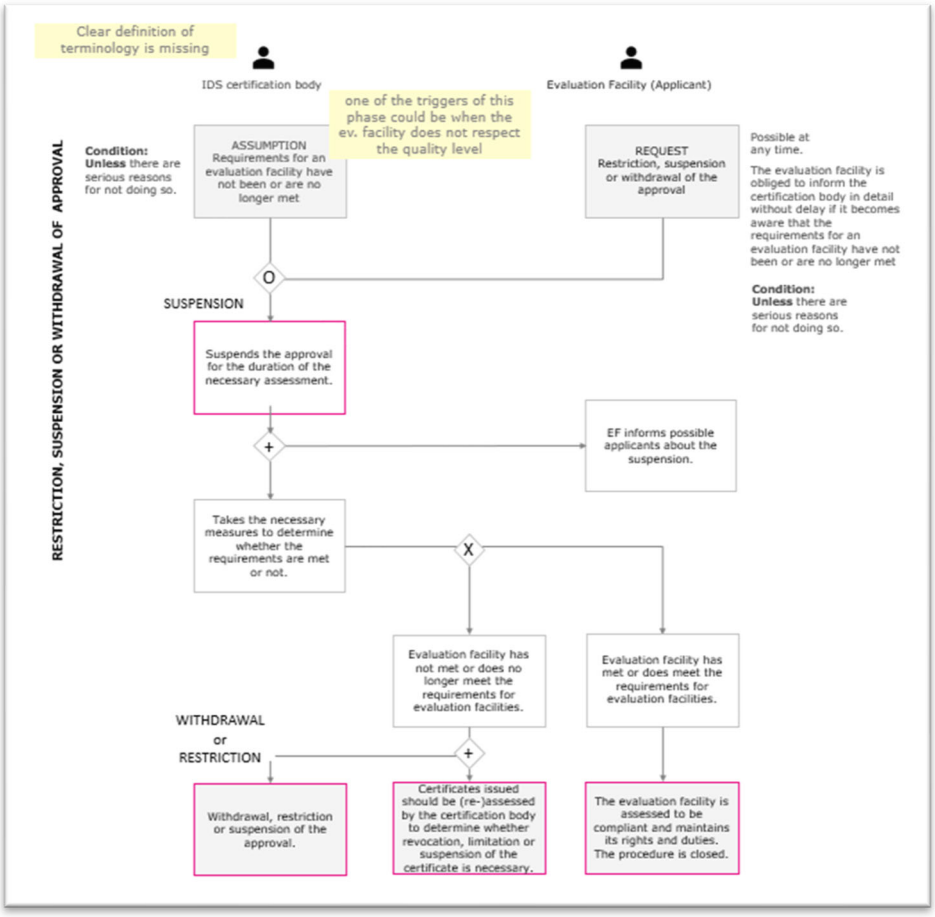


Figure 13 Flow chart Certification Body suspension, restriction and withdrawal

4.2.1.2.2 Evaluation of applicants

The evaluation process is described in the IDSA Certification Scheme. The support office guides applicants through the process. In general, the Certification Body orchestrates the overall process as depicted in Figure 14.

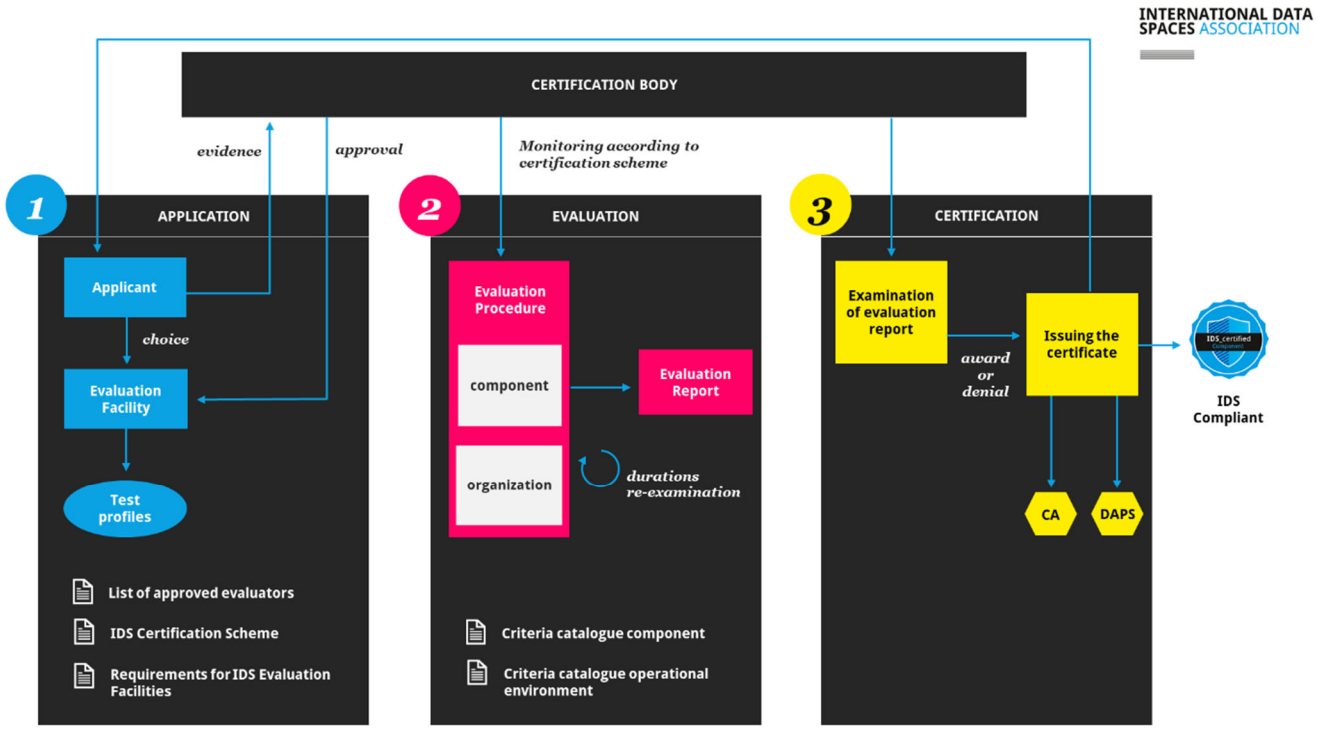


Figure 14 Overall process for applicant evaluation

4.2.1.3 Withdrawal

The Withdrawal process is not further defined in this Rule Book.

4.2.1.4 Warnings, Suspension and Exclusion

Warnings, suspensions and exclusion, as well as measures are not defined in this Rule Book.

4.2.1.5 Incident Management

As IDS is a decentralized ecosystem several types of incidents have to be considered. Those different types of incidents are managed by different roles in the IDS. Basically, three different incident types have to be considered:

- Incidents on security level to be monitored by Dynamic Trust Management (see IDS-RAM), e.g.:
  - Security vulnerability in software component discovered
  - Central entities as the DAPS or the Clearing House are victim to a (DOS) attack
  - A certificate used in the IDS is compromised

  - An attacker gained access to customer data transferred in the IDS
- Incidents Usage Policies and Contracts monitored by the Clearing House (see Clearing House Specification)
  - Violation of Usage Policies
  - Contract Violation
- Service Level monitoring for Essential Services
  - Mis-functioning of the service
  - Unavailability of the service

While the IDS-RAM defines roles to manage incidents on security level and incidents on Usage Policies and contracts, the management of SLAs is not defined here.

In general, each service provider has to set up an incident management process as defined in the Certification Criteria for Operational Environment. As the IDS-SO only provides the services related to the Certification Body, the IDSA-SO has to manage incidents related to this. The IDSA-SO must provide quarterly reports on incidents in the IDS ecosystem to the bodies of the IDSA. Therefore, it must be an obligation to the service providers to provide reports on incidents. This must be incorporated into the SLAs and policies defined in the subsequent chapters. The IDSA-SO provides a contact point for general support, first level support remains the duty of service providers, including evaluators.

4.2.2 Maintenance Processes

The processes described a structured way of interaction between the IDSA bodies and each have a specific goal (i.e., output) and input.

4.2.2.1 Version Management

The goal of version management is to release and use new versions of the IDS standard in a structured manner. Both the IDS community and the IDS standard itself are growing at an enormous pace and it is therefore essential that new improvements are released in a structured manner such that interoperability within the community is ensured.

4.2.2.1.1 The IDS Standard

The IDS standard is composed of a set of sub-standards which each have a separate versioning policy. IDS consists of the following components (see IDS Specifications on page 21):

4.2.2.1.2 Versioning

The above-mentioned subcomponents are combined into a single IDS release. This release contains the right version of all the required components. IDS has three different types of releases which are numbered as follows: major minor errata (e.g. 3.4.1 meaning major version 3, minor version 4, errata version 1).

- **Major Release** contains many (fundamental) changes and might not be backwards compatible with the previous major release. There can be at most a single major release per year.

- **Minor Release** contains enhancements of the major release and should be backwards compatible with the major release. There can be at most two minor releases per year.
- **Errata Release** contains urgent (security) updates, corrections, and clarifications and should be backwards compatible with the major release. This release should not contain any new features. There is no maximum for the number of Errata releases. However, these releases should be avoided.

Note that each IDS subcomponent (see previous section) does have a separate version number, following the same principles as mentioned above. An IDS release contains one version of all IDS subcomponents. It might be the case that in a new IDS release not all subcomponents are updated.

4.2.2.1.3 Release and Adoption Policy

It is essential that all organizations using IDS (e.g., evaluation facilities, service providers, and end-users) migrate in a structured manner to latest IDS release to ensure long-term interoperability. Therefore, strict adoption rules are required.

First, we have to define how releases are created. As is explained in the next sections in more detail, workgroups and task forces work on specific IDS topics. These workgroups and task forces further improve individual IDS components based on the community's feedback. It is important to involve the wider IDS community in the development of new versions and therefore it is required for major and minor releases to first publish one or multiple release candidates as a form of a public consultation.

Based on the feedback of the community, the Chair of a corresponding workgroup can propose the new component version to the Steering Committee for approval. The Steering Committee can approve minor and errata releases, and will prepare some advice for the Executive Board for approval of a major version.

After the version has been approved, the new version will be published, and a migration period will follow where both the current major and the new major version are supported. After the migration period, the old version will be decommissioned and therefore not be used anymore.

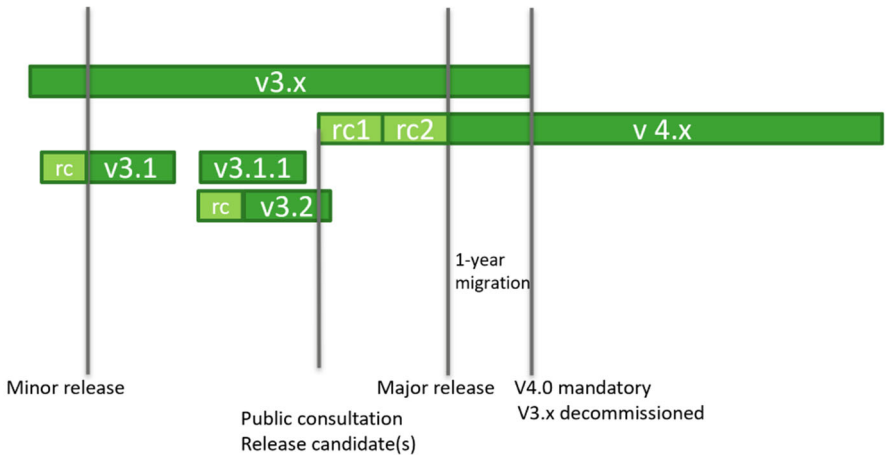


Figure 15 Simplified release scenario

The table below summarizes the process for a new major release. The process is similar for minor releases, only the throughput times are shorter. Errata releases can be published without first publishing a release candidate because of the urgent nature of the release. Finally, minor and errata releases do not require a recertification of the service providers.

Time (months)	Event	Description
M0	Workgroup initiated	The need of a new IDS version is identified and the corresponding workgroups are initiated and given the assignment to prepare a new version.
M6	First Release candidate published	A release candidate is published, which is a comprehensive set of all proposed changes to the old major release. This release candidate is published with the goal of collecting community feedback.
M10	Second Release candidate published	Multiple release candidates can be published.
M12	Major release approved	The major release has been approved by the Executive Board.
M12	Migration period started	The migration period of 12 months starts. During this period, Service Providers have to recertify their services based on the requirements of the new software version. The old version can still be used during the migration period.
M24	New version is ratified	The migration period has ended which means that the old version is now decommissioned and cannot be used anymore. All service providers should now be recertified and ready to use the new major release.

4.2.2.2 Change Management

Change Management concerns controlling the changes to the IDS components based on community feedback. Moreover, Change Management usually coincides with providing technical support, as this is where potential improvements, errors, and security risks are often identified.

The first section describes how changes are classified within the IDSA. Next, the change management process is described and, finally, the relation between Change Management and Version Management is described.

4.2.2.2.1 Types of Changes

Changes (or *issues* as they are called within Agile management frameworks) are classified according to its potential severity, i.e., the potential impact on the IDS community. There are three types of severity levels:

- **Critical issues** are highly urgent issues which might have a severe impact on the IDS standard and the IDS community as a whole. When an issue is classified as critical, it should be fixed as soon as possible. Therefore, an errata release is drafted in consultation with the corresponding workgroup and proposed within four weeks to the Steering Committee.

- **High issues** are changes which can have a significant impact on the IDS standard and community but do not require an immediate action. For this kind of issues, a change is proposed in consultation with the corresponding workgroup. A minor or Errata release is drafted which might contain other high/low priority changes. After a public consultation of a release candidate, the release is proposed to the Executive Board.

- **Low issues:** similar to high-priority issues but will not on its own result in a new releases. Low issues will be part of an already planned minor or major release.

4.2.2.2.2 Change Management Process

This section describes how changes are handled. The main actors in this process are: the IDS Support Organization, Steering Group, and the workgroups & taskforces.

1. An issue is raised by the community via a support ticket.

2. The support organization analyses the issue and identifies whether the issue is: (i) a question, (ii) a request for an already existing functionality, (iii) a request for new functionality, or (iv) a bug report.

    i. The support organization acts as a first support-line and tries to answer the question. If required, the issue is escalated to the Steering Committee (second support-line) who can escalate it to corresponding workgroup or taskforce (final support-line).

    ii. The support organization guides the issue author to the corresponding documentation. If required, a domain expert can be involved to answer the question.

    iii. The support organization classifies the issue as **critical, high,** or **low** and assigned to a workgroup or taskforce.

    iv. The support organization classifies the issue as **critical, high,** or **low** and assigned to a workgroup or taskforce.

3. The workgroups and taskforces together with the Steering Board prioritizes the issues.

4. The issue is handles by the workgroups and taskforces according to its severity as described in the previous section. The issue can result in an Errata release if urgent. A combination of issues can result in both a minor or major release.

5. The workgroup Chair proposes a new release to the Steering Committee. In the case of a minor or major release, this proposal is proceeded by a public consultation in the form of a release candidate.

6. In the case of an Errata or minor release, the Steering Committee can approve the release. In the case of a major release, the Steering Committee prepares an advice for the Executive Board. The Executive Board then asses the release and may formally approve the change.

7. New release is officially published including detailed Release Notes containing a description of all the changes, and the corresponding adoption policy of this release. Releases including critical changes are explicitly annotated.

8. Orchestration with Version Management

It is important to align the change and version management processes. The version management contains a clear regular plan of when releases are scheduled. The change management process is dependent on the community's input and is therefore highly dynamic. However, the issues raised in the change management process are the most valuable input for the content of the new releases. In order to align the processes, the following guidelines are required:

- The incoming issues are classified according to its severity and topic. The corresponding workgroup and taskforce decide, together with the Steering Committee, which issues to tackle in a new release.

- A minor and major release are proceeded by one or multiple release candidates. When the first release candidate has been published, a *feature freeze* for this new release will be announced, meaning that from this moment on the development on new features for this release is halted. The actual release itself may only contain additional bug fixes of the included features compared to its release candidates. This ensures that the community has sufficient time to evaluate the new release and integrating it.

- Issues identified by the workgroups and taskforces themselves are handled by the same process.

4.3 Service Level Agreements and Policies

4.3.1 Dynamic Attribute Provisioning Service (DAPS)

SLA and Policies for DAPS are not defined in Rule Book 1.0.

4.3.2 Participant Information Service (ParIS)

SLA and Policies for ParIS are not defined in Rule Book 1.0.

4.3.3 Certification Body

SLA and Policies for the Certification Body are defined in the Rules of Procedure[22].

4.3.4 Certificate Authority

SLA and Policies for CA are not defined in Rule Book 1.0.

4.3.5 Connectors

SLA and Policies for Connectors are not defined in Rule Book 1.0.

[22] https://industrialdataspace.jiveon.com/docs/DOC-2507

5 Legal Agreements

The previous sections of this IDSA Rule Book have addressed the needs relating to the management of the IDS standards and specifications, and the certification of implementations of the standard. The purpose of this section is to provide guidelines and best practices, endorsed by the International Data Spaces Association, on how organizations may define the rules and legal agreements for compliant collaboration.

International Data Spaces are fundamentally based on the premise of data sovereignty. Any organization deciding to use IDS in their operations can determine for themselves which specific data space they would like to adhere to, with whom they would like to share data, and where they would like their data to be used.

IDS is a functional framework that provides mechanisms to be customized by the participating organizations according to their requirements. While the IDS standards and specifications enable all participants to act in compliance with negotiated rules and processes, it does not make any restrictions or enforce predefined regulations on the use of IDS.

The need for legal agreements depends on the type of data space in question:

- Data marketplace is an environment facilitated by IDS where organizations make data available to be monetized through a financial transaction between any willing parties, facilitated by a clearing house. Legal agreements should be in place to address matters such as liability and cost/gain sharing related to the data being monetized.

- Data exchange refers to situations where IDS provides technical standards to exchange data between known parties in a seamless and interoperable manner. Benefits arise from improved business processes, for example through increased efficiency and new modes of collaboration. The parties typically have a Data Exchange Agreement in place as a bilateral contract between a Data Provider and a Data Consumer regarding the exchange of data. However, if there are more than two parties involved, a more comprehensive rulebook can be necessary.
- Data ecosystem is a data space based on the collaboration of multiple organizations forming a data sharing network. In such a context, IDS can be seen as a ‘plug & play’ implementation method to enable data sovereignty in a particular ecosystem. Such data spaces may adopt their own **data space specific rulebooks** that include the necessary multi-party legal agreements.

The rulebook creation and maintenance process in data ecosystems can be significantly simplified by having **rulebook templates** which organizations can use to setup a data space-specific rulebook.

IDSA sees significant benefits in implementing common elements of data sharing agreements and tailoring them to domain/company specific needs. This increases interoperability that extends beyond technical infrastructure to business, legal and ethical aspects. It also fosters cross-domain use of data across ecosystems.

IDSA recommends that these model rulebook templates use roles and terminology as defined in the IDS Reference Architecture Model. This would allow the specific data spaces to determine, for example:

- What are intermediary roles (broker, clearing house, etc.) required in the data space and who will be operating this for this specific data space?
- How organizations deal with certification?
- Which data access and usage policies should be adopted by the participants?
- Which vocabularies regarding semantics of data should be used?
- What are the liabilities of the participants?
- What is the governance structure of the data space?

As a general principle, data ecosystems should be fair, balanced, and lawful in their processing of data. They must also be just and impartial toward their members and ensure that the rights of third parties are not infringed.

iSHARE has developed a data sharing scheme[23] for logistics data ecosystem in The Netherlands. There is a named **scheme owner** that is an organization managing the rules and agreements. The relationship between the scheme owner and the participants in the scheme, is defined in terms of an accession agreement, and associated terms-of-use, ensuring the legal liabilities of parties in the data sharing scheme. Such liabilities can cover both the relationship between the scheme owner and the participant and the participants amongst each other, notwithstanding the ability of participants to make additional agreements. Participants can choose to adhere to these agreements and innovate their business models and practices accordingly, with data being a crucial enabler.

Sitra has provided a template called Fair Data Economy Rulebook[24] which can be used by organizations wanting to set up a data space ("Data Network" in Sitra's terminology). It considers business, legal, technical, and ethical aspects and covers topics such as roles and responsibilities and provides standardized templates for legal agreements. The Contractual Framework of the rulebook consists of the following parts:

- Constitutive Agreement
  - General Terms and Conditions
  - Governance Model
  - Accession Agreement
  - Dataset Terms of Use
- Description of the Data Network (i.e., Data Ecosystem)
  - Business Part
  - Technology Part

[23] iSHARE (https://www.ishareworks.org/)
[24] Sitra Fair Data Economy Rulebook (https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/)

These templates enable organizations to establish contractual frameworks for their data ecosystem. The participants must plan, design, and document their data ecosystem carefully by amending and supplementing the templates in a manner that best serves the purposes of the contractual framework they require.

6 Appendix

6.1 Notional conventions

The following font and symbols conventions are used in this document:

italic	Not used in this document
bold	Used to highlight terms.
Monospace	not used in this document
[item]	Not used in this document
{item|item}	Braces indicate that only one of the items listed between braces can be selected. A vertical bar (|) separates the items.
<item>	Placeholder

6.2 Related Documents

The references to documents that are related directly to the Rule Book are given in the text. Further relevant documents can be found on:

- the IDSA Homepage
  https://www.internationaldataspaces.org/ressource-hub/publications-ids/
  in different categories
- the IDSA internal collaboration platform Jive
  https://industrialdataspace.jiveon.com/
  which is organized in different spaces.
- the IDSA GitHub repositories:
  https://github.com/International-Data-Spaces-Association/
  where also relevant documents are listed
  https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/relevants
  and the listing of external relevant publications and sources
  https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/references

These sources are continuously updated.

6.3 Glossary

For terms and definitions IDSA provides a glossary on GitHub:

https://github.com/International-Data-Spaces-Association/IDS-G/tree/master/glossary

This document introduces the following new terms and definitions:

Base Services

Essential roles in the IDS are required to provide trust in the ecosystem, Base Services are required to improve usability of the system as a whole and raise the added value of Data Spaces. These roles should be enabled by key participants of the ecosystem. The following service are considered to be base services:

- IDS Meta-Data-Broker
- Clearing House
- App Store

Essential Services

The IDS-RAM defines a role model for Data Spaces. The roles for the provisioning of trusted identities are essential for the operation of Data Spaces:

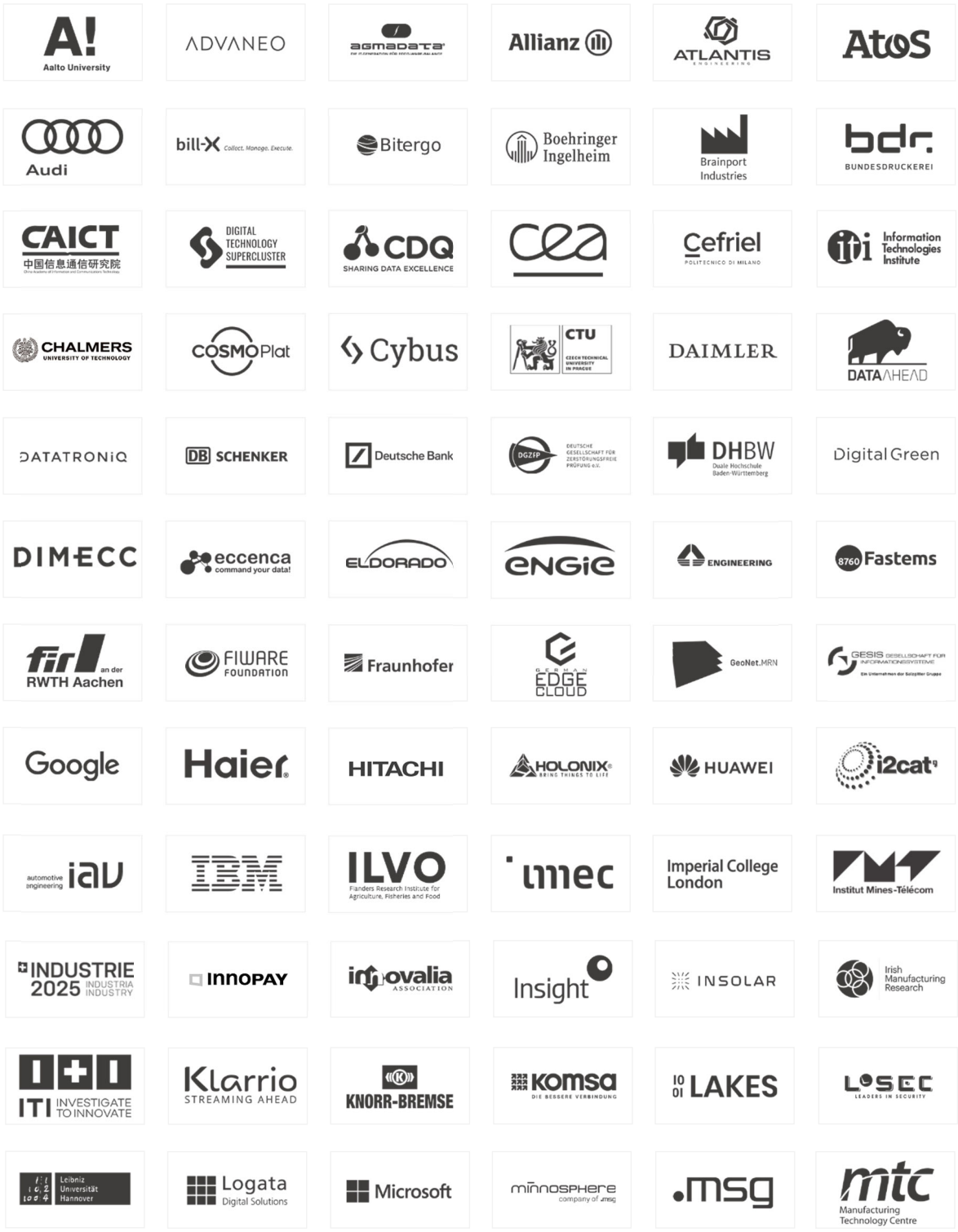
- Certification Body
- Certification Authority
- Dynamic Attribute Provisioning Service
- Participant Information System
- Dynamic Trust Management (DTM)

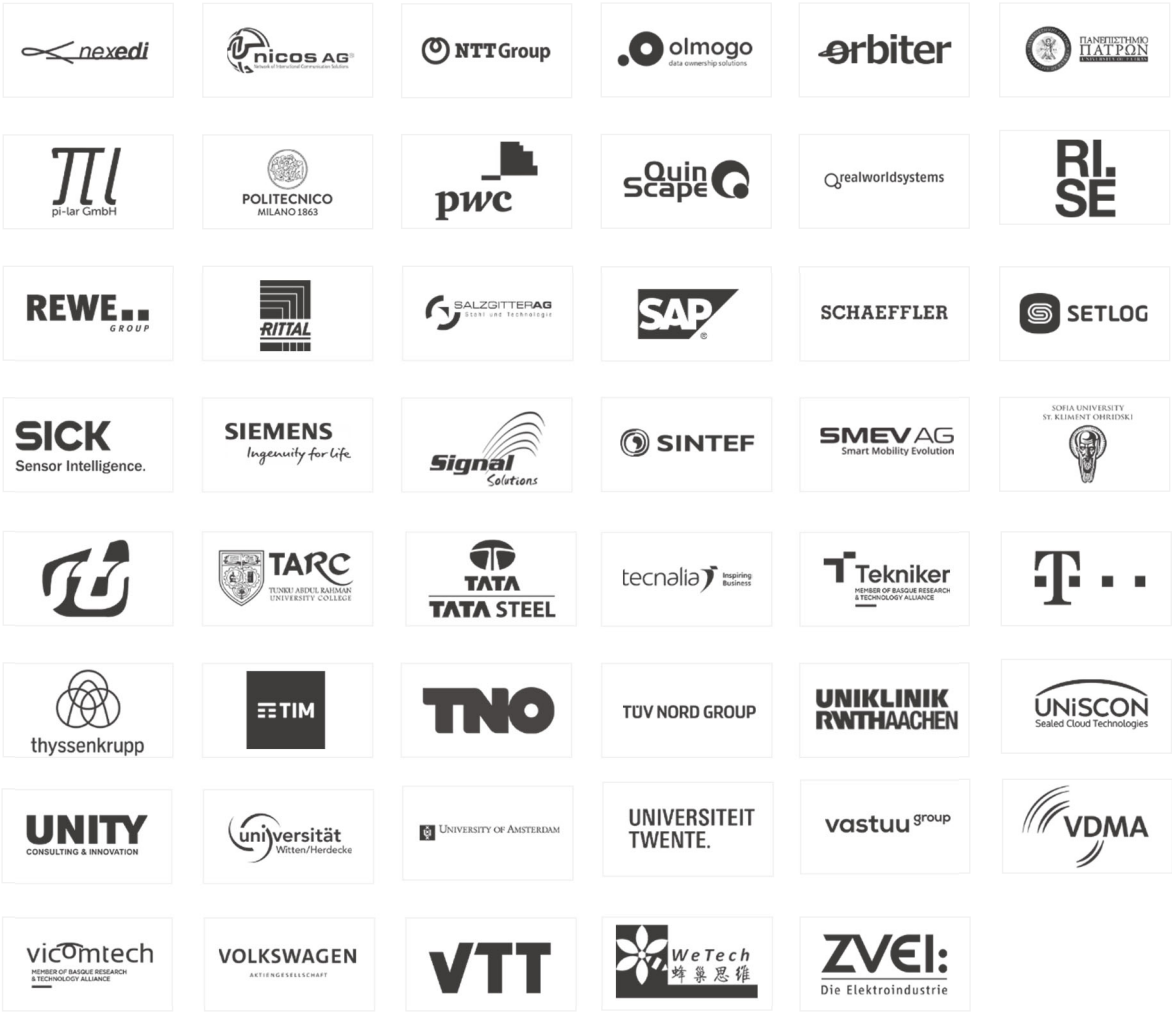
These roles must be operated and controlled in operational terms under the rules of procedure defined by the IDSA.

IDSA-SO
IDSA Support Organization

IDSA Support Organization
This entity is responsible for the orchestration of the essential services which will be provided by several provider companies which perform their service according to the IDS rule book and the right there provided rules of procedure.

OUR MEMBERS


Aalto University
ADVANEO
agmadata
Allianz
ATLANTIS
Atos
Audi
bill-X Collect. Manage. Execute.
Bitergo
Boehringer Ingelheim
Brainport Industries
bdr BUNDESDRUCKEREI
CAICT 中国信息通信研究院
DIGITAL TECHNOLOGY SUPERCLUSTER
CDQ SHARING DATA EXCELLENCE
cea
Cefriel POLITECNICO DI MILANO
iti Information Technologies Institute
CHALMERS UNIVERSITY OF TECHNOLOGY
COSMOPlat
Cybus
CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
DAIMLER
DATAAHEAD
DATATRONIQ
DB SCHENKER
Deutsche Bank
DGZfP DEUTSCHE GESELLSCHAFT FÜR ZERSTÖRUNGSFREIE PRÜFUNG e.V.
DHBW Duale Hochschule Baden-Württemberg
Digital Green
DIMECC
eccenca command your data!
ELDORADO
ENGIE
ENGINEERING
8760 Fastems
fir an der RWTH Aachen
FIWARE FOUNDATION
Fraunhofer
GERMAN EDGE CLOUD
GeoNet.MRN
GESIS GESELLSCHAFT FÜR INFORMATIONSSYSTEME
Google
Haier
HITACHI
HOLONIX BRING THINGS TO LIFE
HUAWEI
i2cat
automotive engineering iav
IBM
ILVO Flanders Research Institute for Agriculture, Fisheries and Food
imec
Imperial College London
Institut Mines-Télécom
INDUSTRIE 2025 INDUSTRIA INDUSTRY
INNOPAY
innovalia ASSOCIATION
Insight
INSOLAR
Irish Manufacturing Research
ITI INVESTIGATE TO INNOVATE
Klarrio STREAMING AHEAD
KNORR-BREMSE
komsa DIE BESSERE VERBINDUNG
LAKES
LSEC LEADERS IN SECURITY
Leibniz Universität Hannover
Logata Digital Solutions
Microsoft
minnosphere company of .msg
.msg
mtc Manufacturing Technology Centre

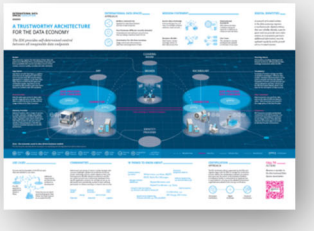

nexedi
nicos AG
NTT Group
olmogo
data ownership solutions
orbiter
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
pi-lar GmbH
POLITECNICO MILANO 1863
pwc
QuinScape
realworldsystems
RI. SE
REWE GROUP
RITTAL
SALZGITTER AG
SAP
SCHAEFFLER
SETLOG
SICK
Sensor Intelligence.
SIEMENS
Ingenuity for life
Signal Solutions
SINTEF
SMEV AG
Smart Mobility Evolution
SOFIA UNIVERSITY
ST. KLIMENT OHRIDSKI
TARC
TUNKU ABDUL RAHMAN UNIVERSITY COLLEGE
TATA
TATA STEEL
tecnalia
Inspiring Business
Tekniker
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
T
thyssenkrupp
TIM
TNO
TÜV NORD GROUP
UNIKLINIK RWTH AACHEN
UNiSCON
Sealed Cloud Technologies
UNITY
CONSULTING & INNOVATION
universität
Witten/Herdecke
UNIVERSITY OF AMSTERDAM
UNIVERSITEIT TWENTE.
vastuu group
VDMA
vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
VOLKSWAGEN
AKTIENGESELLSCHAFT
VTT
WeTech
蜂巢思维
ZVEI:
Die Elektroindustrie

OVERVIEW PUBLICATIONS

Reference Architecture Model

Executive Summary

Image Brochure



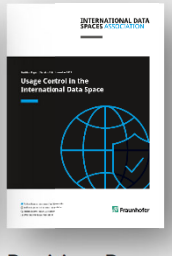
Infographic

Use Case Brochures

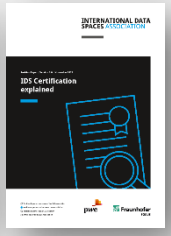
Study on Data Exchange

Position Paper Implementing the European Data Strategy

Position Paper GDPR Requirements and Recommendations



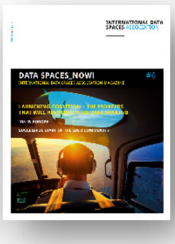
Position Paper Usage Control in the IDS



Position Paper IDS Certification 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

international-data-spaces-association