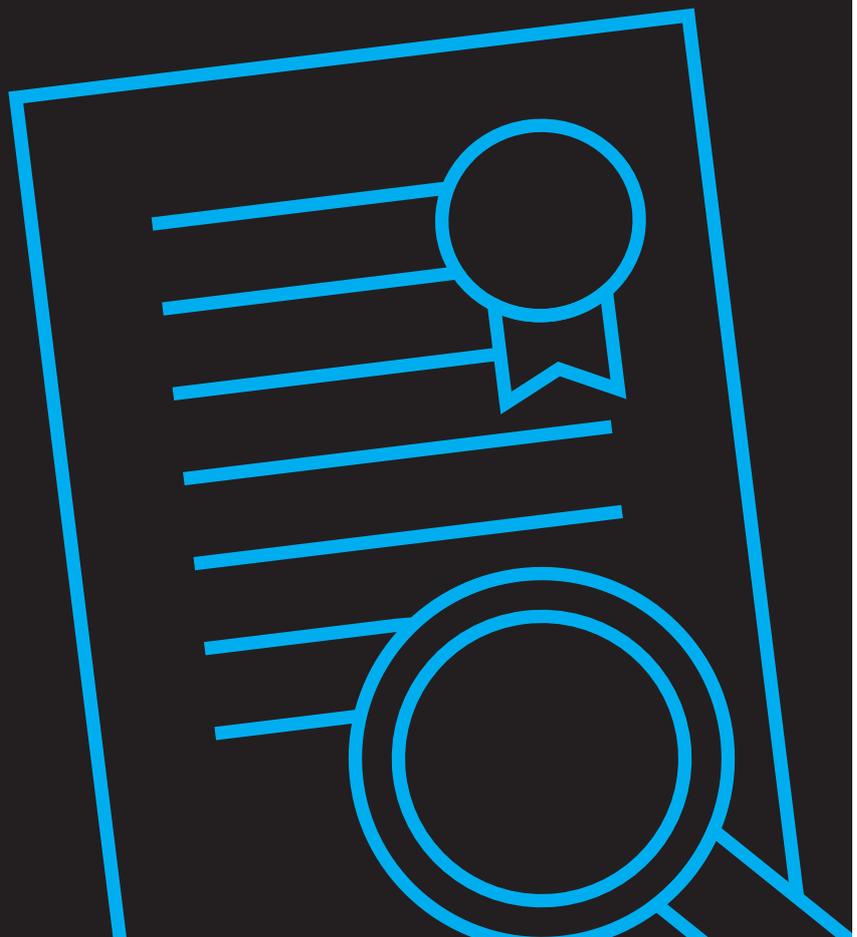




Position Paper | Version 1.0 | November 2019

IDS Certification explained



- 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

Nadja Menz, Fraunhofer FOKUS
Aleksi Resetko, PrivewaterhouseCoopers
Jonas Winkel, PrivewaterhouseCoopers

Copyright

International Data Spaces Association, Dortmund 2019



Cite as

Steinbuss S., Menz N., Resetko A., Winkel J. (2019):
IDS Certification explained. International Data Spaces
Association.
<https://doi.org/10.5281/zenodo.5675945>



Preamble

The Certification of the International Data Space is of fundamental importance for IDS and one of its core components.

Certification in general provides a very high degree of transparency. This transparency is achieved by making the requirements for the auditee and the auditors and the complete certification process available for public. The transparency is also key for the main goal of certification: Trust. Trust is the basis for a successful collaboration between partners, in business as well as in social life. Due to the importance of collaboration for the IDS, certification works as an enabler for business and use cases. Collaboration is the basis for the IDS itself and therefore, it is necessary to establish trust by certification between the partners in IDS.

Certification is providing this trust by ensuring the security for everyone in a transparent way. Security is and will always be relative, but certification defines a standardized level for security related to technical and organizational aspects.

The IDS needs this trust through certification. Therefore, IDS Certification is tailor-made for the specific IDS context. This IDS Certification is compatible with commonly used security standards like ISO 27001 and IEC 62443, so existing documentations and setups for the achieved certifications can be re-used in IDS. This minimizes the effort during IDS certification process for the organizations involved.

The IDS is a heterogeneous environment with different business models and IDS use cases. For this reason, the IDS Certification has a flexible setup and provides different levels of certification according to the intended use cases. In order to build such a customized IDS Certification, various stakeholders have been involved during the development.

To sum it up, IDS Certification is customized for the special conditions in the IDS context and provides the basis for the IDS: Trust.



Aleksei Resetko
Chairman of the IDSA Working Group Certification



IDS Certification Explained

The purpose of this paper is to present the IDS Certification Scheme in a short and comprehensible form. The paper will outline the different evaluation levels, certification criteria and the major steps of a certification process from the point of view of the applicant.

1. Introduction

The International Data Space is a virtual data space leveraging existing standards and technologies, as well as accepted governance models. It enables the secure exchange and easy linkage of data in a trusted business ecosystem.

Data security and trust are two fundamental characteristics of the International Data Space. This paper presents a brief overview of the approach to participant and core component certification within the International Data Space to ensure this two corner stones of the IDS.

Participants and core components shall provide a sufficiently high degree of trust and security regarding the integrity, confidentiality and availability of information exchanged in the IDS. Therefore, using certified core components as well as employing certified technical and organizational security measures is mandatory for participating in the Industrial Data Space.

2. Participant Certification

The participants of the IDS will collaborate by sharing their valuable data. Trust be-

tween all parties involved in this data exchange is absolutely necessary for the success of the IDS.

Evaluating participants regarding their fulfillment of the defined levels of security, including infrastructure reliability and process compliance, can achieve this trust. Therefore, the certification of one participant demonstrates a level of security regarding availability, confidentiality and integrity to all other participants and stakeholders.

The participant certification approach is displayed by two dimensions: The horizontal dimension is Evaluation Depth, describing the level of detail at which an evaluation is performed. The vertical dimension is the increasing extent of the Security Requirements that need to be fulfilled (see Figure 1).

Evaluation Depth

A **Self-Assessment** is a mere self-declaration by the prospective organization in order to clarify the participant's identity and the provisioning of information about their management systems. No evaluation facility is involved in a self-assessment.

The evaluation of the participants **Management System** is the first level at which an

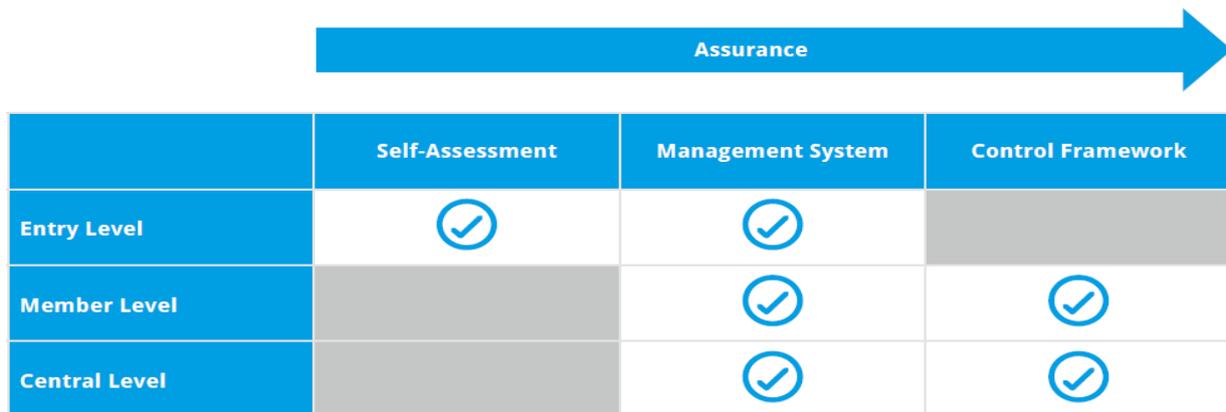


Figure 1: Certification Approach for participants of the International Data Space

evaluation is performed. This evaluation involves analysing whether the applicant has defined a management system and whether the applicant is actively working in accordance to the defined management system.

The highest level of evaluation is the analysis of the **Control Framework**. This evaluation contains not only the review of the management system but also the evaluation of the operational effectiveness of the management system.

Security Requirement Extent

The **Entry Level** covers only the basic security requirements that every participant of the International Data Space needs to fulfil. The entry level therefore serves as a low barrier for companies (especially SMEs) interested in trying out International Data Space participation.

The **Member Level** covers additional security requirements, ensuring an advanced level of security. This level is suitable for most core participants.

The **Central Level** includes special security requirements that are necessary for International Data Space participants providing key services within the International Data Space.

Certification Criteria Catalogue

The participant certification approach is designed to allow the reuse of existing certificates obtained through compliance with other certification schemes, standards, and norms for organizations.

In the following, some example criteria from the participant certification catalogue are presented.

Asset Management

- Media shall be disposed of securely when no longer required, using formal procedures.
- Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

Identity and Access Management

- Asset owners shall review users' access rights at regular intervals.
- The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.



Physical Security

- Security parameters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
- Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

3. Core Components Certification

To secure the intended cross-industrial and cross-company information exchange, the International Data Space core components must provide the required functionality and an appropriate level of security. As such, the core component certification is interoperability- and security-focused, while aiming to strengthen the development and maintenance process of these components.

The component certification approach is displayed by two dimensions: The depth and rigor of an evaluation increases with each of the three defined **Assurance Levels**. Similarly, the security needs required by the data owner and data consumer for data exchange, increase with the three defined **Security Profiles** (Figure 2).

Assurance Level

Checklist Approach

With the **Checklist Approach**, the core component must fulfil security features as defined by a checklist. The developer of the component validates the claims made about the implementation. Additionally, an automated, standardized test suite will be used to verify the component's security features. No evaluation facility is involved in this process.

During a **Concept Review**, an in-depth review by an International Data Space evaluation facility is performed. The review includes an evaluation of the provided concept as well as practical functional and security tests.

For a **High Assurance Evaluation**, in addition to the functional and security tests, the vendor must provide the source code of all security relevant components and an in depth source code review will be performed by an evaluation facility. Furthermore, the development process will be evaluated, including an audit of the development site.

Security Profiles

The **Base Security Profile** offers basic security features to protect against attackers from outside, to ensure integrity and availa-

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

Figure 2: Certification Approach for core components of the International Data Space



bility. It is therefore designed for use in scenarios with only low security requirements. A Connector meeting this profile is suitable for exchanging data with limited trust and security needs, for exchange of data in a contained environments (e.g. a VPN) or for demonstration purposes.

The **Trust Security Profile** includes strict container isolation, integrity-protected logging, encryption of all persisted data, protection against accidental misuse by administrators. This profile is used for scenarios in which the protection of the processed and transmitted data is essential.

In comparison to the Trust profile, the **Trust+ Security Profile** also offers additional protection against misuse of privileged access, i.e. manipulation by administrators. This includes the protection against insider attacks as well as against external attackers who could gain privileged access. This is achieved by actively monitoring users and data on behalf of the data owner.

Certification Criteria Catalogue

The catalogue of certification criteria for the IDS core components is split into three thematic sections, i.e. IDS-specific requirements, functional requirements taken from ISA/IEC 62443-4-2 and best practice requirements for secure software development.

- The IDS-specific requirements aim to evaluate the Core Component's conformity to the IDS Reference Architecture Model, both in regard to functionality as well as security.
- The requirements taken from ISA/IEC 62443-4-2 target the implemented functionality and security measures.

- To round off the catalogue, the best practice requirements for secure software development aim to evaluate the security of the processes during the development of the component.

In the following, some example criteria from the component certification catalogue are presented.

IDS-Specific

- All Connectors in the IDS must be compatible with each other, i.e. support the initial handshake and implement the minimum protocols defined in the IDS Reference Architecture.
- A Connector must self-disclose information about itself when self-information is requested by another IDS component.

62443-4-2

- The component shall provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.
- If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

Secure Development

- The development documentation shall include a design description stating the structure of the entire component in terms of subsystems.
- The configuration management access control measures shall be automated and effective in preventing unauthorised access to the configuration items.

How To: IDS Certification Process

Participants and core components within the IDS ecosystem shall provide sufficiently high degree of security regarding the integrity and confidentiality of the data being processed in the IDS. Therefore, a certification of participants and core components is mandatory. Involved partners are the applicant, evaluation facility and the certification body.

The certification process is divided into the following three stages:

1 THE APPLICATION STAGE

The main goal of this stage is the successful start of the IDS certification process. It starts with the applicant triggering the certification process. The applicant must contact an approved evaluation facility to carry out the evaluation according to the IDS certification schema. The choice of the evaluation facility lies with applicant. The applicant must provide the necessary evidence for the certification body to confirm the application. If the applicant is accepted, the evaluation procedure will be opened and there will be a Kick-Off with all involved partners.

IDS_Ready evaluators: www.internationaldataspaces.org/the-principles/evaluation-facilities

Contact email: certification@internationaldataspaces.org

2 THE EVALUATION STAGE

The main goal of this stage is the evaluation of a participant or IDS core component based on the defined certification criteria. The evaluation facility is responsible for carrying out the detailed technical and / or organizational evaluation work during the certification.

The evaluation facility documents the detailed results in an evaluation report. If deviations have been identified, implementing the corrective actions is the responsibility of the applicant.

Afterwards, a re-examination is necessary. The evaluation is monitored by the certification body to ensure the correct implementation and execution of the IDS certification scheme.

Certification Criteria – Participants: <https://industrialdataspace.jiveon.com/docs/DOC-1799>

Certification Criteria – Components: <https://industrialdataspace.jiveon.com/docs/DOC-2223>

3 THE CERTIFICATION STAGE

The main goal of this stage is the examination of the evaluation report by the certification body as well as the process for issuing the certificate if the result is positive.

The certification body receives the evaluation report from the evaluation facility and is responsible for the final decision about the award or denial of the certificate. If the decision is positive, the applicant will be confirmed as being IDS compliant. The certification body issues the certificate.

Requirements for IDS Evaluation Facilities: <https://industrialdataspace.jiveon.com/docs/DOC-1710>

Whitepaper: <https://bit.ly/2IIRo5z>

Webinar on YouTube: <https://bit.ly/2kBAG5>

Related Documents



IDS Reference Architecture Model Version 3.0
April 2019



White Paper Certification Version 2.0
April 2019



IDSA Webinar: Trust in the IDS-based on the certification of participants and components
January 2019



IDS Certification: Criteria for Participants
(internal)



IDS Certification: Criteria for Core Components
(internal)



IDS Certification: Code of Conduct
(internal)



IDS Certification: Approval Scheme for Evaluation Facilities
(internal)

For publications: www.internationaldataspaces.org/ressource-hub/publications-ids

For internal documents: <https://industrialdataspace.jiveon.com/community/idsa-homepage>

OUR MEMBERS





OVERVIEW PUBLICATIONS



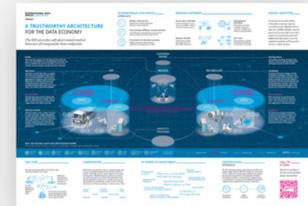
Reference Architecture Model



Executive Summary



Image Brochure



Infographic



Use Case Brochures



Study on Data Exchange



Position Paper Implementing the European Data Strategy



Position Paper GDPR Related Requirements and Recommendations



Position Paper Usage Control in the International Data Space



Position Paper IDS Certification Explained



White Paper Certification



White Paper Sharing data while keeping data ownership



Magazine Data Spaces_Now!

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

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

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

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

WWW.INTERNATIONALDATASPACES.ORG

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

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