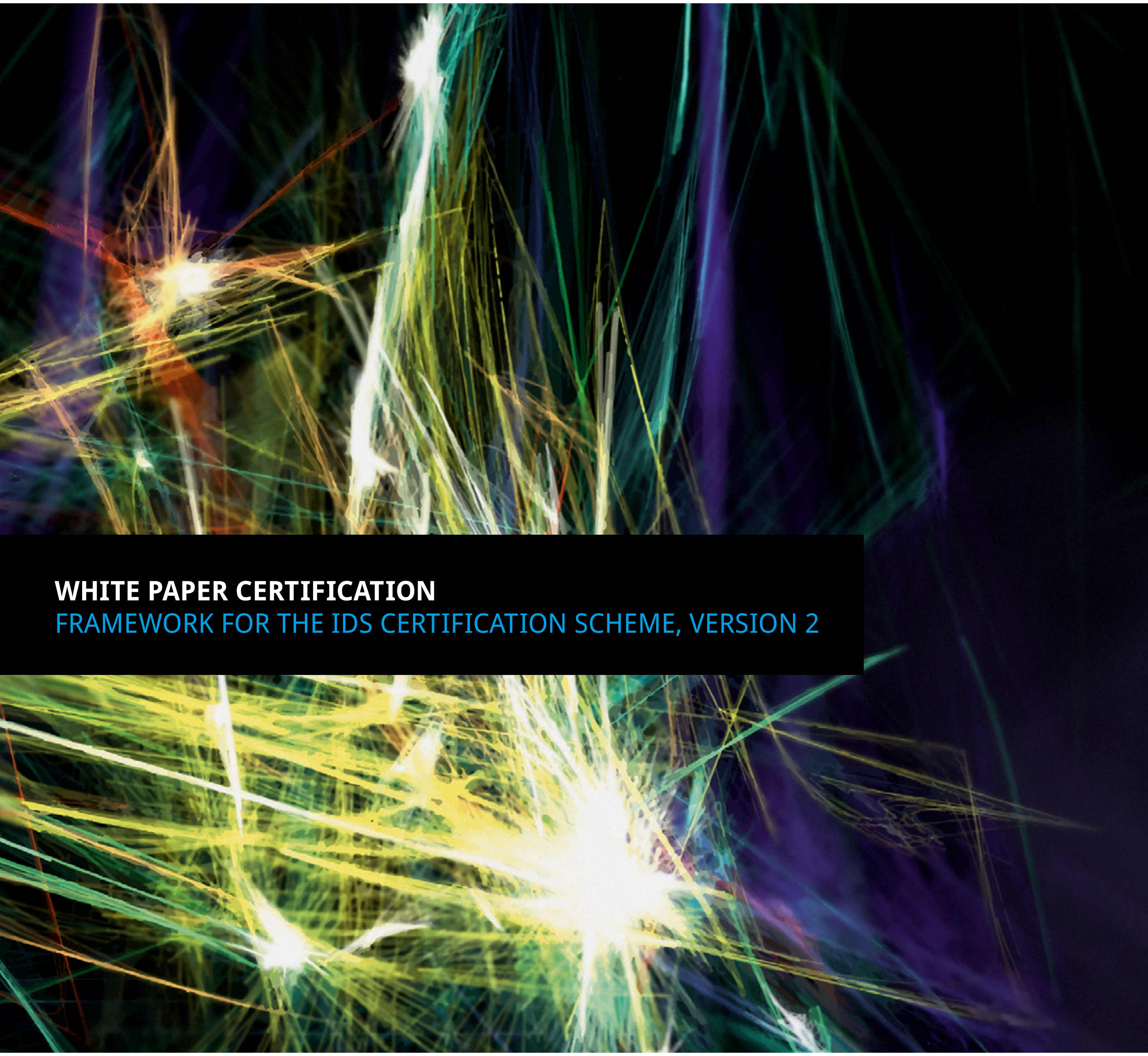
INTERNATIONAL DATA SPACES ASSOCIATION



WHITE PAPER CERTIFICATION

FRAMEWORK FOR THE IDS CERTIFICATION SCHEME, VERSION 2

Fraunhofer Cybus GESIS GESELLSCHAFT FÜR INFORMATIONSSYSTEME A Member of the Salzgitter Group KOMSA pwc SICK Sensor Intelligence. TÜV NORD GROUP

Publisher

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

Editor

Sebastian Steinbuss, International Data Spaces Association

Contributing Projects

Industrial Data Space

Industrial Data Space+

Research Center Data Spaces

www.fraunhofer.de/en/research/lighthouse-projects-fraunhofer-initiatives/industrial-data-space.html

www.cit.fraunhofer.de

Authors & Contributors

Nadja Menz, Fraunhofer FOKUS

Aleksei Resetko, PwC

Prof. Dr. Boris Otto, Fraunhofer ISST

Markus Bartsch, TÜViT

Dr. Anja Beyer-Peters, T-Systems

Thilo Ernst, Fraunhofer FOKUS

Thomas Fedkenhauer, PwC

Dr. Burkhard Heisen, Cybus

Mustafa Ipekcioglu, PwC

Prof. Dr. Jan Jürjens, Fraunhofer ISST

Stefan Kistler, TÜV NORD

Dr. Ralf-Peter Simon, KOMSA Group

Gerrit Stöhr, GESIS

Andreas Teuscher, SICK

Sascha Wessel, Fraunhofer AISEC

Jonas Winkel, PwC

Digital Object Identifier

https://doi.org/10.5281/zenodo.5244858

CONTENT

INTRODUCTION

The Industrial Data Space is a virtual data space leveraging existing standards and technologies, as well as accepted governance models, to facilitate the secure exchange and easy linkage of data in a trusted business ecosystem. The Industrial Data Space is an initiative that is institutionalized by two main activities: the Fraunhofer research projects »Industrial Data Space« and »Industrial Data Space Plus« as well as the »International Data Spaces Association«. While the research projects are concerned with the design and implementation of the Reference Architecture Model, the IDSA unites the requirements from various industries and provides use cases to test the results gained from its implementation.

Data security and data sovereignty are the fundamental characteristics of the Industrial Data Space. Data sovereignty is a natural person's or legal entity's capability of exclusive self-determination with regard to their data goods. Participants within the Industrial Data Space must therefore use certified software (e.g., the »Industrial Data Space Connector«) in order to securely exchange data in a sovereign way. Furthermore, data is only exchanged if the exchange takes place between trustworthy and certified participants. This document therefore presents the approach to participant and core component certification within the Industrial Data Space.

The Industrial Data Space certification scheme encompasses all processes, rules and standards governing the certification of participants and core components within the Industrial Data Space. The purpose of this document is therefore to present the framework for the scheme's structure, processes, evaluation levels and criteria catalogues as defined by the Working Group Certification of the International Data Spaces Association. As such, this paper illustrates the core of our ambition for crafting a flexible and cost-effective certification scheme. As this is a work in progress, adjustments to the certification scheme may be made in the future and published in updated versions of this document.

PART 1 - CERTIFICATION FRAMEWORK

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

This requirement for compliance necessitates the definition of a framework in order to ensure a consistent and comparable evaluation and certification process amongst all Industrial Data Space participants and core components. Hence, a certification scheme has been defined following best practices from other internationally accredited certifications. All certification-related roles described in this paper are specific to the Industrial Data Space, i.e. terms such as "Certification Body" should not be misunderstood to refer to an existing organization already granting certificates. As part of the scheme implementation in 2018, the roles defined here will be assigned to actual organizations.

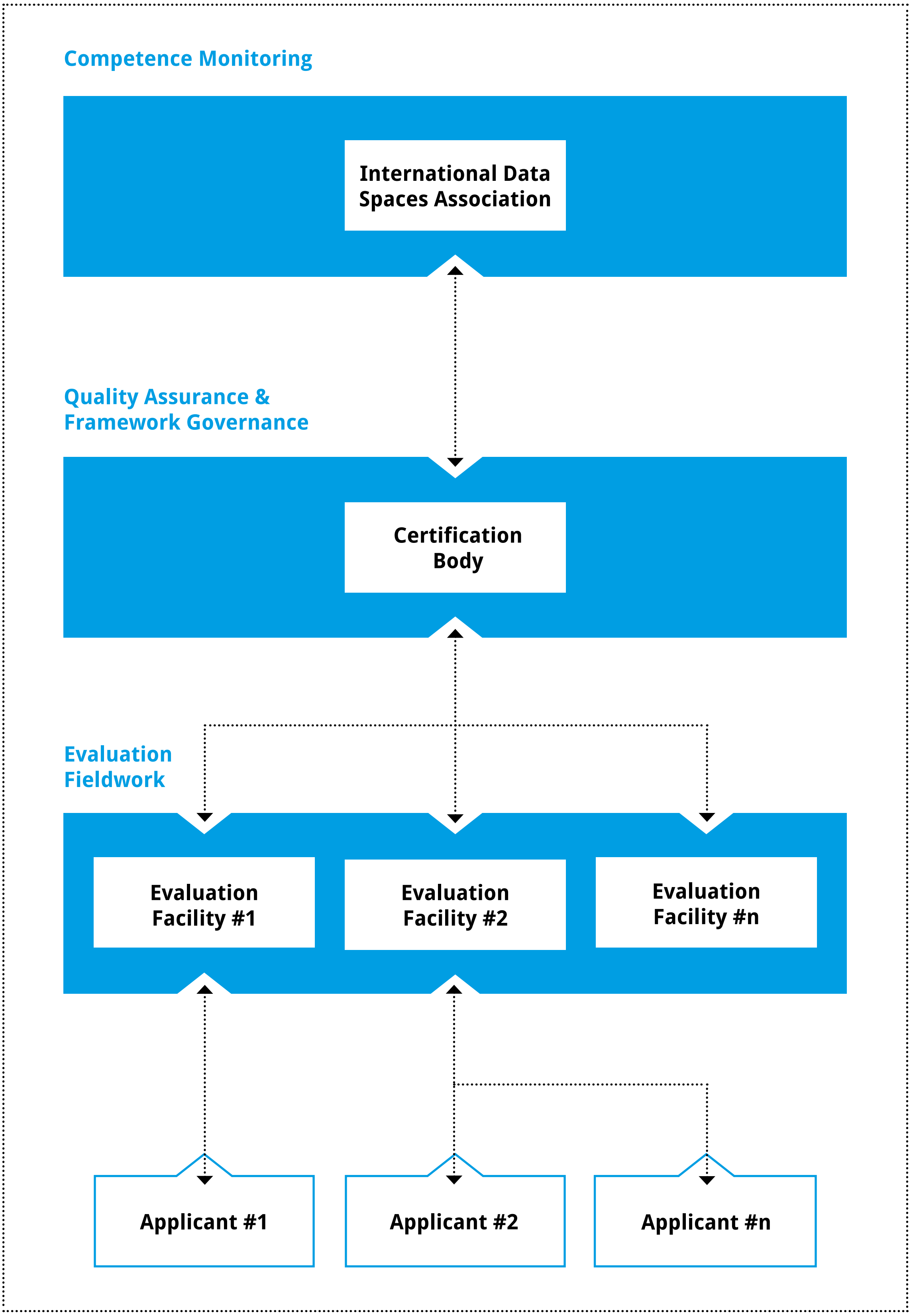


Figure 1: Industrial Data Space Certification - Roles & Responsibilities

The Industrial Data Space initially originated as a German research initiative. Nevertheless, the initiative driven forward by the International Data Spaces Association (IDSA) always had a wider scope in mind, by addressing more and more international members and component developers, as the initiative keeps growing. As such, the initial development of operation of the Industrial Data Space certification scheme will mainly be led by German IDSA members. However, for a future internationalization of the IDS certification, a two-phase process has been designed:

- Phase 1 - Increasing number of international members and developers:
  To ensure an economically sound and from the applicant's point of view, sufficiently accessible certification, the evaluation step of a certification will be conducted by an evaluation facility located in the applicant's country of residence. The certification step, carried out by the Certification Body, together with the approval of international evaluation facilities, however will remain located solely within a single entity. This aims to ensure that the overall framework governance for the certification scheme stays manageable.

- Phase 2 - Increasing overall number of members and developers:
  At this stage, individual certification bodies in the member countries will be commissioned in order to avoid a bottleneck situation, arising from a single certification body. As such, both the evaluation and the certification will be conducted by organizations located in the applicant's country of residence. Once this happens, mutual control processes must be established to ensure that the evaluation and certification processes are equivalent in all member nations. This will be a prerequisite for mutually recognizing the IDS certificates issued by the other nations. These costly measures will be justified, once a substantial market position for the Industrial Data Space in a number of nations has been reached.

International Data Spaces Association

The International Data Spaces Association appoints the IDS Certification Body.

Its responsibilities in the context of the certification scheme include:

- Definining the requirements for the Certification Body and verification of the required technical competencies.
- Monitoring of the Certification Body to ensure a consistent level of quality for the certification of Industrial Data Space participants and core components.
- Monitoring of the current regulatory and legal requirements to evaluate and react to possible influences to the certification scheme.
- Provisioning of recommendations to the Certification Body based on the results of its monitoring activities.
- Continuous improvement of the defined certification scheme including the incorporation of the feedback provided by the Certification Body.

The IDSA is not actively involved in a participant or core component certification and the approval of Evaluation Facilities for performing Industrial Data Space evaluations.

Certification Body

The IDS Certification Body is appointed by the International Data Spaces Association and regularly aligns with the IDSA to manage the certification process, defines the standardized evaluation procedures and supervises the actions of the Evaluation Facilities.

Its responsibilities include:

- Formulating and defining the certification scheme in cooperation with the International Data Spaces Association, including the evaluation procedures, participant and core component certification approaches as well as their underlying criteria catalogues.

- Ensuring correct implementation and execution of the Industrial Data Space certification scheme, including the supervision of ongoing evaluations.
- Ensuring continuous adherence to the Industrial Data Space certification scheme following up on changes und updates received from the IDSA.
- Analyzing existing “base” certificates (e.g. for organizations or for software and hardware security components) to determine their validity and sufficiency, and deciding about their acceptance within the Industrial Data Space certification scheme.
- Reviewing and commenting on the evaluation reports received from Evaluation Facilities.
- Approval of applications for certification.
- Making final decision about the award or denial of a certificate and publishing the awared certificates.
- Authorization/triggering of the generation and revocation of a X.509 certificate. These certificates digitally represent the evaluation certificate and enable automated trust checks between partners prior to data transfer within the Industrial Data Space.
- Decision about approval or exclusion of Evaluation Facilities for/from executing Industrial Data Space evaluations (based on ongoing monitoring and [CRIT-EF]).
- Ongoing monitoring of certification-relevant external developments (e.g. new attack patterns which might circumvent certified security measures).
- Providing input based on the practical quality assurance experiences to future updates of the Industrial Data Space certification scheme to the International Data Spaces Association.

The Certification Body only grants the certificate (called evaluation certificate subsequently) only if both the Evaluation Facility and the experts of the Certification Body have come to the conclusion that all preconditions are fulfilled.

Evaluation Facility

An Evaluation Facility is contracted by an Applicant and is as such responsible for carrying out the detailed technical and/or organizational evaluation work during a certification. The Evaluation Facility issues an evaluation report for the participant or core component, listing details regarding the performed evaluation actions as well as information regarding the confirmed security level. The depth and scope of the performed evaluation actions depend on the desired level of security. These security levels are specified in more detail in Part 2 and 3 of this document.

The responsibilities of the Evaluation Facility include:

- Obtaining approval by the Certification Body to perform evaluations, based on an approval process with criteria defining personnel competencies and organizational requirements [CRIT-EF].
- Applying the criteria specified in the Industrial Data Space certification scheme according to generally accepted standards and best practices (including the execution of any necessary tests and on-site checks).
- Documenting the results in an evaluation report.
- Providing the evaluation report to the Certification Body.

The term Evaluation Facility is used throughout the document to refer both to authorized auditors for management system evaluations (i.e., participant certifications), as well as approved evaluators for product evaluations (i.e., core component certifications). Hence, multiple approved Evaluation Facilities will exist in the Industrial Data Space certification scheme, but in each evaluation only one Evaluation Facility will be involved.

The flexibility of the certification approaches defined in Part 2 and 3 of this document allows for a wide range of evaluation experts to participate in the Industrial Data Space certification scheme, such as software penetration testers, common criteria specialists, ISO 27001 auditors and accounting firms. As such, it is fully expected that all certification levels defined in this document and therefore the needs of startup companies and SMEs as well as those of large corporations will be sufficiently addressed.

Applicant

The Applicant plays an active part in the certification process. As such, the responsibilities of the respective organization include:

- Contract an approved (by the Certification Body) Evaluation Facility to carry out the evaluation according to the Industrial Data Space certification scheme.
- Formally apply for certification (with the Certification Body) in order to trigger the start of the certification process.
- Provide the necessary resources in terms of financing and personnel.
- Communicate swiftly with and provide all necessary information and evidence to the Evaluation Facility and the Certification Body.
- React adequately to findings occurring during the course of the evaluation.

All Applicants need to actively submit an application to start the certification process and have the duties as listed above. This applies to both organizations that develop software components intended to be deployed within the Industrial Data Space (i.e., prospective software providers) and to organizations that intend to become participants in the Industrial Data Space. During the certification process, the primary focus of the evaluation will be either on the product or on the organization itself.

Identity Provider

The Identity Provider creates, maintains and verifies technical identities for the applicant. This happens by using technical X.509 certificates that are not directly related to the certificates described in this paper. Technical identities associate attributes to entities. This happens when a certification level is assigned to an Applicant or a component. Central records for membership status and issued certifications are kept by the IDSA and are modelled into technical identities (e.g., by handing out X.509 certificates or attribute tokens to verify dynamic attributes for entities). So the Identity Provider asserts identity attributes towards other entities and verifies the validity of issued technical certificates. Examples for attributes might be

- Organizational certification status
- Expiry data of a certification status
- Connector security level

These attributes can be used for access & usage control decisions. For more information on identity management in the Industrial Data Space, see the IDS Reference Architecture Model [IDSRA, 4.1.3].

Issuance of Certificates

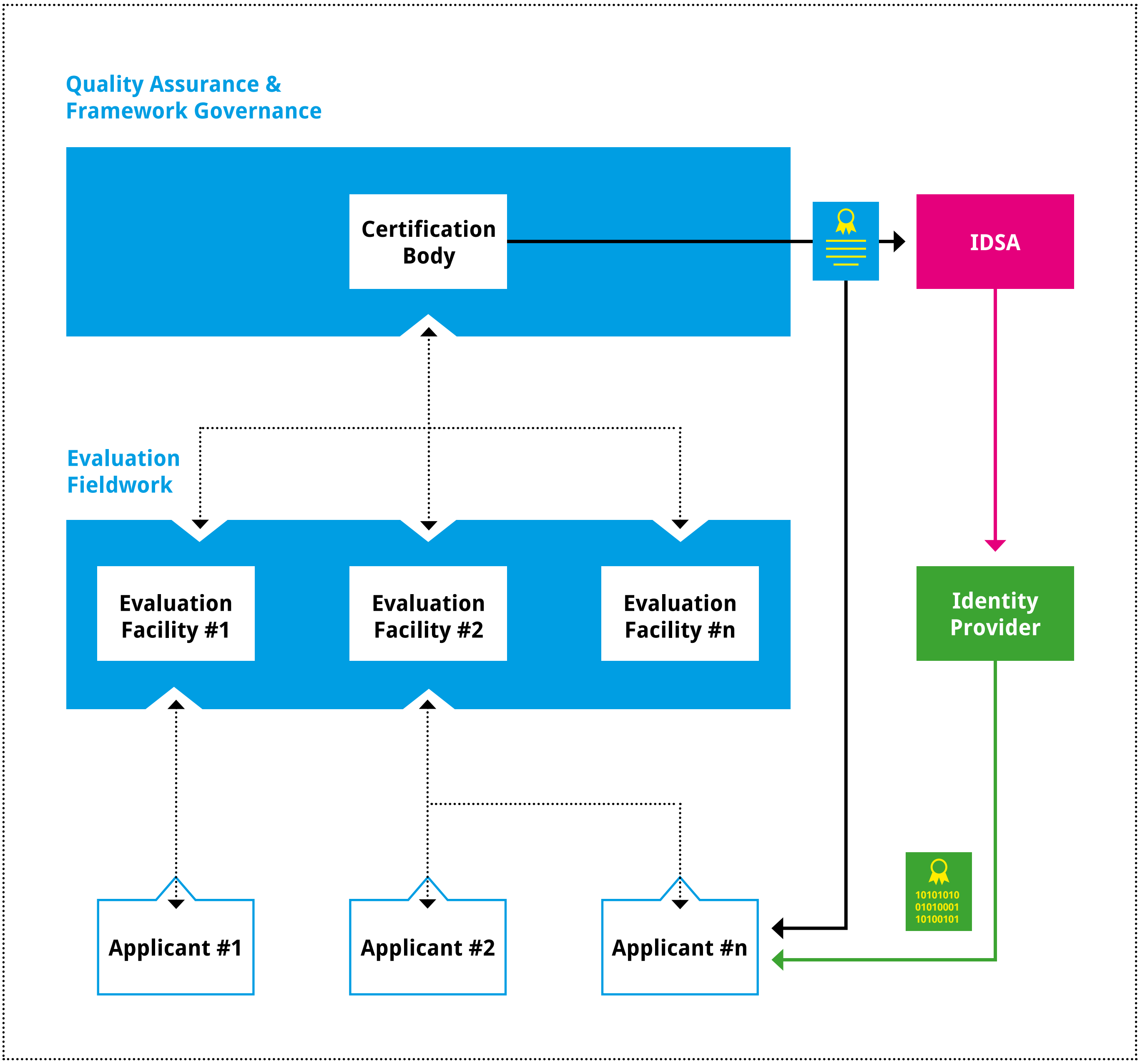


Figure 2: Industrial Data Space Certification – Issuance of Certificates

After a successfully completed evaluation, the Certification Body awards an Industrial Data Space evaluation certificate to the applicant. These certificates will have a limited validity period. In order to renew a certificate before it expires, a re-certification is required, taking into account any relevant external developments that have happened in the meantime. Similarly, re-certification is required if changes are made to the target of certification; in case of minor changes, "lightweight", low-cost re-certification may be sufficient. The definition of major and minor changes will follow the definition used within widely accepted certification standards such as ISO 27001.

For authentication and authorization, each IDS component must have a valid X.509 certificate, in order to verify the identity of other participants. These technical certificates digitally represent the evaluation certificate and enable automated trust checks between partners prior to data transfer within the Industrial Data Space. Upon a successful certification of an organization, such a technical certificate is issued to the organization to confirm certain attributes like organizational name, certification status, etc. This technical certificate can be used to trigger processes such as applying for X.509 connector certificates.

PART 2 - PARTICIPANT CERTIFICATION

One of the Industrial Data Space goals is to evolve towards a global de-facto standard for cross-industrial and cross-company information exchange. Therefore, a low financial and procedural barrier to join the Industrial Data Space is inevitable. It must therefore be ensured that participants of the Industrial Data Space fulfill a certain level of security in order to comply with the security requirements set by the Industrial Data Space.

The participants of the Industrial Data Space will collaborate by sharing their valuable information and data. Trust between the involved participants is necessary for such a collaboration. Furthermore it is essential for the Industrial Data Space and its reputation that the participants are trustworthy. This trust can be achieved by evaluating participants regarding their fulfilment of the defined levels of security, including infrastructure reliability and process compliance. To build this trust in a structured and ongoing way the Industrial Data Space established a well-defined process for participant certification.

This participant certification is based on established certification standards and methods, as described in the following chapter Certification Criteria Catalogue. Therefore the certification of one participant demonstrates a level of security regarding availability, confidentiality and integrity to all other participants and stakeholder. So the process for participant certification as described below is building the necessary trust in the participants of the Industrial Data Space.

To ensure on the one hand a low entry barrier specifically suitable for SMEs and on the other hand a scalable certification to meet high information security requirements, the matrix certification approach as shown in Figure 4 was defined for the certification of participants.

The participant certification approach is displayed by two dimensions. The horizontal dimension is the 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.

Evaluation Depth

The horizontal dimension Evaluation Depth consists of the following three layers, with only the second and third layer containing actual evaluation tasks:

Self-Assessment

A Self-Assessment is a mere self-declaration by the prospective participant in order to clarify the participant's identity and the provisioning of information about the participant's systems. No evaluator is involved in performing a self-assessment and no information of contained in a self-assessment is validated by an evaluation facility.

Due to the fact that no evaluator is involved in the Self-Assessment, no fully-qualified Industrial Data Space certificate is handed out to the participant. The Self-Assessment leads only to a digital X.509 certificate in order to facilitate participation in the Industrial Data Space. Nevertheless, it is a possibility for a prospective participant to explore and test the features of the Industrial Data Space in selected use cases. Another scenario for this layer is the use of a managed connector. It is operated by a fully evaluated service provider and the Self-Assessment would be only a low entry barrier for an end-user of such a managed connector.

Management System

The evaluation of the participant's Management System is the next layer of evaluation depth. This evaluation is performed by an independent evaluation facility and involves analyzing whether the applicant has defined a management system and whether the applicant is actively working according to the defined management system. This layer of evaluation depth usually involves interviews, site audits and exemplary review of information and evidence at a certain point in time.

Control Framework

The deepest layer 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 and the controls defined within the control framework of the applicant. This usually involves interviews, site audits and evidence gathering activities based on randomized sampling to demonstrate that controls were performed over a certain period of time. As with a Management System evaluation, the results are then approved by the Certification Body.

Security Requirement Extent

The extent of the Security Requirements consists of the following three levels and all levels are built on one another containing requirements derived from ISO/IEC 27001[1].

Entry Level

The entry level covers only the basic security requirements that every participant of the Industrial Data Space needs to fulfill. The entry level serves as a low barrier for companies (especially SMEs) interested in trying out Industrial Data Space participation, without facing considerable up-front investments. With that in mind, this level is only combined with the low-cost self-assessment and an evaluation of the participant's Management System.

Member Level

The member level additionally covers all relevant security requirements ensuring an advanced level of security, suitable for most of the core participants as defined in the Business Layer of the IDS Reference Architecture Model [IDSRA, 3.1]: Data Owner, Data Provider, Data Consumer, Broker Service Provider, App Store Provider, Vocabulary Provider, Service Provider. The member level is sufficient for most use cases involving the exchange of sensitive data.

Central Level

Finally, the central level includes special requirements that are necessary for Industrial Data Space participants intending to perform key functionalities and roles within the Industrial Data Space. These requirements are appropriate since these roles have special responsibilities so any security breaches would risk affecting the Industrial Data Space as a whole, or substantial parts of it. Concretely, this applies to the following roles defined in the Business

[1]For more information see https://www.iso.org/isoiec-27001-information-security.html

Layer of the IDS Reference Architecture Model [IDS-RA, 3.1]: Clearing House and Identity Provider.

This distinction of the full qualified Industrial Data Space participants in a member level and a central level have been designed in order to have lower financial and procedural accession criteria.

These two dimensions form a matrix with nine fields as shown in Figure 4, and each field represents a combination of Evaluation Depth and the extent of the Security Requirements. This matrix is used by the data owner to define the degree of security that needs to be provided by other participating organizations in order for them to be allowed to obtain and process the owner's data. Due to this flexible certification approach, the data owner is enabled to specifically tailor their certification based on their business' requirements and capabilities. In addition, other participants benefit from using the matrix. For example, a new participant benefits from a low entry barrier by getting a certificate for entry level and self-assessment. After this, the participant can continuously develop in any direction of the matrix in order to facilitate a cooperation with other participants. This flexibility is especially helpful for start-ups and SMEs. On the other hand, the matrix enables certificates with a rate of security high enough to be sufficient even for large companies or those with strict security requirements. Each participant is therefore enabled to decide the required rate of security for the exchange of data, e.g. entry level for weather data, but member level coupled with Management System for sensitive business data.

	Entry Level	**Member Level**	**Central Level**
Data Owner	Required	Recommended	Optional
Data Provider	Required	Recommended	Optional
Data Consumer	Required	Recommended	Optional
Broker Service Provider		Required	Optional
App Store Provider		Required	Optional
Vocabulary Provider		Required	Optional
Service Provider		Required	Optional
Clearing House			Required
Identity Provider			Required

Figure 3: Mapping of the roles in the Industrial Data Space to the levels of certification

Assurance

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

Figure 4: Certification Approach for participants of the Industrial Data Space

Certification Criteria Catalogue

To further reduce the financial entry barrier for Industrial Data Space applicants, the participant certification approach is designed to allow the re-use of existing certificates obtained through compliance with other certification schemes, standards, and norms. Depending on the desired level and depth of the evaluation, this could for example imply that certain control testing can be inherited from an ISAE3000 certification framework.

In order to enable the participants to reuse their existing certificates, the participant certification criteria catalogue [CRIT-P] has been developed on the basis of established security standards. Due to the nature of the Industrial Data Space and its international approach the standards ISO/ IEC 27001 and BSI C5[2] (Bundesamt für Sicherheit in der Informationstechnologie (engl. Federal Office for Information Security) Cloud Computing Compliance Controls Catalogue) have been chosen. The standard ISO/ IEC 27001 has been chosen due to its international distribution and its reputation for information security. The standard BSI C5 is a standard for information security and developed for modern IT environments like cloud computing.

Out of both standards the requirements relevant for the Industrial Data Space have been selected for their applicability regarding the different levels. These requirements have been grouped in 16 sections with a different number of requirements for each level. Due to the incremental approach of the level all requirements of the entry level are also relevant for the member and central level and all requirements of the member level are also relevant for the central level.

Piloting of Certification Criteria

In order to verify the completeness, applicability, feasibility and relevance of the catalogue of certification criteria for the IDS participant certification, as well as the certification process for participants, piloting workshops with various IDSA members (e.g. GESIS, Komsa, Thyssenkrupp) were conducted. The workshops were organized by the WG Certification, bringing together experts in participant certification from the Working Group with the security officer and / or the compliance officer from the companies. In addition to the audit readiness, this validation gave valuable feedback for the list of certification requirements and the associated questionnaire.

[2] For more information see https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

These 1-day workshops led by the expert from the Working Group were organized as a health check. The certification expert explained the certification process in detail. In a second phase the audit readiness was evaluated by going through the catalogue step by step. No documented evidence was required, only verbal information was collected. This approach enabled all parties to get a better sense of the status of the IDS-readiness for the participant, as well as the significance of each criteria. The results of the workshop were recorded by the evaluation lead and distributed to the company. The anonymized results were reported back to the WG Certification.

In regard to the completeness and applicability of the criteria themselves, the in-depth discussion during the workshops in some cases led to an adjustment of the wording of a criterion. In addition the feedback of the piloting led to a new entry in the dimension matrix of Evaluation Depth and the Extent of the Security Requirements for participant certification (Member Level, Management System).

Participants Overview

This chapter summarizes the description of the architectural roles of the Industrial Data Space participants as defined in [IDSRA, 3.1] and how the participant certification applies to them.

Core Participants

The Data Provider is responsible for the integrity, confidentiality, and availability of the data it publishes and provides. Evaluation and certification of the security mechanisms employed by the data provider shall provide a sufficient degree of security against the risk of relevant security requirements (such as data integrity, confidentiality, or availability) being undermined by attacks.

Data Owners are assumed to often act as a data provider at the same time. In the case of the data owner and the data provider being different entities (i.e., the data owner does not publish the data itself but hands over this task to a data provider), both the data owner and the data provider are responsible for integrity and confidentiality of the data. Responsibility for the availability of the data, however, rests solely with the data provider in this case, provided the data owner has handed over the data to the data provider.

For a data owner not acting as a data provider, evaluation and certification of the technical, physical, and organizational security mechanisms employed provide a sufficient degree of security against the risk of data integrity or confidentiality being undermined by attacks.

As an organization that has access to data provided by a data owner, the Data Consumer also assumes responsibility for the confidentiality and integrity of that data (i.e., in terms of making sure the data cannot leave the Industrial Data Space in an uncontrolled manner and cannot be corrupted before being used). Furthermore, the data consumer has to make sure the data cannot be used for purposes other than permitted. Against all these risks, evaluation and certification of the technical, physical, and organizational security mechanisms employed by the data consumer provide a sufficient degree of security.

Intermediaries

Since preventing sensitive data from ending up in the wrong hands is a central goal of the Industrial Data Space initiative, it is highly critical to eliminate all risks involving manipulation of identities. The integrity and availability of identity-related information processed by the Identity Provider is therefore of utmost importance. Only evaluation and certification of the security mechanisms employed by the respective organization (in combination with technical security measures in relation with the software components used for processing identity-related information) is able to provide a sufficient degree of security against these risks.

Broker Service Providers, providers of Clearing House services, the App Store Provider, and the Vocabulary Provider deal only with metadata, transactions, or apps (i.e., they do not work with the sensitive payload data which the Industrial Data Space is designed to protect). The risk associated with possible breaches of confidentiality, integrity, and availability of metadata is lower (with the exception of clearing house transaction data, which, however, lies beyond the scope of the Industrial Data Space). Nevertheless, an attacker succeeding in exfiltrating or corrupting metadata, or impeding the availability of metadata, would be able to cause considerable damage to the Industrial Data Space or targeted participants – especially if such successful attacks would remain undetected over extended periods of time. Therefore, evaluation and certification tailored to the specific risk profiles of and security mechanisms employed by broker service providers, providers of clearing house services, app store providers, and vocabulary providers is proposed in order to ensure a sufficient degree of security against the risks mentioned. As far as the app store provider is concerned, there is an additional risk in terms of an attacker successfully substituting legitimate apps with modified versions, thereby threatening the payload data indirectly. However, technical measures in the app store implementation (e.g., only apps cryptographically signed by the app developer are accepted and distributed) seem more effective for reducing this risk than organizational measures on the part of the app store provider.

Software / Service Providers

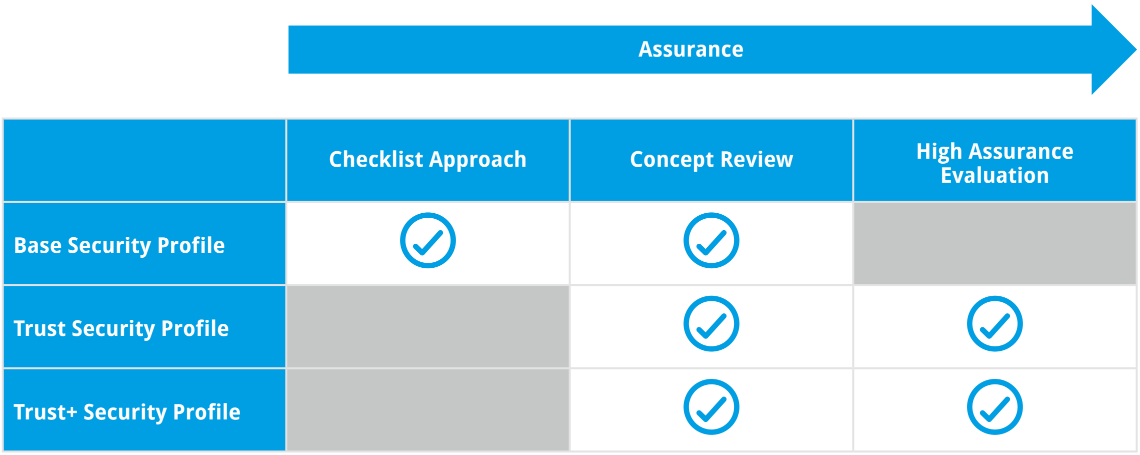
Providers of compliant software usually have no contact with sensitive data, but execute tests with appropriate, non-sensitive test data. Therefore, in most cases no certification of the organizational security is required. If access to actual data of the Industrial Data Space is necessary, the Software Provider assumes the role of data consumer or data provider for as long as such access is needed. In that case, the certification requirements of the corresponding roles apply.

If a participant does not deploy the technical infrastructure required to participate in the Industrial Data Space itself, it can outsource certain tasks, like publishing their data in the Industrial Data Space to a Service Provider hosting the required infrastructure. If this is the case, this Service Provider assumes the role of a Data Provider, Data Consumer, Broker Service Provider, etc. and performs the corresponding activities. They inherit the original role's responsibilities and risks, and shall therefore be subject to the corresponding requirements regarding certification.

PART 3 – CORE COMPONENTS CERTIFICATION

To secure the intended cross-industrial and cross-company information exchange, the Industrial 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.

Similar to the participant certification, a matrix certification approach as shown in Figure 5 was defined for the core components of the Industrial Data Space. This ensures on the one hand a low entry barrier specifically suitable for SMEs and on the other hand a scalable certification to meet high information security requirements.



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

Figure 5: Certification Approach for core components of the Industrial Data Space

Assurance Levels

The depth and rigor of an evaluation consists of the following three assurance levels as defined by the Industrial Data Space certification scheme:

Checklist Approach

The core component must fulfill security features (security requirements, security properties, security functions) as defined by the corresponding checklist. The vendor of the component validates the claims made about the implementation. Additionally, an automated test suite will be used to verify the component's security features.

Concept Review

Instead of the checklist approach, an in-depth review by an Industrial Data Space evaluation facility is necessary. The review includes an evaluation of the provided concept as well as practical functional and security tests.

High Assurance Evaluation

For the third level, 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

Whenever two components establish a communication channel, it's up to them to decide which information they will send to the communication partner. Therefore, the identity and certification level (for both the participant and the component) must be provided by each component in the form of a digital certificate containing this information. As with the participant certification, this approach enables the data owner and data consumer to specify the security profile required for the core components used during data exchange.

For this purpose, the Industrial Data Space certification scheme defines three security profiles for the core components defined in the section Component Overview of this paper.

Base Security Profile

This profile includes basic security requirements: limited isolation of software components, secure communication including encryption and integrity protection, mutual authentication between components, as well as basic access control and logging. However, neither the protection of security related data (key material, certificates) nor trust verification are required. Persistent data is not encrypted and integrity protection for containers is not provided. This security profile is therefore meant for communication inside of a single security domain.

Trust Security Profile

This profile includes strict isolation of software components (apps/services), secure storage of cryptographic keys in an isolated environment, secure communication including encryption, authentication and integrity protection, access and resource control, usage control and trusted update mechanisms. All data stored on persistent media or transmitted via networks must be encrypted.

Trust+ Security Profile

This profile requires hardware based trust anchors (in the form of a TPM or a hardware-backed isolation environment) and supports remote integrity verification (i.e., remote attestation). All key material is stored in dedicated hardware isolated areas.

Certification Criteria Catalogue

The catalogue of certification criteria for the IDS core components [CRIT-C] was defined as part of the Fraunhofer research project »Industrial Data Space« and fine-tuned with the members of the WG Certification. The catalogue is split into three thematic sections, i.e. IDS-specific requirements, functional requirements taken from the industry standard ISA/ IEC 62443-4-2 [62443-4-2] and best practice requirements for secure software development.

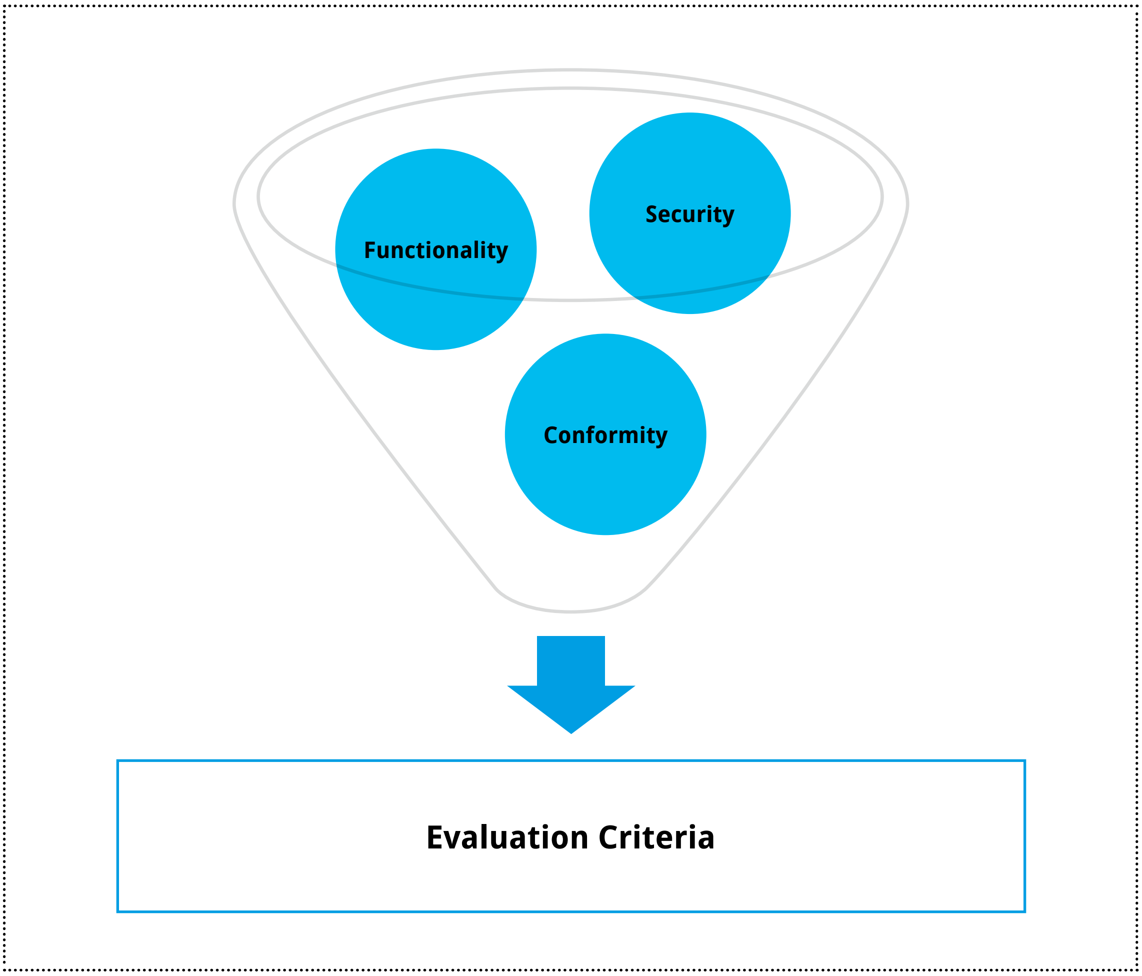


Figure 6: Criteria Synergy

Each criteria section targets a set of evaluation goals:

- The IDS-specific requirements aim to evaluate the Core Component's conformity to the IDS Reference Architecture Model, both in regard to functionality (e.g. support of the IDS information model) as well as security (e.g. conformance to the IDS security architecture).
- The requirements taken from ISA/IEC 62443-4-2 target the implemented functionality and security measures in relation to industry-wide accepted requirements for industrial automation and control systems, e.g. the capability to obscure feedback of authentication information during the authentication process.
- 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, e.g. design documentation, physical security measures and test processes.

To reduce the financial entry barrier not only for Industrial Data Space participants but also for the developers of core components, the component certification approach is designed to use existing certification schemes whenever reasonable. Where such certification schemes do not exist or aren't widely recognized, e.g., for Industrial Data Space-specific aspects, criteria defined within the Industrial Data Space certification scheme will be employed.

The functional and security requirements of the core components to be evaluated will be defined based on the IDS Reference Architecture Model, specific component specifications like the Connector Specification as well as widely recognized requirement catalogues like ISA/IEC 62443-4-2 (e.g. for functional requirements such as data confidentiality and system integrity).

The evaluation at the various assurance levels can also be supported and facilitated by requiring appropriate measures used throughout the lifecycle of the component as defined in ISA/IEC 62443-4-2, such as using the approach for thorough elicitation of the Security Requirements, enforcing those Security Requirements at the Architecture level (e.g., using Security-by-Design) and tracing them to the Secure Implementation level, supported by relevant Guidance Documents, Verification & Validation approaches, as well as a Secure Defect Management & Secure Update Management.[3]

Piloting of Certification Criteria

In order to verify the completeness and applicability of the catalogue of certification criteria for the IDS core component »Connector« to real-world implementations, as well as the IDS-readiness of these implementations, piloting workshops with various IDSA members (e.g. Fraunhofer AISEC, T-Systems, Cybus) were conducted. The workshops were organized by the WG Certification, bringing together Fraunhofer IDS certification experts, developers and product owners. While Fraunhofer had the best knowledge about certification requirements, the developers and product owners (consisting at least of the project manager and lead developer) brought their in-depth knowledge about real-world implementations of connector components as well as a business/market perspective to the table.

During these 2-day workshops led by Fraunhofer FOKUS, the Connector implementation was evaluated by going through the catalogue step by step and looking into the implemented measures meeting the requirements as well as the existing developer documentation. This approach enabled all parties to get a better sense of the status of the IDS-readiness of the implementation under evaluation. The results of the workshop were recorded by the evaluation lead and distributed to the developer. The anonymized results were reported back to the WG Certification.

In regard to the completeness and applicability of the requirements themselves, the in-depth discussions during the workshops in some cases led to an adjustment of the wording of a requirement, the addition of new requirements or the removal of non-applicable requirements (either entirely or for a specific Security Profile). As such, each piloting workshop led to a new version of the requirements catalogue.

[3] US Cert: Build Security In: Modeling Tools, 2013

Component Overview

This chapter summarizes the Industrial Data Space core components as assessed in [IDSRA, 4.2] that are targets of the component certification.

Connector

Being the point of access to the Industrial Data Space, the Connector provides a controlled environment for processing and exchanging data, ensuring secure transfer of data from the data provider to the data consumer. As such, the necessary trust in the correct and complete implementation of the functionality required by the IDS Reference Architecture Model and the Connector specification can only be ensured by independent evaluation and certification from an approved evaluation facility and the certification body of the Industrial Data Space.

Broker

A Broker service does not have access to primary data, but only to metadata provided by data providers, which is generally considered less sensitive. Likewise, Broker services do not assign or enforce access rights, but merely support data exchange. Nevertheless, integrity and availability of metadata (i.e., correct and secure storing and handling of metadata) is of high importance for the Industrial Data Space. Compatibility with the required functionality as defined by the certification body is therefore evaluated and certified.

Apps and Services

Data Apps and Services have direct contact with primary data, which means that a compromised Data App or Service may compromise the integrity of data. However, confidentiality and availability of data is ensured by the measures defined in the Security Architecture of the Industrial Data Space, which strongly limit the potential damage caused by Data Apps and Services. Also, Apps and Services will typically use the security features provided by the Connector. Therefore, not every Data App or Service to be made available in the Industrial Data Space requires a medium or high assurance level certification. However, the automated test suite mentioned above for the basic security level will be integrated in the upload process of each Industrial Data Space App Store.

App Store

While the App Store itself does not have direct contact with primary data, the Apps and Services they provide do. Compromised security of the App Store, particularly of the test suite used during app and service upload, could lead to the circulation of compromised Apps and Services. Compatibility with the required functionality and security features is therefore to be evaluated and certified.

Hardware

For certain security profiles as defined in the IDS Reference Architecture Model, additional hardware security components are required to achieve an appropriate level of protection for access to sensitive data. In addition to the core software components of the Industrial Data Space, these hardware components must therefore also be considered in the context of certification. In the interest of trustworthiness, and to avoid double certification, the use of third-party certified hardware components will be required (e.g., Trusted Platform Modules certified in accordance with the Protection Profiles BSI-CC-PP-0030-2008 or ANSSI-CC-PP-2015/07). Certification activities of the Industrial Data Space regarding these components will be limited to checking the validity of existing base certificates.

PART 4 – HOW-TO: IDS CERTIFICATION PROCESS

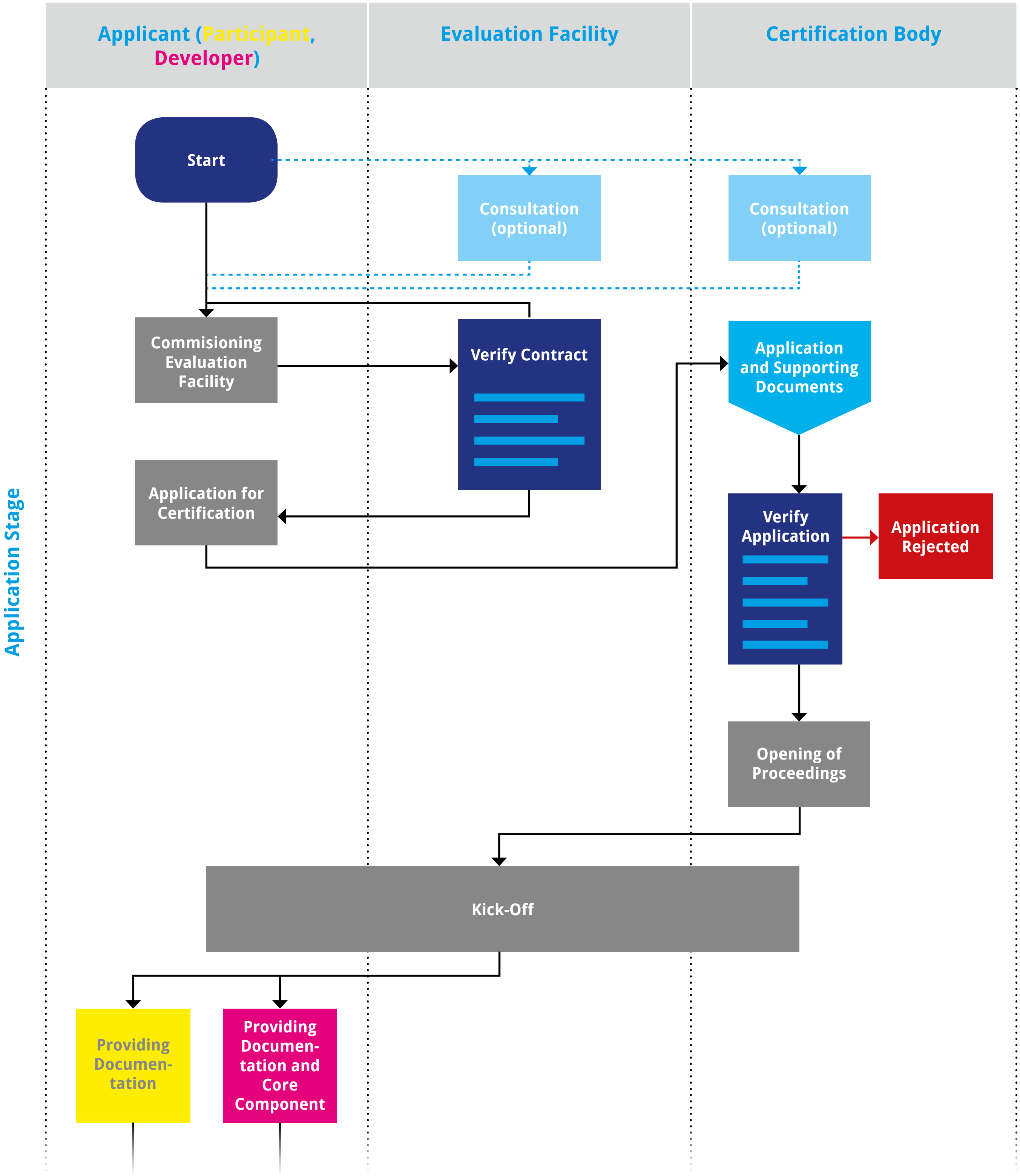
Participants and core components within the IDS ecosystem shall provide sufficiently high degree of security regarding the integrity and confidentiality of the data being processed in the IDS. Therefore, a certification of participants and core components is mandatory. Involved partners are the applicant,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

Application Stage

The main goal of this stage is the successful start of the IDS certification process.

- The certification process for any applicant starts with the applicant triggering the certification process.
- Before this, an optional consultation can take place between the applicant and the evaluation facility or the applicant and the certification body. Possible topics are for example: Presentation of test competence and test procedure of the evaluation facility or advice on IDS certification process and certification criteria from the certification body. Especially for new participants or manufacturers this consultation is highly recommended.
- 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 the applicant.
- The applicant must apply for certification to trigger the start of the certification process.
- The applicant must provide the necessary evidence for the certification body to confirm the application. This includes, for example, the following documents: company profile, list of current certificates, detailed information of the present changes in case of recertification.
- This confirmation by the certification body may result in a rejection of the application. In this case, the certification process ends at this point and there is no review by the evaluation facility or the issue of a certificate.
- If the application is accepted, the evaluation procedure will be opened and there will be a Kick-Off with all involved partners (applicant, evaluation facility, certification body).

For the next phase (evaluation stage), the applicant must provide the necessary documents and, in case of the certification of a core component certification, also the component with the necessary associated documentation, to the evaluation facility and the certification body.



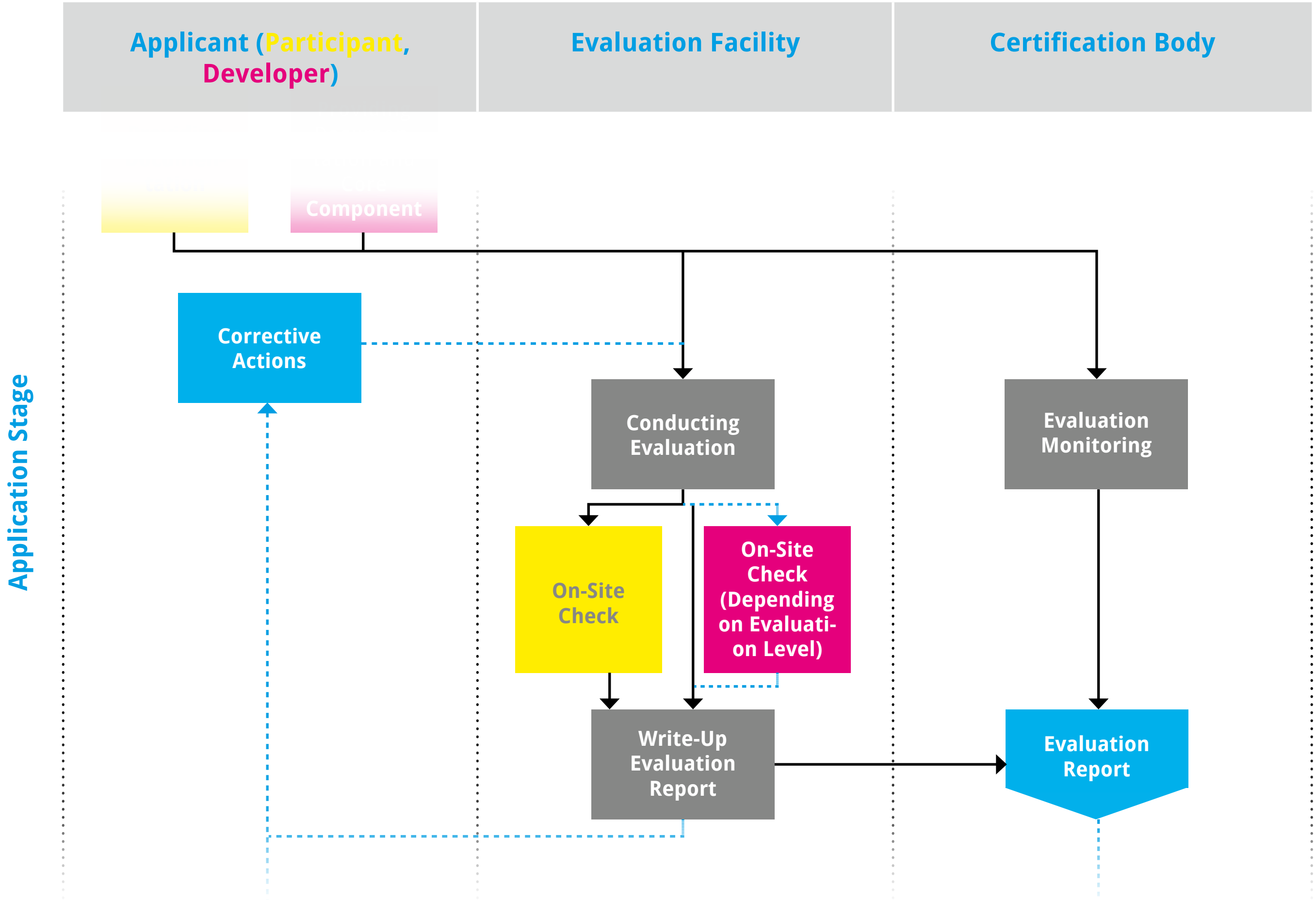
Applicant (Participant, Developer)
Evaluation Facility
Certification Body
Application Stage
Start
Consultation (optional)
Consultation (optional)
Commisioning Evaluation Facility
Verify Contract
Application and Supporting Documents
Application for Certification
Verify Application
Application Rejected
Opening of Proceedings
Kick-Off
Providing Documen-tation
Providing Documen-tation and Core Component

Evaluation Stage

The main goal of this stage is the evaluation of a participant or IDS core component based on the defined certification criteria. If necessary, corrective actions need to be performed by the applicant to achieve a successful certification. The parties mainly involved at this stage are the applicant and evaluation facility; it includes the following steps:

- The evaluation facility is responsible for carrying out the detailed technical and/or organizational evaluation work during the certification. The basis for the evaluation is either the certification criteria catalog for the participant certification or the criteria catalog for the component. This includes the execution of all necessary tests and on-site checks, with the details depending on the chosen certification level.
- The evaluation facility documents the detailed results in an evaluation report. The recipients of this report are the applicant and the certification body.
- If deviations have been identified, corrective actions will be defined. Implementing these corrective actions is the responsibility of the applicant. Afterwards, a re-examination is necessary. A renewed on-site check is only required for serious defects, i.e. in cases where the rectification can only be checked on-site.
- The evaluation is monitored by the certification body to ensure the correct implementation and execution of the IDS certification scheme. This can include the accompaniment of the evaluation facility during an on-site check.

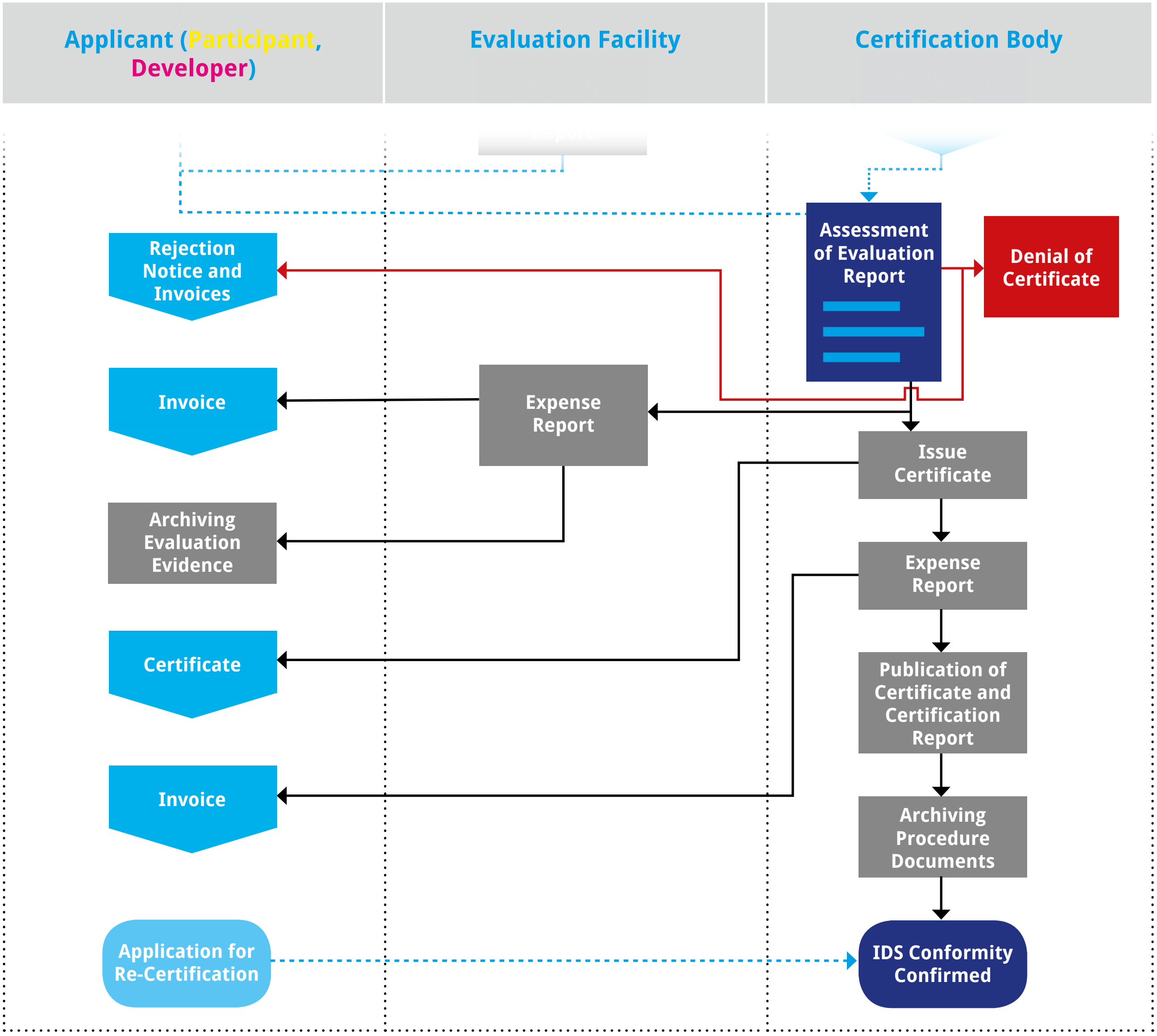
The result of this stage is the evaluation report, created by the evaluation facility. The report serves the certification body in the next stage as a basis for the decision-making for the approval of the certificate.



Certification Stage

The main topics of this stage are the examination of the evaluation report by the certification body as well as the processes for issuing the certificate if the result is positive. The parties applicant and certification body are mainly involved at this stage; it includes the following steps:

- 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 corrective actions and re-examination are required, updated evaluation reports will be provided.
- The decision may be that no certificate can be issued. In this case, the procedure is terminated and the applicant receives a rejection notice.
- If the decision is positive, the applicant will be confirmed as being IDS compliant. The certification body issues the certificate, triggers the generation of a X.509 certificate and publishes the certificate and the certification report online.
- The certification body archives the procedural documents.
- The applicant is responsible for archiving the evidence documentation as used during the evaluation.
- Independent of the final decision by the certification body (acceptance or rejection), an invoice will be send to the applicant by the evaluation facility and the certification body.


Applicant (Participant, Developer)
Evaluation Facility
Certification Body
Assessment of Evaluation Report
Denial of Certificate
Rejection Notice and Invoices
Invoice
Expense Report
Issue Certificate
Archiving Evaluation Evidence
Expense Report
Certificate
Publication of Certificate and Certification Report
Invoice
Archiving Procedure Documents
Application for Re-Certification
IDS Conformity Confirmed

Certification Stage

PART 5 – FUTURE WORK

After having finalized version 1 of the Certification Criteria Catalogues for IDS Participants and Core Components, the Working Group will focus next on the Criteria Catalogue for IDS Evaluation Facilities.

It is foreseen that the IDS Certification Body, on top of being monitored by the IDSA, will be accredited by the national accreditation body (e.g., DAkkS in Germany) in the future. Its responsibilities in the context of the IDS Certification Scheme will include:

- Auditing the Certification Body to verify, for example, their adherence to regulatory and normative requirements[4].
- Provisioning of recommendations to the Certification Body based on the results of its monitoring activities.

The Accreditation Body will be a nationally unique entity, supervising the nations certificate-granting institutions. It will not be actively involved in a participant or core component certification and the approval of Evaluation Facilities for performing Industrial Data Space evaluations.

[4] For more information on the specific DAkkS requirements, see https://www.dakks.de/content/allgemeine-regeln-zur-akkreditierung-von-konformitätsbewertungsstellen

REFERENCES

[IDSRA] Otto, B. et al.: IDS Reference Architecture Model - International Data Space. Fraunhofer Gesellschaft and International Data Space e.V., Version 2.0, 2018. http://www.industrialdataspace.org/ressource-hub/publikationen/

[CRIT-P] WG Certification: Certification Criteria Catalogue for IDS Participants, Version 1.0.0

[CRIT-C] WG Certification: Certification Criteria Catalogue for IDS Core Components, Version 1.0.0

[CRIT-EF] WG Certification: Criteria Catalogue for IDS Evaluation Facilities, Version 0.3 (Draft for Comment).

[62443-4-2] ISA99 Committee: ISA-62443-4-2 - Security for industrial automation and control systems - Technical security requirements for IACS components, 2017-10 (Draft for Comment).

INTERNATIONAL DATA
SPACES ASSOCIATION

CONTACT

Head Office
INTERNATIONAL DATA SPACES ASSOCIATION
Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund

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

WWW.INDUSTRIALDATASPACE.ORG