INDUSTRIAL DATA SPACE ASSOCIATION

STRATEGY PAPER CERTIFICATION

FRAMEWORK FOR THE INDUSTRIAL DATA SPACE CERTIFICATION SCHEME

Fraunhofer

GESIS GESELLSCHAFT FÜR INFORMATIONSSYSTEME
A Member of the Salzgitter Group

komsa

pwc

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

Thilo Ernst, Fraunhofer FOKUS

Thomas Fedkenhauer, PwC

Mustafa Ipekcioglu, PwC

Prof. Dr. Jan Jürjens, Fraunhofer ISST

Stefan Kistler, TÜV NORD

Dr. Ralf-Peter Simon, KOMSA Group

Gerrit Stöhr, GESIS

Sascha Wessel, Fraunhofer AISEC

AUTHORS

Markus Bartsch (TÜViT), Thilo Ernst (Fraunhofer FOKUS), Thomas Fedkenhauer (PwC), Mustafa Ipekcioglu (PwC), Jan Jürjens (Fraunhofer ISST), Stefan Kistler (TÜV NORD), Nadja Menz (Fraunhofer FOKUS), Aleksei Resetko (PwC), Ralf-Peter Simon (KOMSA Group), Gerrit Stöhr (GESIS), Sascha Wessel (Fraunhofer AISEC)

TABLE OF CONTENTS

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: a Fraunhofer research project entitled »Industrial Data Space« and the »Industrial Data Space Association«. While the research project is concerned with the design and prototype implementation of the Reference Architecture Model, the association 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 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 an 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. After presenting the framework for the scheme's structure, the main focus of this paper is on the certification approach proposed by the Working Group Certification of the Industrial Data Space Association, including evaluation levels and the selection and re-use of widely accepted standards and norms within different parts of the scheme. As such, this paper illustrates the core of our strategy for crafting a flexible and cost-effective certification scheme. As this is a work in progress, adjustments to the proposed certification scheme may be made in the future.

Data security and data sovereignty are the fundamental characteristics of the Industrial Data Space. Furthermore, data is only exchanged if the exchange takes place between trustworthy and certified participants.

PART 1 - ROLES AND RESPONSIBILITIES

Participants and core components should 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.

Accreditation Body

A nationally unique entity within the Industrial Data Space certification scheme is the Accreditation Body. The Accreditation Body supervises each certificate-granting institution and issues the accreditation. A Certification Body is accredited on a regular basis and consequently the Accreditation Body is not directly involved in a participant or core component certification.

Its responsibilities include:

- Continuous improvement of the defined certification scheme including the incorporation of the feedback provided by the Certification Body.
- Monitoring of the current regulatory and legal requirements to evaluate and react to possible influences to the certification scheme.

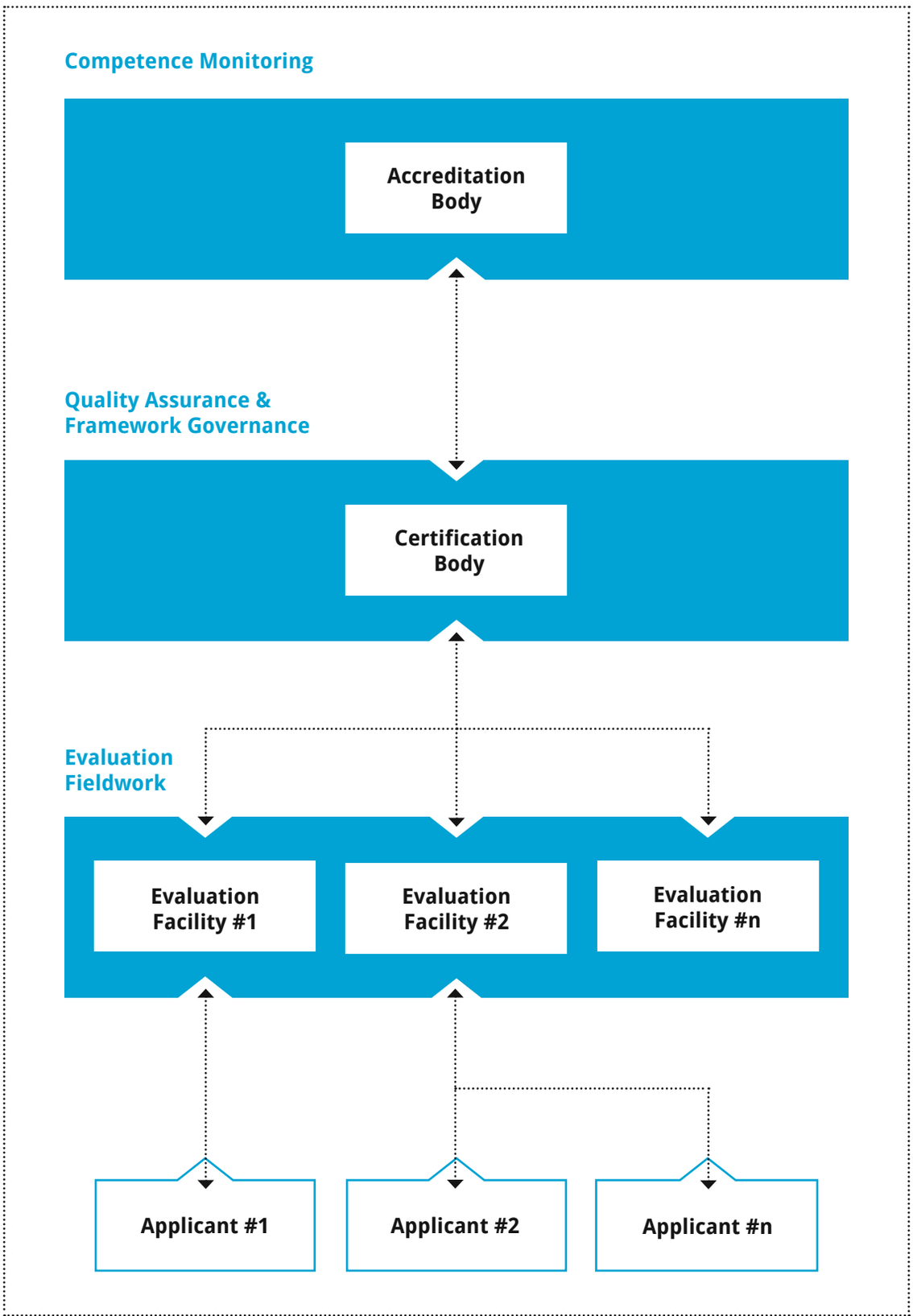


Figure 1: Industrial Data Space Certification - Roles & Responsibilities

- Auditing the Certification Body to verify the technical competencies as well as the adherence to regulatory and normative requirements.
- Accreditation of the Certification Body against the defined evaluation procedures and requirements set for every Industrial Data Space participant or core component.
- Monitoring of the Certification Body to ensure a consistent level of quality for the certification of Industrial Data Space participants and core components.
- Provisioning of recommendations to the Certification Body based on the results of its monitoring activities.

A Certification Body is accredited on a regular basis and consequently the Accreditation Body is not directly involved in a participant or core component certification.

Certification Body

A Certification Body, which is appointed and regularly audited by the Accreditation Body to manage the certification process, defines the standardized evaluation procedures and supervises the actions of the Evaluation Facilities. It only grants the certificate (also called evaluation certificate subsequently) if and when both the Evaluation Facility and the experts of the Certification Body have come to the conclusion that all preconditions are fulfilled.

Its responsibilities include:

- Formulating and defining the certification scheme in cooperation with the Industrial Data Space Association, including the evaluation procedures, participant and core component certification approaches as well as their underlying requirements.
- Ensuring correct implementation and execution of the Industrial Data Space certification scheme.
- Ensuring continuous adherence to the Industrial Data Space certification scheme following up on changes und updates received from the Accreditation Body.
- 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.
- Final decision about the award or denial of a certificate.
- Authorization/triggering of the generation of a X.509 certificate digitally representing the evaluation certificate. These digital certificates 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).
- 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 Accreditation Body.

Industrial Data Space certificates will have a limited validity period. In order to renew a certificate before it expires, a re-certification needs to be done. This will take into account any relevant external developments that have happened in the meantime. Similarly, re-certification is needed after changes to the Target of Evaluation. In case of minor changes only a very light-weight, low-cost re-certification process (also referred to as “maintenance process”) is employed. The definition of major and minor changes will follow the definition used within widely accepted certification standards such as ISO 27001 and Common Criteria.

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.
- 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 and SME companies 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.

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. All Applicants need to actively submit an application to start the certification process and have the duties as listed above. During the certification process, the primary focus of the evaluation will be either on the product or on the organization itself.

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.
To ensure on the one hand a low entry barrier specifically suitable for SME's and on the other hand a scalable certification to meet high information security requirements, the matrix certification approach as shown in Figure 2 was defined for the certification of participants.

The participant certification approach is displayed by two dimensions. The horizontal dimension is the depth of evaluation, 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.

The horizontal dimension "evaluation depth" consists of the following three layers:

Self-Assessment

The Self-Assessment is a mere self-declaration by the prospective participant. The purpose of this first layer is to clarify the participant's identity and the provisioning of information about the participant's systems. No evaluator is involved in producing or handing over the self-assessment and no information of the certificate is validated by an independent evaluation facility.

Management System

The evaluation of the participant's Management System is the next layer of evaluation depth. This evaluation needs to be 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.

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:

Entry Level

The entry level covers only the basic security requirements that every participant of the Industrial Data Space needs to fulfill.

Member Level

The member level additionally covers all relevant security requirements ensuring an advanced level of security, suitable for most of the core participants.

Central Level

Finally, the central level includes special requirements that are necessary for Industrial Data Space participants keen to perform key functionalities and roles within the Industrial Data Space.
These two dimensions form a matrix with nine fields and each field represents a combination of depth of evaluation and extent of evaluation. This matrix is used by the data owner to define the rate of security that needs to be provided by other organizations in order to process their data. Due to this flexible certification approach the data owner is enabled to specifically tailor their certification based on their businesses requirements and capabilities. In addition, other participants benefit from using the matrix.

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

Figure 2: Certification Approach for Participants of the Industrial Data Space

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 Control Framework for sensitive business data.

Conformity to Standards and Norms

To further reduce the financial entry barrier for Industrial Data Space applicants, the participant certification approach is designed to allow the reuse 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

Participants Overview

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 should 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.

Service Providers are employed by other participants of the Industrial Data Space in order to outsource certain tasks, like publishing their data in the Industrial Data Space. They inherit the original role's responsibilities and risks, and should 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 fulfill a fitting level of security. Similar to the participant certification, a matrix certification approach as shown in Figure 3 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.

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

Checklist and Test Suite

The core component (Target of Evaluation) 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 Target of Evaluation. Additionally, an automated test suite will be used to verify the target's security features.

Concept Evaluation and Practical Tests

In addition to 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.

Source Code Review

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 a source code review will be performed by an evaluation facility. Furthermore, the development process will be evaluated, including an audit of the development site.

The Industrial Data Space certification scheme defines three levels of security features for all core components defined in the section Component Overview of this paper.

Basic Security Features

This level includes basic security requirements: isolation of software components (apps/services), secure storage of cryptographic keys in an isolated environment, secure communication including encryption, authentication and integrity protection,

	Checklist and Test Suite	Concept Evaluation and Practical Tests	Source Code Review
Basic Security Features			
Local Integrity Protection			
Remote integrity Verification			

Figure 3: Certification Approach for Core Components of the Industrial Data Space

access control, usage control and update mechanisms. All data stored on persistent media or transmitted via networks must be encrypted.

Local Integrity Protection

Additionally to the basic security features, the component must implement boot-time and run-time integrity protection for code and data.

Remote Integrity Verification

In addition to the previously mentioned security features, the component must implement integrity verification of all communication partners before any information is exchanged and it must provide all necessary information to allow its communication partner to verify its own integrity (remote attestation).

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 the identity and the certification levels. As with the participant certification, this approach enables the data owner and data consumer to specify the certification level required for the core components used during data exchange.

Conformity to Standards and Norms

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 (e.g., Common Criteria for security requirements of the Trusted Connector). Where such certification schemes do not exist or aren't widely recognized, e.g., for purely functional as well as 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 Reference Architecture Model for the Industrial Data Space, specific component specifications like the Connector Specification as well as widely recognized requirement catalogues like Part 2 of the Common Criteria (e.g. Security Management and Trusted Channels) and ISA/IEC 62443-4-2 (e.g. Data Confidentiality and System Integrity).

The evaluation, depending on the specific assurance level, should cover the widely recognized evaluation aspects as defined by the Common Criteria standard, i.e., Development, Guidance Documentation, Lifecycle, Developer and Evaluator Tests, and Vulnerability Assessment. 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[1].

Component Overview

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 Industrial Data Space Architecture 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

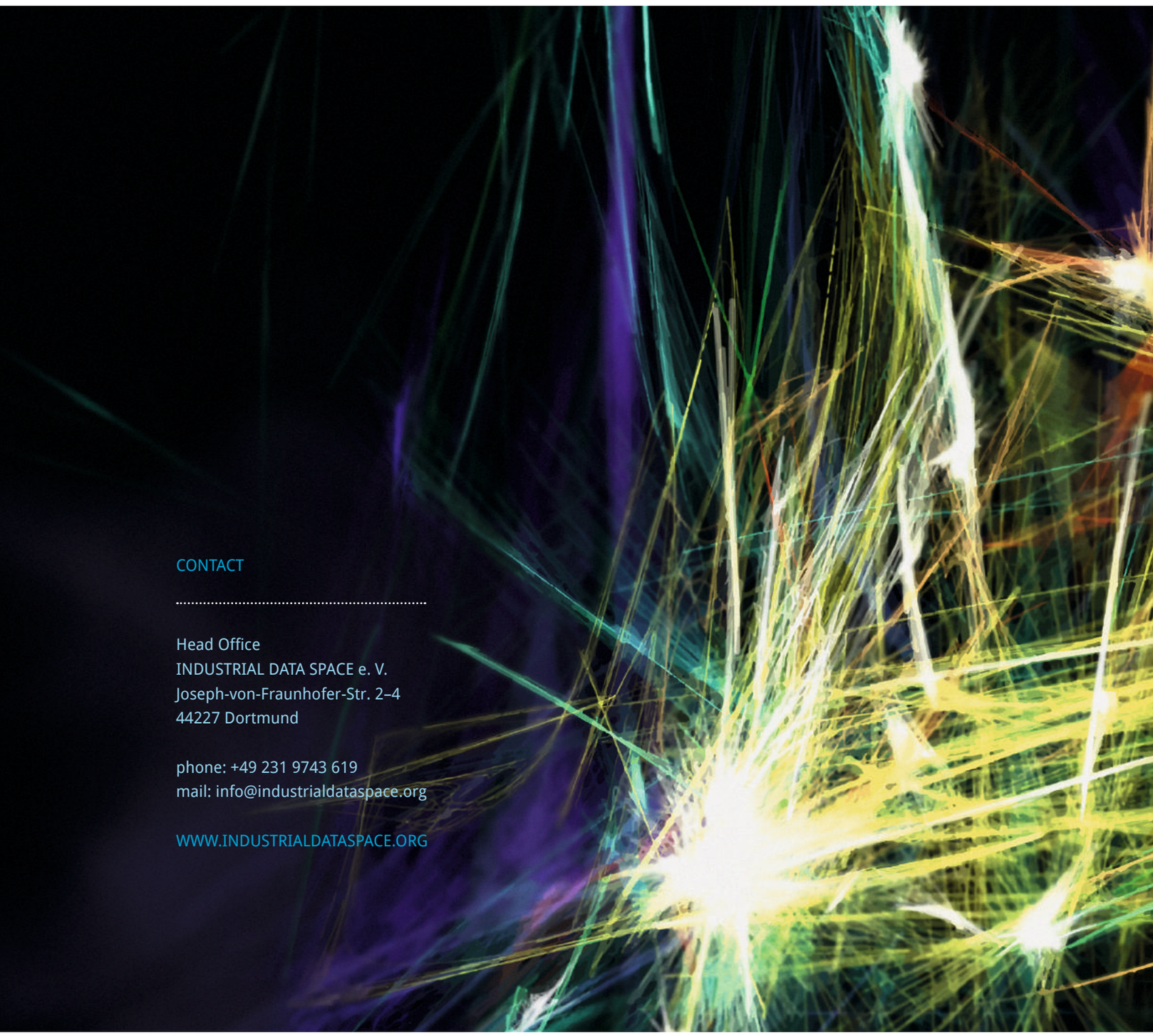
While the App Store itself does not have direct contact with primary data, the Apps and Services they provide do. Compromised security of the App Store, particularly of the test suite used during app and service upload, could lead to the circulation of compromised Apps and Services. Compatibility with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

Hardware

For certain security profiles as defined in the Industrial Data Space 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.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.

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

INDUSTRIAL DATA SPACE ASSOCIATION



CONTACT

Head Office
INDUSTRIAL DATA SPACE e. V.
Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund

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

WWW.INDUSTRIALDATASPACE.ORG