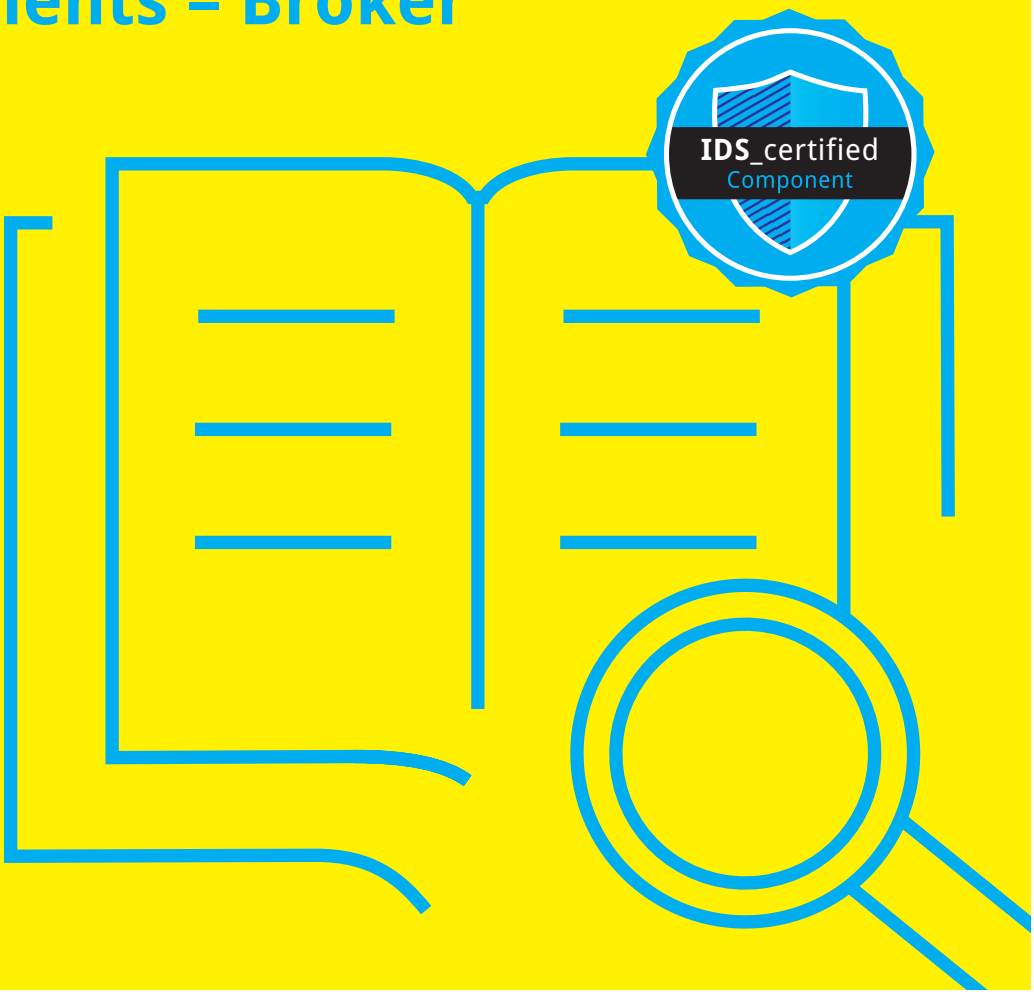
INTERNATIONAL DATA SPACES ASSOCIATION

White Paper | Version 1.0 | September 2020

Criteria Catalogue: **Components – Broker**



- ○ 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

Corresponding Author

- Sebastian Bader, Fraunhofer IAIS

Authors & Contributors

- Dennis Oliver Kubitza, Fraunhofer IAIS
- Monika Huber, Fraunhofer AISEC
- Sascha Wessel, Fraunhofer AISEC
- Sascha Hackel, Fraunhofer FOKUS
- Nadja Menz, Fraunhofer FOKUS

Cite as

Steinbuss S. (2020): Criteria Catalogue. Components - Broker. International Data Spaces Association. https://doi.org/10.5281/zenodo.5675735

IDS CERTIFICATION

Data security and data sovereignty are the fundamental characteristics of the International Data Space. Participants within the International Data Space must therefore use certified software (e.g., a »Connector« or a »Broker«) in order to securely exchange data in a sovereign way. Furthermore, data is only exchanged if the exchange takes place between certified participants that operate trustworthy operational environments.

The International Data Space Certification Scheme is of fundamental importance for making this happen. Certification provides a very high degree of transparency and trust. This transparency is achieved by making the certification requirements available to the public. Evaluating the components regarding their fulfilment of the defined levels of security can achieve the necessary trust.

This document therefore presents the criteria catalogue for the Broker component.

1 Introduction

The IDS Meta Data Broker is a service for publishing and searching metadata of Connectors and resources between International Data Spaces Participants. In order to ensure the necessary interoperability and general interactions, an IDS Meta Data Broker (like the App Store) is also defined as a specialized IDS Connector.

The communication between an IDS Connector and an IDS Meta Data Broker is based on the same principles as any other Connector-Connector communication within the International Data Spaces. Still, an IDS Meta Data Broker provides a collection of additional functionalities:

- Indexing services in order to effectively and efficiently respond to queries and present known Connectors and other resources
- Interfaces for Users or IDS-Messages to ensure access to the stored information.

This catalogue outlines the criteria an IDS Meta Data Broker must adhere to, i.e. which functionalities it must support and which services other IDS components can expect from a Broker. The described content is aligned with the IDSA Meta Data Broker Specification published in May 2020.

In addition to the general requirements each IDSA core component must comply with, the catalogue additionally contains the minimal requirements specifically defined for the Broker component, as well as two advanced Broker Profiles, enhancing the standard Broker functionalities by improved information management and usage policies.

2 Criteria to Certification Level Mapping

ID	Criteria Title	Basic	Advanced Information	Usage Control
IDS Specification (Component: Connector)				
Communication Integrity				
COM 01	Protected connection	x	x	x
COM 02	Mutual authentication	x	x	x
COM 03	State of the art cryptography	x	x	x
COM 04	Remote attestation	-	-	x
COM 05	Platform integrity	-	-	x
COM 06	Configuration and app integrity	-	-	x
Data Usage Control				
USC 01	Definition of usage policies	-	-	-
USC 02	Sending of usage policies	-	-	-
USC 03	Usage policy enforcement	-	-	x
USC 04	Usage policy changes	-	-	x
USC 05	Usage policy changes by administrator	-	-	x
Information Model				
INF 01	Self-Description (at Connector)	x	x	x
INF 02	Self-Description (at Broker)	-	-	-
INF 03	Self-Description content	x	x	x
INF 04	Self-Description evaluation	-	-	-
INF 05	Dynamic attribute tokens	x	x	x
Identity and Access Management				
IAM 01	Connector identifier	x	x	x
IAM 02	Time Service	x	x	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
IAM 03	Online certificate status check	x	x	x
IAM 04	Attestation of dynamic attributes	x	x	x
Broker Service				
BRK 01	Broker service inquiries	-	-	-
BRK 02	Broker registration	-	-	-
BRK 03	Broker registration update	-	-	-
Operating System				
OS 01	Container support	x	x	x
OS 02	App separation	-	-	x
OS 03	Service authenticity and integrity	-	-	x
OS 04	System component authenticity and integrity	-	-	x
OS 05	Container separation	-	-	x
OS 06	Backup encryption	x	x	x
Apps and App Store Connection				
APS 01	App signature	x	x	x
APS 02	App signature verification	x	x	x
APS 03	Terms of use	-	-	x
APS 04	Requirements for the runtime environment	-	-	x
APS 05	App installation	x	x	x
APS 06	App Store	x	x	x
Data Usage Transparency				
AUD 01	Access control logging	x	x	x
AUD 02	Data access logging	x	x	x
AUD 03	Configuration changes logging	x	x	x
AUD 04	Resource availability logging	-	-	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
IDS Specification (Component: Broker)				
General Requirements				
BR-GEN 01	Communication Guide	x	x	x
BR-GEN 02	Self-Description	x	x	x
BR-GEN 03	Minimal endpoint	x	x	x
BR-GEN 04	Logging	x	x	x
Functional Requirements				
BR-FR 01	Information Model for storage	x	x	x
BR-FR 02	HTTPS	x	x	x
BR-FR 03	Types of interaction	x	x	x
BR-FR 04	Authority over metadata	x	x	x
BR-FR 05	IDS Identifiers	x	x	x
BR-FR 06	Vocabulary restriction	x	x	x
BR-FR 07	Content of self-description	x	x	x
Message Requirements				
BR-MR 01	Information Model for messages	x	x	x
BR-MR 02	Incoming messages	x	x	x
BR-MR 03	Message ID	x	x	x
BR-MR 04	DescriptionRequestMessages	x	x	x
BR-MR 05	QueryMessages	x	x	x
BR-MR 06	Rejection of non-conform messages	x	x	x
BR-MR 07	Registration processing	x	x	x
BR-MR 08	Rejection messages	x	x	x
BR-MR 09	DdoS protection	x	x	x
Behavioral Requirements				

ID	Criteria Title	Basic	Advanced Information	Usage Control
BR-BER 01	Rejection of invalid messages	x	x	x
BR-BER 02	Metadata for removed components	x	x	x
BR-BER 03	Metadata updates	x	x	x
Business Requirements				
BR-BUR 01	Handling of usage restrictions	x	x	x
BR-BUR 02	Usage Contracts for already stored metadata	x	x	x
BR-BUR 03	Outlining of usage restrictions and licenses	x	x	x
BR-BUR 04	Selling access to metadata	x	x	x
Query Language Requirements				
BR-QLR 01	Supported query languages	x	x	x
BR-QLR 02	Native query languages	x	x	x
Advanced Information Profile				
BR-AIP 01	Tracking removed components	-	x	-
BR-AIP 02	Verifying availability of components	-	x	-
BR-AIP 03	Search for data sources	-	x	-
BR-AIP 04	Version indicators	-	x	-
BR-AIP 05	Dereferencable URIs	-	x	-
BR-AIP 06	PublishingMessages	-	x	-
BR-AIP 07	Information Model support for incoming messages	-	x	-
BR-AIP 08	External vocabularies	-	x	-
BR-AIP 09	Required endpoints	-	x	-
BR-AIP 10	History feature	-	x	-
Usage Control Profile				
BR-UCP 01	Usage Control engine and enforcement	-	-	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
BR-UCP 02	Data exchange agreements	-	-	x
BR-UCP 03	Limited access to metadata	-	-	x
BR-UCP 04	Behavior for limited access	-	-	x
62443-4-2				
IAC: Identification and authentication control				
CR 1.1	Human user identification and authentication	x	x	x
CR 1.1 (1)	Unique identification and authentication	x	x	x
CR 1.1 (2)	Multifactor authentication for all interfaces	-	-	x
CR 1.2	Software process and device identification and authentication	x	x	x
CR 1.2 (1)	Unique identification and authentication	x[1]	x	x
CR 1.3	Account management	x	x	x
CR 1.4	Identifier management	x	x	x
CR 1.5	Authenticator management	x	x	x
CR 1.5 (1)	Hardware security for authenticators	-	-	x
CR 1.7	Strength of password-based authentication	x	x	x
CR 1.7 (1)	Password generation and lifetime restrictions for human users	-	-	x
CR 1.8	Public key infrastructure certificates	x	x	x
CR 1.9	Strength of public key-based authentication	x	x	x
CR 1.9 (1)	Hardware security for public key-based authentication	-	-	x
CR 1.10	Authenticator feedback	x	x	x
CR 1.11	Unsuccessful login attempts	x	x	x

[1] Requirements from 62443-4-2 marked green in this table extend the 62443 SL. The extension is explained in Application Note of the requirement.

ID	Criteria Title	Basic	Advanced Information	Usage Control
CR 1.12	System use notification	x[2]	x	x
CR 1.14	Strength of symmetric key-based authentication	x	x	x
CR 1.14 (1)	Hardware security for symmetric key-based authentication	-	-	x
UC: Use Control				
CR 2.1	Authorization enforcement	x	x	x
CR 2.1 (1)	Authorization enforcement for all users (humans, software processes and devices)	-	-	x
CR 2.1 (2)	Permission mapping to roles	-	-	x
CR 2.1 (3)	Supervisor override	-	-	x
CR 2.2	Wireless use control	x	x	x
CR 2.5	Session lock	x	x	x
CR 2.6	Remote session termination	-	-	x
CR 2.7	Concurrent session control	-	-	x
CR 2.8	Auditable events	x	x	x
CR 2.9	Audit storage capacity	x	x	x
CR 2.9 (1)	Warn when audit record storage capacity threshold reached	-	-	x
CR 2.10	Response to audit processing failures	x	x	x
CR 2.11	Timestamps	x	x	x
CR 2.11 (1)	Time synchronization	-	-	x
CR 2.11 (2)	Protection of time source integrity	-	-	x
CR 2.12	Non-repudiation	x	x	x

[2] Requirements from 62443-4-2 marked blue in this table are relevant only in an industrial context (i.e. in context of DIN Spec 27070).

ID	Criteria Title	Basic	Advanced Information	Usage Control
CR 2.12 (1)	Non-repudiation for all users	-	-	x
SI: System integrity				
CR 3.1	Communication integrity	x	x	x
CR 3.1 (1)	Communication authentication	x	x	x
CR 3.3	Security functionality verification	x	x	x
CR 3.4	Software and information integrity	x	x	x
CR 3.4 (1)	Authenticity of software and information	-	-	x
CR 3.4 (2)	Automated notification of integrity violations	-	-	x
CR 3.5	Input validation	x	x	x
CR 3.6	Deterministic output	x	x	x
CR 3.7	Error handling	x	x	x
CR 3.8	Session integrity	x	x	x
CR 3.9	Protection of audit information	-	-	x
DC: Data confidentiality				
CR 4.1	Information confidentiality	x	x	x
CR 4.2	Information persistence	-	-	x
CR 4.2 (1)	Erase of shared memory resources	x	x	x
CR 4.2 (2)	Erase verification	-	-	x
CR 4.3	Use of cryptography	x	x	x
RDF: Restricted data flow				
CR 5.1	Network segmentation	x	x	x
TRE: Timely response to events				
CR 6.1	Audit log accessibility	x	x	x
CR 6.1 (1)	Programmatic access to audit logs	-	-	x
CR 6.2	Continuous monitoring	-	-	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
RA: Resource availability				
CR 7.1	Denial of service protection	x	x	x
CR 7.1 (1)	Manage communication load from component	-	-	x
CR 7.2	Resource management	x	x	x
CR 7.3	Control system backup	x	x	x
CR 7.3 (1)	Backup integrity verification	-	-	x
CR 7.4	Control system recovery and reconstitution	x	x	x
CR 7.6	Network and security configuration settings	x	x	x
CR 7.6 (1)	Machine-readable reporting of current security settings	-	-	x
CR 7.7	Least functionality	x	x	x
CR 7.8	Control system component inventory	-	-	x
NDR: Network device requirements				
NDR 1.6	Wireless Access Management	x	x	x
NDR 1.6 (1)	Unique identification and authentication	-	-	x
NDR 1.13	Access via untrusted networks	x	x	x
NDR 1.13 (1)	Explicit access request approval	-	-	x
NDR 2.4	Mobile code	x	x	x
NDR 2.4 (1)	Mobile code authenticity check	-	-	x
NDR 2.13	Use of physical diagnostic and test interfaces	-	-	x
NDR 2.13 (1)	Active monitoring	-	-	x
NDR 3.2	Protection from malicious code	x	x	x
NDR 3.10	Support for updates	x	x	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
NDR 3.10 (1)	Update authenticity and integrity	-	-	x
NDR 3.11	Physical tamper resistance and detection	-	-	x
NDR 3.11 (1)	Notification of a tampering attempt	-	-	x
NDR 3.12	Provisioning product supplier roots of trust	-	-	x
NDR 3.13	Provisioning asset owner roots of trust	-	-	x
NDR 3.14	Integrity of the boot process	x	x	x
NDR 3.14 (1)	Authenticity of the boot process	-	-	x
NDR 5.2	Zone boundary protection	x	x	x
NDR 5.2 (1)	Deny all, permit by exception	-	-	x
NDR 5.2 (2)	Island mode	-	-	x
NDR 5.2 (3)	Fail close	-	-	x
NDR 5.3	General purpose, person-to-person communication restrictions	x	x	x
Secure Development				
D: Development Documentation				
D_AD.1	Secure initialisation	x	x	x
D_AD.2	Tamper protection	x	x	x
D_AD.3	Security-enforcing mechanisms	x	x	x
D_IS.1	Interface purpose and usage	x	x	x
D_IS.2	Interface parameters	x	x	x
D_IS.3	Error messages	-	-	x
D_DD.1	Subsystem structure	x	x	x
D_DD.2	Module structure	-	-	x
D_DD.3	Subsystem-Module mapping	-	-	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
D_DD.4	Parameters, invocation conventions and return values	-	-	x
D_SC.1	Source code	-	-	x
G: Guidance Documentation				
G_AP.1	Acceptance procedures	x	x	x
G_AP.2	Installation procedures	x	x	x
G_OG.1	Interface usage for each user role	x	x	x
G_OG.2	Possible modes of operation	x	x	x
S: Secure Development				
S_CM.1	Unique component reference	x	x	x
S_CM.2	Consistent usage of component reference	x	x	x
S_CM.3	Configuration management access control measures	-	-	x
S_CM.4	Automated procedures for production	-	-	x
S_CM.5	Component reflecting source code	-	-	x
S_CM.6 (1)	Configuration list content (1)	x	x	x
S_CM.6 (2)	Configuration list content (2)	-	-	x
S_CM.7	Unique identification based on configuration list	x	x	x
S_CM.8	Developer Information	x	x	x
S_DL.1	Secure delivery	x	x	x
S_DS.1	Operational security measures	-	-	x
S_FR.1	Tracking of reported security flaws	x	x	x
S_FR.2	Security flaw description	x	x	x
S_FR.3	Status of corrective measures	x	x	x
S_FR.4	Safeguards	-	-	x

ID	Criteria Title	Basic	Advanced Information	Usage Control
S_FR.5	Contact for user reports and enquires	-	-	x
S_LC.1	Life-cycle model	-	-	x
T: Developer Testing				
T_CA.1	Test coverage analysis	x	x	x
T_CA.2	Test procedures for subsystems	x	x	x
T_CA.3	Test procedures for interfaces	-	-	x
T_TD.1	Test documentation	x	x	x
T_TD.2	Test configuration	x	x	x
T_TD.3	Ordering Dependencies	x	x	x

3 IDS Specification (Component)

3.1 Communication Integrity

COM 01 Protected connection

Connectors communicate with each other only via authenticated, encrypted and integrity protected connections.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

COM 02 Mutual authentication

Connector certificates (see DIN SPEC 6.4.5) facilitate mutual authentication of Connectors every time connection is established.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

COM 03 State of the art cryptography

Encryption and integrity protection is facilitated by means of mechanisms considered state of the art by BSI TR 02102-1, NIST SP 800-175b, or an equivalent crypto catalouge.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

COM 04 Remote attestation

Connectors allow each other to check integrity of each other's software stack via remote attestation.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

COM 05 Platform integrity

Proof of integrity refers to the deployed Core Container and all necessary platform dependencies (kernel, bootloader or platform integrity for Trusted Execution Environment).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Depending on the way COM 06 is implemented, in certain instances, integrity can be reached without implementing COM 05.

COM 06 Configuration and app integrity

Proof of integrity additionally refers to Connector's

a) configuration and

b) apps installed.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

3.2 Data Usage Control

USC 03 Usage policy enforcement

Connector facilitates technical enforcement of data usage policy specified.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

USC 04 Usage policy changes

Changes to data usage policy can be made only by the data owner or data provider. In case of changes made to policy, connection between two Connectors is re-established.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

This is necessary in cases in which the Connector requesting data does not meet the requirements regarding the data usage policy anymore.

USC 05 Usage policy changes by administrator

The administrators of the data provider side cannot change rules regarding data flow without data provider taking notice of the change and approving it.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

3.3 Information Model

INF 01 Self-Description (at Connector)

Connector provides self-description (i.e. metadata) via a defined interface.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

INF 03 Self-Description content

The self-description contains at least the following information:

a) cryptographic hash of Connector certificate,

b) Connector operator,

c) data endpoints offered by Connector,

d) log format of data endpoints offered,

e) security profile of Connector (i.e. security features supported),

f) Connector ID.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

INF 05 Dynamic attribute tokens

Dynamic attribute tokens belonging to two communicating Connectors are transmitted every time a connection is established (see DIN Spec 6.4.2) and can therefore be used for access control decisions.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

3.4 Identity and Access Management

IAM 01 Connector identifier

Connector is unambiguously identified by means of an identifier derived from a X.509v3 certificate (see also CR 1.2 (1)).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

IAM 02 Time Service

Connector supports central time service (e.g. to verify certificates).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

IAM 03 Online certificate status check

Connector supports online status check of certificates issued (e.g. Online Certificate Status Protocol, OCSP).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

IAM 04 Attestation of dynamic attributes

Connector supports the external attestation of dynamic attributes, from which it receives certified attribute information (e.g. through JSON Web Tokens).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

3.5 Operating System

OS 01 Container support

Connector supports installation and execution of containers.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

OS 02 App separation

Connector enforces strict separation of data processing apps. Communication between apps takes place via approved channels only (i.e. whitelisting of data exchange channels).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

OS 03 Service authenticity and integrity

Connector verifies authenticity and integrity of data services prior to installation and execution.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

OS 04 System component authenticity and integrity

Connector verifies authenticity and integrity of all system components prior to execution.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

OS 05 Container separation

Containers are strictly separated from each other and from underlying operating system layers.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

OS 06 Backup encryption

System data backups as well as backups of data transferred between Connectors are always encrypted before being stored outside system.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

3.6 Apps and App Store Connection

APS 01 App signature

Connector supports only apps possessing a valid signature. This signature is the signed check sum of the software artefact, which was created by means of a private key of the app publisher.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

APS 02 App signature verification

Connector verifies signature after app was downloaded and before it is installed, and before every execution of app. Public key of app publisher is contained in an X.509v3 certificate signed by a Certification Authority accepted by data provider and data consumer.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

APS 03 Terms of use

Connector supports apps carrying terms of use, allowing restriction of use and encapsulation of licensing information.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

APS 04 Requirements for the runtime environment

Connector checks minimum requirements of apps regarding runtime environment (e.g. with regard to memory capacity or number of CPU cores) and ensures these requirements are fulfilled as long as app is active.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Among other things, this requirement is important to ensure that the use of an app does not impair the functionality of other apps (or of the Connector itself).

APS 05 App installation

Connector supports apps delivered and installed as independent software containers (i.e. apps bring along possible dependencies of e.g. software modules themselves and can be used irrespective of Connector's configuration).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

APS 06 App Store

Connector receives apps from a central app store.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

3.7 Data Usage Transparency

AUD 01 Access control logging

Connector logs each access control decision in the form of an integrity protected log entry in its domain.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

AUD 02 Data access logging

Connector logs every access to data in the form of an integrity protected entry in its domain.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

AUD 03 Configuration changes logging

Connector logs any changes made to its configuration in the form of integrity protected entries in its domain.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

AUD 04 Resource availability logging

Connector logs every case in which a service receives fewer resources than requested (e.g. fewer RAM capacity).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

4 IDS Specification (Component: Broker)

4.1 General Requirements

BR-GEN 01 Communication Guide

The communication between a Connector and an IDS Meta Data Broker relies on the general IDS communication between two connectors as specified by the IDS Communication Guide at least of Version 1.0. Thus, the communication of an IDS Meta Data Broker must not act contrary to the communication guide.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-GEN 02 Self-Description

An IDS Meta Data Broker must provide a Self-Description document at

<scheme>://<authority>[:port][/path/to/broker]/ according to the IDS Information Model version it announced.

- Basic Broker Profile: x

- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-GEN 03 Minimal endpoint

An IDS Meta Data Broker must have at least one of the following:

a) an HTML-based UI at https://<authority>[:port][/path/to/broker]/browse

b) an HTTPS endpoint for IDS Multipart messages at https://<authority>[:port][/path/to/broker]/infrastructure.

c) an IDS-CP socket at idscp://<authority>[:port]/ responding to Broker-related messages.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-GEN 04 Logging

An IDS Meta Data Broker has to protocol all executed actions or queries. This log is used for error and problem report and is not public and sufficiently protected. Log request must be addressed to the admin and management team of the broker. Retention time of the log is specified by the International Data Spaces.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.2 Functional Requirements

BR-FR 01 Information Model for storage

An IDS Meta Data Broker must provide capabilities to persistently store metadata conforming to the IDS Information Model. The conforming Information model has to be at least of version 3.0.0.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 02 HTTPS

The default interaction protocol of an IDS Meta Data Broker is HTTPS.

A usage of unsecured HTTP is not allowed.

Additional protocols may be implemented.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 03 Types of interaction

An interaction not meant for meta-data retrieval with an IDS Meta Data Broker contains exactly one of the following functions (see also Figure 1):

a) Register (a new entry)

b) Update (an existing entry)

c) Passivate (an existing entry)

d) Activate (an existing entry)

e) Remove (an existing entry)

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 04 Authority over metadata

Only the according Sovereign (defined according to IDS RAM 3.0) may register, change, or delete Connector or Resource metadata. Following restrictions apply:

a) The Sovereign can authorize a third party with this task, for instance if the Sovereign itself does not operate an own IDS Connector. In this case, the requesting Connector must supply an IDS AuthorizationToken proofing his permission. The IDS Meta Data Broker must verify this AuthorizationToken before executing the requested task.

b) An IDS Meta Data Broker Operator is allowed to administer the contained data. In particular, an IDS Meta Data Broker Operator is allowed to delete or passivate metadata if it holds trustworthy indications that for instance the respective Connector Resource left an

International Data Space or stopped responding. In any case, an IDS Meta Data Broker Operator must not manipulate metadata in any way resulting in wrong information.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 05 IDS Identifiers

The identifier of all IDS Resources contains a unique character sequence, which is assigned by an authorized Connector. Connectors must receive their identity key from an IDS Identity Provider. This key is based on an URI, which has to be resolvable for all IDS members (must not contain localhost or local IP addresses). This URI is called the IDS Identifier. An IDS-Meta Data Broker is required to check the uniqueness and integrity of these Identifiers and reject any violating Resource Updates.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 06 Vocabulary restriction

An index service must not store external RDF vocabularies, not belonging to the Information Model. See IDS-RAM 3.0 explanations for Vocabulary Hubs.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-FR 07 Content of self-description

In difference to other Connectors the Self-Description of an IDS Meta Data Broker has to be supplied at a specified URL (http(s)://<broker.authority>[:port]/<path to broker root>) and gives additional information about the index service. This information contains at least:

a) supported (native) query languages

b) supported identity providers (like Connector)

c) available add-on service (like data endpoints)

d) publication of local index service rules (→ B18)

Additional obligatory information may be specified in the respective information model version and must be supported.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.3 Message Requirements

BR-MR 01 Information Model for messages

An IDS Meta Data Broker must announce the supported IDS Information Model versions for outbound and inbound messages through its Self-Description document.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 02 Incoming messages

An IDS Meta Data Broker supports the following incoming messages:

a) Update Messages from a Connector, as defined in the Information Model

b) Description Request Messages

c) Query Messages in the native Query Language

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 03 Message ID

Every Message contains a unique messageID (URI). The corresponding ResponseMessages must contain this messageID as a correlationMessage attribute.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x

- Usage Control Broker Profile: x

BR-MR 04 DescriptionRequestMessages

A DescriptionRequestMessage sent to an IDS Meta Data Broker targets at most one of the following IDS entities identified by their own specific URI:

a) a Connector

b) a Resource

c) a Catalog

If not provided with an URI a DescriptionRequestMessage has to be interpreted as a Request of a SelfDescription of the Broker. If provided with an URI for its own Catalog, the IDS Meta Data Broker must provide at least a list of all available Resources.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 05 QueryMessages

A QueryMessage send to an IDS Meta Data Broker contains exactly one action:

a) Query (one or multiple meta datasets by a query expression)

An IDS Meta Data broker must reject QueryMessages that have another intention then Queryieng, for example Update Queries.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 06 Rejection of non-conform messages

An IDS Meta Data Broker must reject messages if they do not conform to the IDS Information Model.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 07 Registration processing

If An IDS Meta Data Broker accepts a registration attempt, it must acknowledge it using a MessageProcessedNotification. A MessageProcessedNotification must not be sent if the indexing led to an error.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 08 Rejection messages

If an IDS Meta Data Broker denies a Message (for non-security related reasons), it must inform the connector with a RejectionMessage with a RejectionCode and an explanation message. This must in particular work for the following error cases:

a) messages with a wrong syntax

b) provision of an invalid security token

c) denying of access because requirements are not met

d) unavailable resources

e) unsupported message types

f) unsupported versions of the Information Model

g) internal errors

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-MR 09 DdoS protection

An IDS Meta Data Broker must support the prevention of DDoS attacks by blocking a distinct Connector for an arbitrary period based on internal rules. If such a rule is triggered, no ResponseMessage must be send, not even a RejectionMessage.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.4 Behavioral Requirements

BR-BER 01 Rejection of invalid messages

In case an invalid or corrupted message is received, An IDS Meta Data Broker must reject it.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-BER 02 Metadata for removed components

An IDS Meta Data Broker must not present data of a removed or passivated component after its removing has been acknowledged to the requesting entity.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-BER 03 Metadata updates

An IDS Meta Data Broker must allow updates of a registered IDS Connector if the update request was originally initiated by this Connector, or by the IDS entity controlling the Connector, if this relation has been made visible to the Broker.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.5 Business Requirements

BR-BUR 01 Handling of usage restrictions

In case an IDS Meta Data Broker supports usage restrictions on meta data, it must outline these restrictions to requesting connectors and enforce the restrictions for received meta data. If an IDS Meta Data Broker cannot enforce a requested usage restriction, it must reject the meta data.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-BUR 02 Usage Contracts for already stored metadata

In case an IDS Meta Data Broker accepts an IDS Usage Contract describing usage restrictions targeting a already/previously stored metadata element, an IDS Meta Data Broker must also enforce the contained restrictions. If an IDS Meta Data Broker cannot enforce the Usage Contract, it must reject it.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-BUR 03 Outlining of usage restrictions and licenses

An IDS Meta Data Broker must outline usage restrictions and licenses for data as far as it is aware of them and allowed to share them.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-BUR 04 Selling access to metadata

If an IDS Meta Data Broker sells the access to its data content:

a) IDS Meta Data Broker must outline how data can be bought and which usage restriction or license applies.

b) an IDS Meta Data Broker must provide »One Click« agreement

c) an IDS Meta Data Broker must be able to execute a Transaction Accounting

d) an IDS Meta Data Broker must be able to send notifications to an IDS Clearing House for Data Exchange Clearing

e) if a ContractAgreementMessage has been acknowledged by a Broker and another entity, an IDS Meta Data Broker must behave according to this Agreement.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.6 Query Language Requirements

BR-QLR 01 Supported query languages

SPARQL is the query language of the Semantic Web and Linked Data. IDS Meta Data Brokers may accept SPARQL queries as payloads of QueryMessages but can also provide support for path-based query languages (JSON-Path, XPath, ...), other graph-related query languages (Gremlin) or any other standardized query language. If an IDS Meta Data Broker provides querying possibilities, it must indicate the supported languages in their Self-Description.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

BR-QLR 02 Native query languages

Some persistence technologies provide native query languages, which might not be standardized. An index-service may allow native queries in BrokerQueryMessages which is not obligatory. Here is a list of native query languages:

SQL ==> RDBMS (B24 c)

LDAP-Query ==> LDAP / AD (B24 d)

SPARQL ==> RDF(B24 e) and as an additional component:

full-text search ==> query engine like Apache Lucene (B24 a-e)

If such native query languages are implemented in the Broker, they must be stated within an IDS Meta Data Brokers Self Description like other supported query languages.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

4.7 Advanced Information Profile

BR-AIP 01 Tracking removed components

An IDS Meta Data Broker must keep track of removed components.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 02 Verifying availability of components

An IDS Meta Data Broker must daily verify the existence of its indexed IDS components and synchronize its indexed meta-data with the components self-descriptions.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 03 Search for data sources

An IDS Meta Data Broker supports the search for data sources offered by Connectors. Possible search criteria are key words, taxonomies, multi-criteria facets.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 04 Version indicators

An IDS Meta Data Broker must provide version indicators, outlining that metadata has been updated. If implemented, one of the following solutions has to be applied:

a) the unique metadata key (URI) contains a version number (not recommended),

b) the metadata contains a version number, which is incremented by the Connector or an IDS Meta Data Broker.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 05 Dereferencable URIs

IDS Participants should use dereferencable URIs according to the Linked Data Principles (Linked Data - Design Issues1) for increased interoperability. An IDS Meta Broker must check the deferenced URIs for their validity and availability.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 06 PublishingMessages

An IDS Meta Data Broker is responsible of validating the content of received PublishingMessages. This contains following cases

a) a Connector can be reached as described by the metadata

b) a Connector exposes a data endpoint as published in the metadata

c) a RDF vocabulary is available at the given URL

If the information is invalid, the broker message must be rejected, if it is not capable of correcting it.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 07 Information Model support for incoming messages

An IDS Meta Data Broker must support more than one major IDS Information Model versions for incoming messages.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 08 External vocabularies

An IDS Meta Data Broker may support external vocabularies for component or data resource descriptions. In this case, an IDS Meta Data Broker must provide links to further information about these vocabularies (cf. Vocabulary Hub).

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 09 Required endpoints

An IDS Meta Data Broker must offer the following interfaces:

a) an HTML-based UI at /browse and

b) an HTTPS endpoint for IDS Multipart messages at /infrastructure and

c) an IDSCP socket at idscp://<authority>[:port]/

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

BR-AIP 10 History feature

An IDS Meta Data Broker may provide a history feature for changed or deleted metadata. If available, a QueryMessage that contains a timestamp or a version number and the Broker must return the meta data that was valid at that point in time or in that version.

- Basic Broker Profile: -
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: -

4.8 Usage Control Profile

BR-UCP 01 Usage Control engine and enforcement

An IDS Meta Data Broker must implement at least one usage control engine, which can interpret and enforce IDS Usage Contracts as specified by the IDS Information Model. The used technologies should be clearly outlined, together with information what can and cannot be enforced by the Usage Control engines.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

BR-UCP 02 Data exchange agreements

Where an IDS Meta Data Broker has the legal rights to do so, it should be able to negotiate or at least provide data exchange agreements for stored Meta-Data.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

BR-UCP 03 Limited access to metadata

An IDS Meta Data Broker must filter or prohibit access to indexed metadata if the data sovereign demands this in the accepted IDS Usage Contracts for the Meta Data.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

BR-UCP 04 Behavior for limited access

If demanded by the accepted IDS Usage Contracts, an IDS Meta Data broker must either

a) indicate that a rule or contract inhibits access or

b) pretend that the requested information does not exist.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5 62443-4-2

5.1 IAC: Identification and authentication control

CR 1.1 Human user identification and authentication

The component shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

An "IDS user" that interacts directly with a Connector is not forseen. Within the scope of IDS-evaluations, all IAC requirements therefore relate to administrative users.

CR 1.1 (1) Unique identification and authentication

The component shall provide the capability to uniquely identify and authenticate all human users.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.1 (2) Multifactor authentication for all interfaces

The component shall provide the capability to employ multifactor authentication for all human user access to the component.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 1.2 Software process and device identification and authentication

The component shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 SR1.2.

If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to IEC 62443-3-3 SR1.1 may be part of the component identification and authentication process towards the other components.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.2 (1) Unique identification and authentication

The component shall provide the capability to uniquely and securely identify and authenticate itself to any other component.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.3 Account management

The component shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 62443-3-3 SR 1.3.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.4 Identifier management

The component shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to IEC62443-3-3 SR 1.4.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

For IDS Connectors, the system is the PKI managing the Connector Identifiers.

CR 1.5 Authenticator management

Components shall provide the capability to:

a) support the use of initial authenticator content;

b) support the recognition of changes to default authenticators made at installation time;

c) function properly with periodic authenticator change/refresh operation; and

d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.5 (1) Hardware security for authenticators

The authenticators on which the components rely shall be protected via hardware mechanisms.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 1.7 Strength of password-based authentication

For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The requirement CR 1.7 (together with (1) and (2)) is not mapped to the Base Connector, as it is expected to only support user accounts with OS-level admin privileges, so that this requirement can not be technically enforced.

In order to nevertheless fulfill these state-of-the-art password requirements, respective

instructions for the administrator are expected to be contained in the guidance documentation for the component.

CR 1.7 (1) Password generation and lifetime restrictions for human users

The component shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

For all IDS components that support the setting of the password lifetime, only the setting of the maximum lifetime is mandatory.

The component should provide the capability to prompt the user to change their password upon a configurable time prior to expiration.

CR 1.8 Public key infrastructure certificates

When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 SR1.8.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.9 Strength of public key-based authentication

For components that utilize public key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to:

a) validate certificates by checking the validity of the signature of a given certificate;

b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;

c) validate certificates by checking a given certificate's revocation status;

d) establish user (human, software process or device) control of the corresponding private key;

e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; and

f) ensure that the algorithms and keys used for the public key authentication conform to 8.5.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Regarding item m) above: Usage of self-signed certificates is not compliant with IDS.

CR 1.9 (1) Hardware security for public key-based authentication

Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 1.10 Authenticator feedback

When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authentication information during the authentication process.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.11 Unsuccessful login attempts

When a component provides an authentication capability, the component shall provide the capability to:

a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and

b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached. An administrator may unlock an account prior to the expiration of

the timeout period.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.12 System use notification

When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

This requirement is only relevant for IDS Connectors in the industrial domain. Further domains might be added in a later version of this catalogue.

CR 1.14 Strength of symmetric key-based authentication

For components that utilize symmetric keys, the component shall provide the capability to:

v) establish the mutual trust using the symmetric key;

w) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);

x) restrict access to the shared secret; and

y) ensure that the algorithms and keys used for the symmetric key authentication conform to 8.5.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 1.14 (1) Hardware security for symmetric key-based authentication

Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5.2 UC: Use Control

CR 2.1 Authorization enforcement

The component shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

An "IDS user" that interacts directly with a Connector is not forseen. Within the scope of IDS-evaluations, all IAC requirements therefore relate to administrative users.

CR 2.1 (1) Authorization enforcement for all users (humans, software processes and devices)

The component shall provide an authorization enforcement mechanism for all users based on

their assigned responsibilities and least privilege.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

For the Base Connector, this requirement can not be technically enforced as it is expected to only support user accounts with admin privileges.

CR 2.1 (2) Permission mapping to roles

The component shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users. Roles should not be limited to fixed nested hierarchies in which a higher-level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

This RE is applicable to software processes and devices as well.

CR 2.1 (3) Supervisor override

The component shall support a supervisor manual override for a configurable time or sequence of events.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Implementation of a controlled, audited and manual override of automated mechanisms in the event

of emergencies or other serious events allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human

user.

CR 2.2 Wireless use control

If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.5 Session lock

If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability

a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and

b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.6 Remote session termination

If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 2.7 Concurrent session control

The component shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 2.8 Auditable events

The component shall provide the capability to generate audit records relevant to security for the following categories:

a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events.

Individual audit records shall include:

g) timestamp; h) source (originating device, software process or human user account); i) category; j) type; k) event ID; and l) event result.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.9 Audit storage capacity

The component shall

a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and

b) provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.9 (1) Warn when audit record storage capacity threshold reached

The component shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 2.10 Response to audit processing failures

The component shall

a) provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and

b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

For the Connector, the focus in case of audit failures is on ensuring data security, not availability.

CR 2.11 Timestamps

The component shall provide the capability to create timestamps (including date and time) for use in audit records.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.11 (1) Time synchronization

The component shall provide the capability to create timestamps that are synchronized with a system-wide time source.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 2.11 (2) Protection of time source integrity

The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 2.12 Non-repudiation

If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action.

Control elements that are not able to support such capability shall be listed in component documents.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 2.12 (1) Non-repudiation for all users

The component shall provide the capability to determine whether a given user (human, software process or device) took a particular action.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5.3 SI: System integrity

CR 3.1 Communication integrity

The component shall provide the capability to protect integrity of transmitted information.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.1 (1) Communication authentication

The component shall provide the capability to verify the authenticity of received information during communication.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Communication authentication can be achieved with or without communication confidentiality (encryption).

CR 3.3 Security functionality verification

Components shall provide the capability to support verification of the intended operation of security functions according to IEC 62443-3-3 SR3.3.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.4 Software and information integrity

Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.4 (1) Authenticity of software and information

Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 3.4 (2) Automated notification of integrity violations

If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 3.5 Input validation

The component shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.6 Deterministic output

Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

This requirement is only relevant for IDS Connectors in the industrial domain. Further domains might be added in a later version of this catalogue.

CR 3.7 Error handling

Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.8 Session integrity

The component shall provide mechanisms to protect the integrity of communications sessions including:

a) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions);

b) the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and

c) the capability to generate unique session identifiers with commonly accepted sources of randomness.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 3.9 Protection of audit information

Components shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5.4 DC: Data confidentiality

CR 4.1 Information confidentiality

The component shall

a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

b) support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 SR 4.1.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

For the Base Connector, only supporting the protection of the confidentiality of information in transit is required.

CR 4.2 Information persistence

The component shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 4.2 (1) Erase of shared memory resources

The component shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Volatile memory resources are those that generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the control system for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.

CR 4.2 (2) Erase verification

The component shall provide the capability to verify that the erasure of information occurred.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 4.3 Use of cryptography

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

5.5 RDF: Restricted data flow

CR 5.1 Network segmentation

Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

5.6 TRE: Timely response to events

CR 6.1 Audit log accessibility

The component shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 6.1 (1) Programmatic access to audit logs

The component shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 6.2 Continuous monitoring

Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5.7 RA: Resource availability

CR 7.1 Denial of service protection

Components shall provide the capability to maintain essential functions when operating in a degraded mode during a DoS event.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.1 (1) Manage communication load from component

The component shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 7.2 Resource management

The component shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.3 Control system backup

The component shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.3 (1) Backup integrity verification

The component shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

CR 7.4 Control system recovery and reconstitution

The component shall provide the capability to recovered and reconstitute to a known secure state after a disruption or failure.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.6 Network and security configuration settings

The component shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.6 (1) Machine-readable reporting of current security settings

The component shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -

- Usage Control Broker Profile: x

CR 7.7 Least functionality

The component shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

CR 7.8 Control system component inventory

The component shall provide the capability to support a control system component inventory according to IEC62443-3-3 SR 7.8.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

5.8 NDR: Network device requirements

NDR 1.6 Wireless Access Management

A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 1.6 (1) Unique identification and authentication

The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 1.13 Access via untrusted networks

The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 1.13 (1) Explicit access request approval

The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 2.4 Mobile code

In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the network device:

a) Control execution of mobile code;

b) control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; and

c) control the code execution based upon integrity checks on mobile code and prior to the code being executed.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 2.4 (1) Mobile code authenticity check

The network device shall provide the capability to enforce a security policy that allows the

device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 2.13 Use of physical diagnostic and test interfaces

Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g., JTAG debugging).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 2.13 (1) Active monitoring

Network devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

If all debug interfaces are deactivated, monitoring is not needed.

NDR 3.2 Protection from malicious code

The network device shall provide for protection from malicious code.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 3.10 Support for updates

Network devices shall support the ability to be updated and upgraded.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 3.10 (1) Update authenticity and integrity

Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 3.11 Physical tamper resistance and detection

Network devices shall provide anti-tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 3.11 (1) Notification of a tampering attempt

Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 3.12 Provisioning product supplier roots of trust

Network devices shall provide the capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 3.13 Provisioning asset owner roots of trust

Network devices shall a) provide the capability to provision and protect the confidentiality, integrity and authenticity of asset owner keys and data to be used as “roots of trust”; and b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 3.14 Integrity of the boot process

Network devices shall verify the integrity of the firmware, software and configuration data needed for the component’s boot process prior to it being used in the boot process.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

NDR 3.14 (1) Authenticity of the boot process

Network devices shall use the component’s product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 5.2 Zone boundary protection

A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the riskbased zones and conduits model.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

If no zones boundaries are touched, this requirement does not need to be fulfilled.

NDR 5.2 (1) Deny all, permit by exception

The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception)

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 5.2 (2) Island mode

The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 5.2 (3) Fail close

The network component shall proide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

NDR 5.3 General purpose, person-to-person communication restrictions

A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

6 Secure Development

6.1 D: Development Documentation

D_AD.1 Secure initialisation

The development documentation shall include an architectural description stating how the component preserves security during initialisation, i.e. how an initial secure state is reached.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The information provided by the developer relating to the initialisation of the security functionality is directed at the parts that are involved in bringing the security functionality into an initial secure state (i.e. when all parts are operational) when power-on or a reset is applied. This description should list the system initialisation parts and the processing that occurs in transitioning from the "down" state to the initial secure state.

Note 2: It is often the case that the components that perform this initialisation function are not accessible after the secure state is achieved; if this is the case then the description shall identify these components and explain how they are not reachable by untrusted entities after the security functionality has been established. In this respect, the property that needs to be preserved is that these components either 1) cannot be accessed by untrusted entities after the secure state is achieved, or 2) if they provide interfaces to untrusted entities, these interfaces cannot be used to tamper with the security functionality.

D_AD.2 Tamper protection

The development documentation shall include an architectural description stating how the component is able to protect itself from tampering by untrusted active entities.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: "Self-protection" refers to the ability of the component to protect itself from manipulation from external entities that may result in changes to its security functionality. For the purpose of the development documentation, the notion of self-protection applies only to the services provided by the component through its interfaces, and not to services provided by underlying IT entities that it uses.

Note 2: Self-protection is typically achieved by a variety of means, ranging from physical and logical restrictions on access to the component; to software-based means (e.g. boundary checking of inputs on a trusted server); to hardware-based means (e.g. "execution rings" and memory management functionality). The developer shall ensure that all such mechanisms are described.

Note 3: The developer shall ensure that the development documentation covers how user input is handled by the component in such a way that the security functionality is not subject to being corrupted by that user input. For example, the security functionality might implement the notion of privilege and protect itself by using privileged-mode routines to handle user input. The component might implement software protection constructs or coding conventions that contribute to implementing separation of software domains, perhaps by delineating user address space from system address space. And the security functionality might be reliant on its environment to provide some support to the protection of the security functionality.

All mechanisms contributing to domain separation are to be described.

D_AD.3 Security-enforcing mechanisms

The development documentation shall include an architectural description containing an analysis that adequately describes how the security-enforcing mechanisms of the component cannot be bypassed.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: Non-bypassability is a property of the component, meaning that the security functionality is always invoked. For example, if access control to files is specified as a capability of the component, there must be no interfaces through which files can be accessed without invoking the access control mechanism (such as an interface through which a raw disk access takes place).

Note 2: Suppose there is a interface whose sole purpose is to display the time of day. The description would have to adequately make it clear that this interface is not capable of manipulating any protected resources and does not invoke any security functionality.

D_IS.1 Interface purpose and usage

The development documentation shall include an interface specification stating the purpose of and method of use for each interface of the component.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The purpose of a interface is a general statement summarising the functionality provided by the interface. It is not intended to be a complete statement of the actions and results related to the interface, but rather a statement to help the evaluator understand in general what the interface is intended to be used for.

Note 2: The method of use for a interface summarises how the interface is manipulated in order to invoke the actions and obtain the results associated with the interface. From the description it should become clear how to use each interface. Different types of interfaces will require different method of use specifications. APIs, network protocol interfaces, system configuration parameters, and hardware bus interfaces all have very different methods of use, and this should be taken into account by the developer when writing the interface specification.

Note 3: For administrative interfaces whose functionality is documented as being inaccessible to untrusted users, the functional description describes the method of making the functions inaccessible.

D_IS.2 Interface parameters

The development documentation shall include an interface specification completely and accurately describing all parameters associated with every interface.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: Parameters are explicit inputs or outputs to an interface that control the behaviour of that interface. For examples, parameters are the arguments supplied to an API; the various fields in packet for a given network protocol; etc.

Note 2: A parameter description tells what the parameter is in some meaningful way. For instance, the interface foo(i) could be described as having “parameter i which is an integer”; this is not an acceptable parameter description. A description such as “parameter i is an integer that indicates the number of users currently logged in to the system” is much more acceptable.

D_IS.3 Error messages

The development documentation shall include an interface specification completely and accurately describing all errors messages and their meaning resulting from an invocation of each interface.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: Errors (and the associated error messages) come about through the invocation of an interface. The processing that occurs in response to the interface invocation may encounter error conditions, which trigger (through an implementation-specific mechanism) an error message to be generated. In some instances this may be a return value from the interface itself; in other instances a global value may be set and checked after the invocation of an interface.

Note 2: Errors can take many forms, depending on the interface being described. For an API, the interface itself may return an error code; set a global error condition, or set a certain parameter with an error code. For a configuration file, an incorrectly configured parameter may cause an error message to be written to a log file.

Note 3: In order to determine accuracy, the meaning of the error must be clear. For example, if an interface returns a numeric code of 0, 1, or 2, one would not be able to understand the error if the interface specification only listed: “possible errors resulting from invocation of the foo() interface are 0, 1, or 2”. Instead the the errors shall be described such as: “possible errors resulting from invocation of the foo() interface are 0 (processing successful), 1 (file not found), or 2 (incorrect filename specification)”.

D_DD.1 Subsystem structure

The development documentation shall include a design description stating the structure of the entire component in terms of subsystems.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The description shall identify all of the subsystems of the component. This requirement is on the entire component rather than on only the security functionality.

D_DD.2 Module structure

The development documentation shall include a design description stating the structure of the entire component in terms of modules.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Unlike subsystems, modules describe the implementation in a level of detail that can later serve the evaluator as a guide to reviewing the source code. A description of a module should be such that one could create an implementation of the module from the description, and the resulting implementation would be 1) identical to the actual implementation in terms of the interfaces presented, 2) identical in the use of interfaces that are mentioned in the design, and 3) functionally equivalent to the description of the purpose of the module.

For instance, RFC 793 provides a high-level description of the TCP protocol. It is necessarily implementation independent. While it provides a wealth of detail, it is not a suitable design description because it is not specific to an implementation. An actual implementation can add to the protocol specified in the RFC, and implementation choices (for instance, the use of global data vs. local data in various parts of the implementation) may have an impact on the analysis that is performed. The design description of the TCP module would list the interfaces presented by the implementation (rather than just those defined in RFC 793), as well as an algorithm description of the processing associated with the modules

implementing TCP (assuming it was part of the security functionality).

D_DD.3 Subsystem-Module mapping

The development documentation shall include a design description stating a mapping between the subsystems and the modules.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The developer can provide a simple mapping showing how the modules are allocated to the subsystems. All subsystems must map to at least one module, and all modules must map to exactly one subsystem.
Note 2: An "inaccurate" mapping is one where the module is mistakenly associated with a subsystem where its functions are not used within the subsystem.

D_DD.4 Parameters, invocation conventions and return values

The development documentation shall include a design description containing a complete description of the security-related parameters, the invocation conventions for each module interface, and any values returned directly by the interface.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The security-related interfaces of a module are those interfaces used by other modules as a means to invoke the security-related operations provided, and to provide inputs to or receive outputs from the module. The purpose in the specification of these interfaces is to permit the exercise of them during testing. Inter-module interfaces that are not security-related need not be specified or described, since they are not a factor in testing. Likewise, other internal interfaces that are not a factor in traversing security-related paths of execution (such as those internal paths that are fixed) need not be specified or described, since they are not a factor in testing.

Note 2: Security-related interfaces are described in terms of how they are invoked, and any values that are returned. This description would include a list of security-related parameters, and descriptions of these parameters. Note that global data would also be considered parameters if used by the module (either as inputs or outputs) when invoked. If a parameter were expected to take on a set of values (e.g., a "flag" parameter), the complete set of values the parameter could take on that would have an effect on module processing would be specified. Likewise, parameters representing data structures are described such that each field of the data structure is identified and described.

Note 3: In terms of the assessment of parameters (inputs and outputs) to a module, any use of global data must also be considered. A module "uses" global data if it either reads or writes the data.

Note 4: Values returned through the interface refer to values that are either passed through parameters or messages; values that the function call itself returns in the style of a "C" program function call; or values passed through global means.

D_SC.1 Source code

The developer shall provide the source code to the evaluation facility and the certification body in the form used by development personnel.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The developer makes available the source code in the form they use, so that the evaluation facility may use automated techniques in the analysis. This also increases the confidence that the source code examined

is actually the one used in the production of the component (as opposed to the case where it is supplied in an alternate presentation format, such as a word processor document).

Note 2: Some forms of the source code may require additional information because they introduce significant barriers to understanding and analysis. Examples include shrouded source code or source code that has been obfuscated in other ways such that it prevents understanding and/or analysis. While the shrouded representation is what is compiled and may be closer to the implementation (in terms of structure) than the original, un-shrouded representation, supplying such obfuscated code may cause significantly more time to be spent in analysis tasks involving the representation. When such forms of representation are created, the components require details on the shrouding tools/algorithms used so that the un-shrouded representation can be supplied, and the additional information can be used to gain confidence that the shrouding process does not compromise any security mechanisms.

6.2 G: Guidance Documentation

G_AP.1 Acceptance procedures

The developer shall provide a guidance documentation describing the acceptance procedures, i.e. the steps necessary for secure acceptance of the component by the end user.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The acceptance procedures should reflect the steps the user has to perform in order to accept the delivered component.

Note 2: The acceptance procedures should include as a minimum, that the user has to check that all parts of the component as indicated in the IDS certificate have been delivered in the correct version.

Note 3: The acceptance procedures should provide detailed information about how the user can:

a) ensure that the delivered component is the complete evaluated instance;

b) detect modification/masquerading of the delivered component.

G_AP.2 Installation procedures

The developer shall provide a guidance documentation describing the installation procedures, i.e. the steps necessary for secure installation of the component and the secure preparation of the operational environment.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: If it is not anticipated that installation procedures will or can be applied (e.g. because the component may already be delivered in an operational state), this should be described instead.

Note 2: The installation procedures should provide detailed information about the following, if applicable:

a) minimum system requirements for secure installation;

b) requirements for the operational environment;

c) the steps the user has to perform in order to get to an operational component being commensurate with its evaluated configuration. Such a description shall include - for each step - a clear scheme for the decision on the next step depended on success, failure or problems at the current step;

d) changing the installation specific security characteristics, for example parameters, settings or passwords;

e) handling exceptions and problems.

G_OG.1 Interface usage for each user role

The developer shall provide an operational user guidance describing for each user role, the secure use of the available interfaces provided by the component.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The operational user guidance should provide advice regarding effective use of the security functionality (e.g. reviewing password composition practises, suggested frequency of backups, discussion on the effects of changing user access privileges).

G_OG.2 Possible modes of operation

The operational user guidance shall identify all possible modes of operation of the component (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

6.3 S: Secure Development

S_CM.1 Unique component reference

The component shall be labelled with a unique reference.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: This could be achieved through labelled packaging or media, or by a label displayed by the operational component. This is to ensure that it would be possible for consumers to identify the component (e.g. at the point of purchase or use).

Note 2: The component may provide a method by which it can be easily identified. For example, a software component may display its name and version number during the start up routine, or in response to a command line entry.

S_CM.2 Consistent usage of component reference

The component reference shall be used consistently.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

If the component is labelled more than once then the labels have to be consistent. For example, it should be possible to relate any labelled guidance documentation supplied as part of the component to the evaluated operational component. This ensures that consumers can be confident that they have purchased the evaluated version, that they have installed this version, and that they have the correct version of the guidance to operate the component.

S_CM.3 Configuration management access control measures

The configuration management access control measures shall be automated and effective in preventing unauthorised access to the configuration items.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

S_CM.4 Automated procedures for production

The configuration management documentation shall describe the automated procedures for supporting the production of the component.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The term “production” applies to those processes adopted by the developer to progress the component from the source code to a state acceptable for delivery to the end customer.

Note 2: The following is an example for automated means supporting the production of the component: a “make” tool (as provided with many software development tools).

S_CM.5 Component reflecting source code

The production support procedures shall be effective in ensuring that a component is generated that reflects its source code.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The production support procedures shall describe which tools have to be used to produce the final component from the source code in a clearly defined way.

Note 2: The production support procedures shall ensure that the correct configuration items would be used to generate the component. For example, in a software component this may include checking that the automated production procedures ensure that all source files and related libraries are included in the compiled object code. Moreover, the procedures should ensure that compiler options and comparable other options are defined uniquely.

S_CM.6 (1) Configuration list content (1)

The configuration list shall include the following set of items:

a) the component itself;

b) the evaluation evidence required for the evaluation.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

S_CM.6 (2) Configuration list content (2)

The configuration list shall include the following set of items:

a) the source code;

b) the documentation used to record details of reported security flaws associated with the implementation (e.g., problem status reports derived from a developer's problem database).

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

S_CM.7 Unique identification based on configuration list

The configuration list shall uniquely identify each configuration item.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The configuration list shall contain sufficient information to uniquely identify which version of each item has been used, typically a version number.

S_CM.8 Developer Information

The configuration list shall indicate the developer of each security functionality relevant configuration item.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

If only one developer (= company, not development personnel) is involved in the

development of the the component, this requirement is not applicable.

S_DL.1 Secure delivery

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the component or parts of it to the consumer.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The delivery documentation describes proper procedures to maintain security during transfer of the component or its parts and to determine the identification by the user.

Note 2: The delivery documentation shall cover the entire component, but may contain different procedures for different parts of the component.

Note 3: The delivery procedures should be applicable across all phases of delivery from the production environment to the installation environment (e.g. packaging, storage and distribution). Standard commercial practise for packaging and delivery may be acceptable.

Note 4: Cryptographic checksums or a software signature may be used to ensure that tampering or masquerading can be detected. Tamper proof seals additionally indicate if the confidentiality has been broken. Confidentiality might be assured by using encryption. If availability is of concern, a secure transportation might be required.

Note 5: The emphasis in the delivery documentation is likely to be on measures related to integrity, as integrity of the component is always important. However, confidentiality and availability of the delivery will be of concern in some cases; procedures relating to these aspects of the secure delivery should also be discussed in the procedures where applicable.

S_DS.1 Operational security measures

The development security policies shall detail all security measures employed in the development environment that are necessary to protect the confidentiality and integrity of the component design and implementation.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The following types of security measures should be considered in the documentation:

a) physical, for example physical access controls used to prevent unauthorised access to the development environment (during normal working hours and at other times);

b) procedural, for example covering:

- granting of access to the development environment or to specific parts of the environment such as development machines

- revocation of access rights when a person leaves the development team

- transfer of protected material within and out of the development environment and between different development sites in accordance with defined acceptance procedures

- admitting and escorting visitors to the development environment

- roles and responsibilities in ensuring the continued application of security measures, and the detection of security breaches.

c) personnel, for example any controls or checks made to establish the trustworthiness of new development staff;

d) other security measures, for example the logical protections on any development machines.

Note 2: The development security documentation should identify the locations at

which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development could occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the component or the unfinished component between different development sites are to be covered here, whereas the transport of the finished component to the consumer is dealt with in Delivery (S_DL.1).

Note 3: The following shall be included in the policies:

a) what information relating to the development needs to be kept confidential, and which members of the development staff are allowed to access such material;

b) what material must be protected from unauthorised modification in order to preserve the integrity of the component, and which members of the development staff are allowed to modify such material.

Note 4: The developer should ensure that these policies are described in the development security documentation, that the security measures employed are consistent with the policies, and that they are complete.

S_FR.1 Tracking of reported security flaws

The flaw remediation procedures shall describe the procedures used to track all reported security flaws in each release of the component.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The procedures describe the actions that are taken by the developer from the time each suspected security flaw is reported to the time that it is resolved. This includes the flaw's entire time frame, from initial detection through ascertaining that the flaw is a security flaw, to resolution of the security flaw.

Note 2: If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the Flaw remediation requirements) for the flaw remediation procedures to track it further; only that there be an explanation of why the flaw is not security-relevant.

S_FR.2 Security flaw description

The application of the flaw remediation procedures shall produce a description of each security flaw in terms of its nature and effects.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The procedures identify the actions that are taken by the developer to describe the nature and effects of each security flaw in sufficient detail to be able to reproduce it. The description of the nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design, a flaw in the implementation, etc. The description of the security flaw's effects identifies the portions of the component that are affected and how those portions are affected.

S_FR.3 Status of corrective measures

The application of flaw remediation procedures shall identify the status of finding a correction to each security flaw.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The flaw remediation procedures identify the different stages of security flaws. This differentiation includes at least: suspected security flaws that have been reported, suspected security flaws that have been confirmed to be security flaws, and security flaws whose solutions have been

implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet investigated, flaws that are under investigation, security flaws for which a solution has been found but not yet implemented) be included.

S_FR.4 Safeguards

The application of the flaw remediation procedures shall result in safeguards that the potential correction contains no adverse effects.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: Through analysis, testing, or a combination of the two, the developer may reduce the likelihood that adverse effects will be introduced when a security flaw is corrected.

Note 2: For instances where the source of the security flaw is a documentation problem, the procedures shall include the means of safeguarding against the introduction of contradictions with other documentation.

S_FR.5 Contact for user reports and enquires

The operational guidance shall identify specific points of contact for user reports and enquiries about security issues involving the component.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

S_LC.1 Life-cycle model

The description of the life-cycle model covers the development and maintenance process.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The description of the life-cycle model shall include:

a) information on the life-cycle phases of the component and the boundaries between the subsequent phases;

b) information on the procedures, tools and techniques used by the developer (e.g. for design, coding, testing, bug-fixing);

c) overall management structure governing the application of the procedures (e.g. an identification and description of the individual responsibilities for each of the procedures required by the development and maintenance process covered by the life-cycle model);

d) information on which parts of the component are delivered by subcontractors, if subcontractors are involved.

Note 2: This does not require the model used to conform to any standard life-cycle model.

6.4 T: Developer Testing

T_CA.1 Test coverage analysis

The test coverage analysis shall show a complete correspondence between the components interfaces and the tests in the test documentation.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

All interfaces that are described in the development documentation have to be present in the test coverage analysis and mapped to tests in order for completeness to be claimed. Incomplete coverage would be evident if an interface was identified in the development documentation and no test was mapped to it.

This does not imply that all tests in the test documentation must map to interfaces in the interface specification.

T_CA.2 Test procedures for subsystems

The test procedures shall contain descriptions of the security-related subsystem behaviour and interaction that are tested.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: All descriptions of security-related subsystem behaviour and of interactions among security-related subsystems that are provided in the component design have to be tested. Incomplete depth of testing would be evident if a description of security-related subsystem behaviour or of interactions among TSF subsystems was identified in the design and no tests could be attributed to it. This does not imply that all tests in the test documentation must map to the subsystem behaviour or interaction description in the design.

Note 2: When D_DD.2 is included, the level of detail needed to map the test cases to the behaviour of the subsystems may require information from the module description to be used. This is because D_DD.2 allows the description of details to be shifted from the subsystem level to the module level.

T_CA.3 Test procedures for interfaces

The developer testing shall contain test procedures for all interfaces of security-related modules.

- Basic Broker Profile: -
- Advanced Information Broker Profile: -
- Usage Control Broker Profile: x

Application Note(s):

All interfaces of security-related modules that are provided in the design have to be tested. Incomplete depth of testing would be evident if any interface of any security-related modules was identified in the design and no tests could be attributed to it.

This does not imply that all tests in the test documentation must map to an interface of an security-related module in the design.

T_TD.1 Test documentation

The test documentation shall include scenarios for performing each test, expected test results and actual test results.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

The test plan shall provide information about how to execute the test: any necessary automated set-up procedures (and whether they require privilege to run), inputs to be applied, how these inputs are applied, how output is obtained, any automated clean-up procedures (and whether they require privilege to run), etc. This information should be detailed enough to ensure that the test is reproducible.

T_TD.2 Test configuration

The test configuration shall be consistent with the configuration list (S_CM.6).

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Note 1: The test plan shall provide information about the test configuration being used: both on the configuration of the component and on any test equipment being used. This information should be detailed enough to ensure that the test configuration is reproducible.

Note 2: The component referred to in the developer's test plan should have the same unique reference as established by the configuration management (S_CM).

T_TD.3 Ordering Dependencies

The test documentation shall provide sufficient instructions for any ordering dependencies of the tests.

- Basic Broker Profile: x
- Advanced Information Broker Profile: x
- Usage Control Broker Profile: x

Application Note(s):

Some steps may have to be performed to establish initial conditions. For example, user accounts need to be added before they can be deleted. An example of ordering dependencies on the results of other tests is the need to perform actions in a test that will result in the generation of audit records, before performing a test to consider the searching and sorting of those audit records. Another example of an ordering dependency would be where one test case generates a file of data to be used as input for another test case.

For further details, see the spreadsheet Certification Criteria - Components v2.1.0 in Jive[3].

3 https://industrialdataspace.jiveon.com/docs/DOC-2811

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: certiication@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: industrialdataspace.jiveon.com/docs/DOC-1799
Certification Criteria – Components: 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: industrialdataspace.jiveon.com/docs/DOC-1710

Whitepaper 2018: bit.ly/2lIRo5z
Webinar on YouTube: bit.ly/2kBGAG5

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)

OUR MEMBERS


Aalto University
ADVANEO
agrarmarkt informatik
Allianz
Atos
Audi
bill-X Collect. Manage. Execute.
Boehringer Ingelheim
Brainport Industries
bdr BUNDESDRUCKEREI
CAICT
SUPERCLUSTER
CDQ SHARING DATA EXCELLENCE
cea
Cefriel POLITECNICO DI MILANO
iti Information Technologies Institute
CHALMERS UNIVERSITY OF TECHNOLOGY
COSMOPlat
Cybus
CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
DAIMLER
DATAHEAD
DATATRONIQ
DB SCHENKER
Deloitte.
Deutsche Bank
DGZfP
DHBW Duale Hochschule Baden-Württemberg Ravensburg
Digital Green
DIMECC
DR. SCHNEIDER UNTERNEHMENSGRUPPE
eccenca command your data!
EcoDataCenter
ELDORADO
ENGIE
ENGINEERING
8760 Fastems
fir an der RWTH Aachen
FIWARE
Leibniz Universität Hannover
Fraunhofer
GateHouse Logistics
EDGE CLOUD
GESIS
Google
HITACHI Inspire the Next
HUAWEI
i2cat
iav
IBM
ILVO Instituut voor Landbouw-, Visserij- en Voedingsonderzoek
imec
Imperial College London
Institut Mines-Télécom
INDUSTRY 2025 INDUSTRIE INDUSTRIA
INNOPAY
innovalia ASSOCIATION
Insight
Irish Manufacturing Research
ITI INVESTIGATE TO INNOVATE
Klarrio
komsa DIE BESSERE VERBINDUNG
LOSEC LEADERS IN SECURITY
Lobster
Logata Digital Solutions
LOGENIOS
minnosphere
msg
nexedi
nicos AG
olmogo data ownership solutions


orbiter

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ

pi-lar GmbH

POLITECNICO
MILANO 1863

pwc

QuinScape

realworldsystems

RI
SE

REWE
GROUP

RITTAL

SALZGITTERAG
Stahl und Technologie

SAP

SCHAEFFLER

SETLOG
The Smart Connective

SICK
Sensor Intelligence.

SIEMENS
Ingenuity for life

Signal
Solutions

SINTEF

SMEV AG
Smart Mobility Evolution

TARC

tecnalia
Inspiring Business

IK4 TEKNIKER


mtc
Manufacturing Technology Centre

thyssenkrupp

TNO innovation for life

TÜV NORD GROUP

TÜV
SÜD

UNIKLINIK
RWTH AACHEN

UNiSCON
Sealed Cloud Technologies

UNITY
CONSULTING & INNOVATION

universität
Witten/Herdecke

University of Amsterdam

UNIVERSITY
OF TWENTE.

vastuu group

VDMA

VOLKSWAGEN
AKTIENGESELLSCHAFT

VTT

WELOTEC
a byte smarter

WeTech
IDS-China

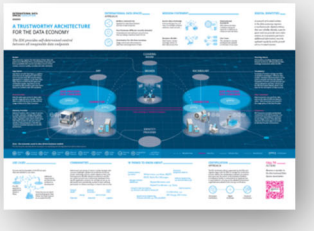
ZVEI:
Die Elektroindustrie

OVERVIEW PUBLICATIONS

Reference Architecture Model

Executive Summary

Image Brochure



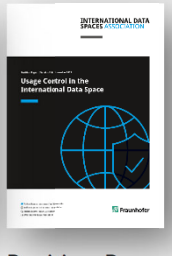
Infographic

Use Case Brochures

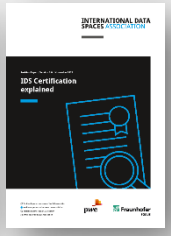
Study on Data Exchange

Position Paper Implementing the European Data Strategy

Position Paper GDPR Requirements and Recommendations



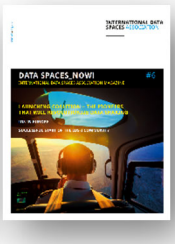
Position Paper Usage Control in the IDS



Position Paper IDS Certification Explained

White Paper Certification

Sharing data while keeping data ownership



Magazine Data Spaces_Now!

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

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

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

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

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association