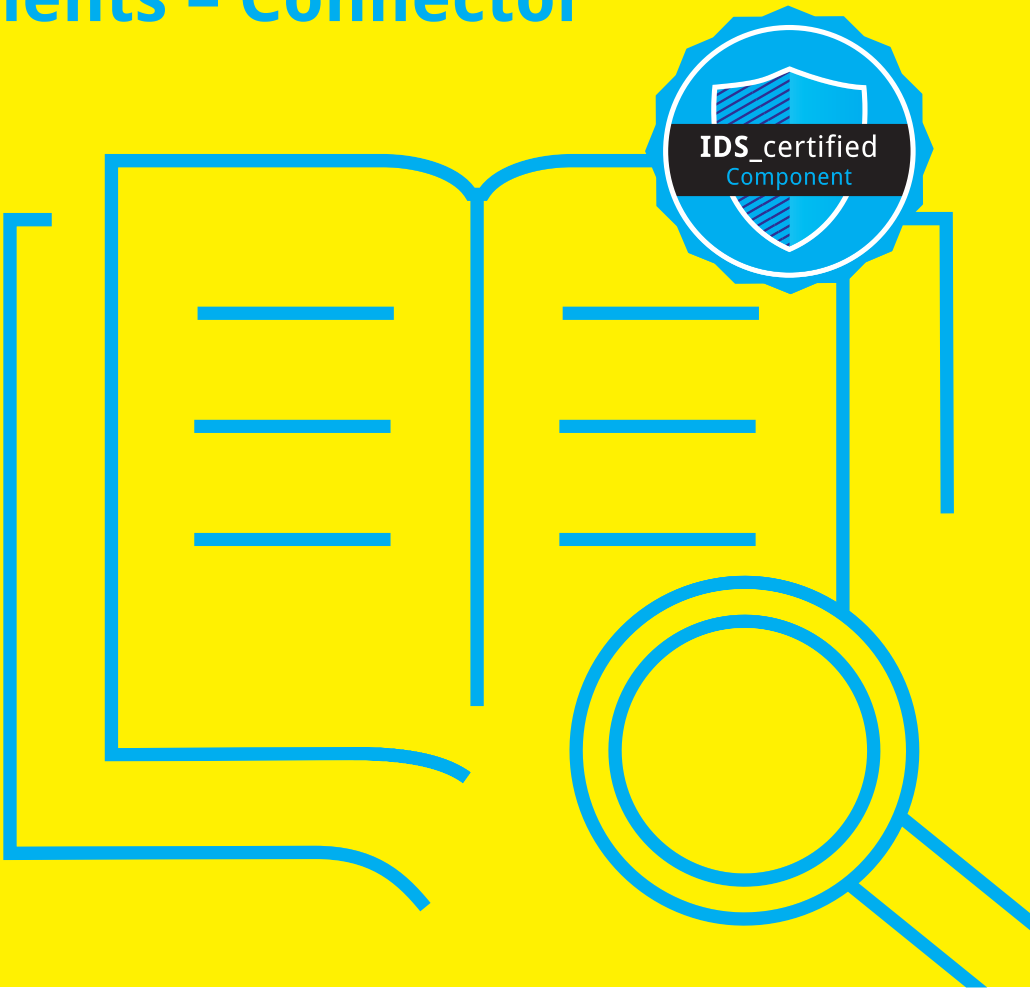
INTERNATIONAL DATA
SPACES ASSOCIATION

White Paper | Version 1.0 | March 2020

Criteria Catalogue:
Components – Connector



○ Position Paper of members of the IDS Association

○ Position Paper of bodies of the IDS Association

○ Position Paper of the IDS Association

● White Paper of the IDS Association

Publisher

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

Editor

Sebastian Steinbuss,
International Data Spaces Association

Authors & Contributors

- Nadja Menz, Fraunhofer FOKUS
- Aleksei Resetko, PrivewaterhouseCooper
- Monika Huber, Fraunhofer AISEC
- Sascha Wessel, Fraunhofer AISEC

Cite as

Steinbuss S. et al. (2020): Criteria Catalogue. Components - Connector. International Data Spaces Association. https://doi.org/10.5281/zenodo.5675774

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«) 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 Connector component.

1 Introduction

The Connector shall provide a sufficiently high degree of trust and security regarding the integrity, confidentiality and availability of information exchanged in the IDS. Nevertheless, the IDS Certification has a flexible setup and provides different levels of certification according to the intended use cases.

One of the International Data Space goals is to evolve towards a global de-facto standard for cross-industrial and cross-company information exchange. Therefore, a low financial and procedural barrier to join the International Data Space is inevitable. To ensure on the one hand a low entry barrier specifically suitable for SME's and on the other hand a scalable certification to meet high information security requirements, three different security levels, with an increasing extent of the security requirements that need to be fulfilled, were defined:

- The Base Security Profile offers basic security features to protect against attackers from outside, to ensure integrity and availability. It is therefore designed for use in scenarios with only low security requirements. A Connector meeting this profile is suitable for exchanging data with limited trust and security needs, for exchange of data in a contained environments or for demonstration purposes.
- The Trust Security Profile includes strict container isolation, integrity-protected logging, encryption of all persisted data, protection against accidental misuse by administrators. This profile is used for scenarios in which the protection of the processed and transmitted data is essential.
- In comparison to the Trust profile, the Trust+ Security Profile also offers additional protection against misuse of privileged access, i.e. manipulation by administrators. This includes the protection against insider attacks as well as against external attackers who could gain privileged access. This is achieved by actively monitoring users and data on behalf of the data owner.

2 Criteria to Certification Level Mapping

ID	Criteria Title	Base	Trust	Trust+
IDS Specification (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	X
COM 05	Platform integrity	-	X	X
COM 06	Configuration and app integrity	-	-	X
Data Usage Control				
USC 01	Definition of usage policies	X	X	X
USC 02	Sending of usage policies	-	X	X
USC 03	Usage policy enforcement	-	X	X
USC 04	Usage policy changes	-	X	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)	X	X	X
INF 03	Self-Description content	X	X	X
INF 04	Self-Description evaluation	X	X	X
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
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	X	X	X
BRK 02	Broker registration	X	X	X
BRK 03	Broker registration update	X	X	X
Operating System				
OS 01	Container support	X	X	X
OS 02	App separation	-	X	X
OS 03	Service authenticity and integrity	-	X	X
OS 04	System component authenticity and integrity	-	X	X
OS 05	Container separation	-	X	X
OS 06	Backup encryption	-	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	X
APS 04	Requirements for the runtime environment	-	X	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	X

ID	Criteria Title	Base	Trust	Trust+
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	-	-	-
CR 1.2	Software process and device identification and authentication	-	X	X
CR 1.2 (1)	Unique identification and authentication	X	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	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	X
CR 1.7 (2)	Password lifetime restrictions for all users (human, software process or device)	-	X	X
CR 1.8	Public key infrastructure certificates	X	X	X
CR 1.9	Strength of public key-based authentication	-	X	X
CR 1.9 (1)	Hardware security for public key-based authentication	-	X	X
CR 1.10	Authenticator feedback	X	X	X
CR 1.11	Unsuccessful login attempts	X	X	X
CR 1.12	System use notification	X	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	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	X
CR 2.1 (2)	Permission mapping to roles	-	X	X
CR 2.1 (3)	Supervisor override	-	X	X
CR 2.1 (4)	Dual approval	-	-	-
CR 2.2	Wireless use control	(X)	(X)	(X)
CR 2.3	Use control for portable and mobile devices	X	X	X
CR 2.5	Session lock	X	X	X
CR 2.6	Remote session termination	-	X	X
CR 2.7	Concurrent session control	-	X	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	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	X
CR 2.11 (2)	Protection of time source integrity	-	X	X
CR 2.12	Non-repudiation	-	X	X
CR 2.12 (1)	Non-repudiation for all users	-	X	X
SI: System integrity				
CR 3.9	Protection of audit information	-	X	X
CR 3.9 (1)	Audit records on write-once media	-	-	-
DC: Data confidentiality				

ID	Criteria Title	Base	Trust	Trust+
CR 4.1	Information confidentiality	X	X	X
CR 4.2	Information persistence	-	X	X
CR 4.2 (1)	Erase of shared memory resources	X	X	X
CR 4.2 (2)	Erase verification	-	X	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	X
CR 6.2	Continuous monitoring	-	X	X
RA: Resource availability				
CR 7.1	Denial of service protection	X	X	X
CR 7.1 (1)	Manage communication load from component	-	X	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	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	X
CR 7.7	Least functionality	X	X	X
CR 7.8	Control system component inventory	-	X	X
NDR: Network device requirements				
NDR 1.6	Wireless Access Management	X	X	X
NDR 1.6 (1)	Unique identification and authentication	-	X	X
NDR 1.13	Access via untrusted networks	X	X	X
NDR 1.13 (1)	Explicit access request approval	-	X	X
NDR 2.4	Mobile code	X	X	X
NDR 2.13	Use of physical diagnostic and test interfaces	-	X	X
NDR 2.13 (1)	Active monitoring	-	X	X
NDR 3.2	Protection from malicious code	X	X	X
NDR 3.10	Support for updates	X	X	X
NDR 3.10 (1)	Update authenticity and integrity	-	X	X
NDR 3.11	Physical tamper resistance and detection	-	X	X
NDR 3.11 (1)	Notification of a tampering attempt	-	X	X
NDR 3.12	Provisioning product supplier roots of trust	-	X	X
NDR 3.13	Provisioning asset owner roots of trust	-	X	X
NDR 3.14	Integrity of the boot process	X	X	X
NDR 3.14 (1)	Authenticity of the boot process	-	X	X
NDR 5.2	Zone boundary protection	X	X	X
NDR 5.2 (1)	Deny all, permit by exception	-	X	X
NDR 5.2 (2)	Island mode	-	X	X
NDR 5.2 (3)	Fail close	-	X	X
NDR 5.3	General purpose, person-to-person communication restrictions	X	X	X
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

ID	Criteria Title	Base	Trust	Trust+
D_IS.3	Error messages	-	X	X
D_DD.1	Subsystem structure	X	X	X
D_DD.2	Module structure	-	X	X
D_DD.3	Subsystem-Module mapping	-	X	X
D_DD.4	Parameters, invocation conventions and return values	-	X	X
D_SC.1	Source code	-	X	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	X
S_CM.4	Automated procedures for production	-	X	X
S_CM.5	Component reflecting source code	-	X	X
S_CM.6	Configuration list content	X (a-b)	X (a-d)	X (a-d)
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	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	X
S_FR.5	Contact for user reports and enquires	-	X	X
S_LC.1	Life-cycle model	-	X	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	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

3.1 Communication Integrity

COM 01 - Protected connection

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

COM 02 - Mutual authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

COM 03 - State of the art cryptography

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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 catalogue.

COM 04 - Remote attestation

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

COM 05 - Platform integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

Application Note: 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

- Base Security Profile: -
- Trust Security Profile: -
- Trust+ Security Profile: x

Proof of integrity additionally refers to Connector's

a) configuration and

b) apps installed.

3.2 Data Usage Control

USC 01 - Definition of usage policies

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector allows data providers to define usage policies that will be published together with the data offered.

USC 02 - Sending of usage policies

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector offering data sends usage policy to be applied to Connector requesting data every time connection is established.

USC 03 - Usage policy enforcement

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector facilitates technical enforcement of data usage policy specified.

USC 04 - Usage policy changes

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: 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

- Base Security Profile: -
- Trust Security Profile: -
- Trust+ Security Profile: x

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

3.3 Information Model

INF 01 - Self-Description (at Connector)

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

INF 02 - Self-Description (at Broker)

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

To register with a Broker, a Connector must be able to provide the Broker with this self-description.

INF 03 - Self-Description content

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

INF 04 - Self-Description evaluation

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector offering data evaluates self-description of Connector requesting data.

INF 05 - Dynamic attribute tokens

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

3.4 Identity and Access Management

IAM 01 - Connector identifier

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

IAM 02 - Time Service

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

IAM 03 - Online certificate status check

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

IAM 04 - Attestation of dynamic attributes

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

3.5 Broker Service

BRK 01 - Broker service inquiries

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector supports broker service inquiries by means of browsing self-descriptions of Connectors registered there.

BRK 02 - Broker registration

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector supports registration with a broker by transmitting self-description.

BRK 03 - Broker registration update

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector supports updates of self-description stored at broker (e.g. when new service is offered) and marking itself as available / unavailable.

3.6 Operating System

OS 01 - Container support

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector supports installation and execution of containers.

OS 02 - App separation

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

OS 03 - Service authenticity and integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

OS 04 - System component authenticity and integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

OS 05 - Container separation

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

OS 06 - Backup encryption

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

3.7 Apps and App Store Connection

APS 01 - App signature

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

APS 02 - App signature verification

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

APS 03 - Terms of use

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

APS 04 - Requirements for the runtime environment

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: 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

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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).

APS 06 - App Store

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Connector receives apps from a central app store.

3.8 Data Usage Transparency

AUD 01 - Access control logging

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

AUD 02 - Data access logging

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

AUD 03 - Configuration changes logging

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

AUD 04 - Resource availability logging

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

4 IEC 62443-4-2

4.1 IAC: Identification and authentication control

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

CR 1.1 – Human user identification and authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.1 (1) - Unique identification and authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 1.1 (2) - Multifactor authentication for all interfaces

- Base Security Profile: -
- Trust Security Profile: -
- Trust+ Security Profile: -

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

CR 1.2 – Software process and device identification and authentication

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.2 (1) - Unique identification and authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 1.3 – Account management

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.4 – Identifier management

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

CR 1.5 – Authenticator management

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.5 (1) - Hardware security for authenticators

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

Application Note: The requirements for wireless access management for the device type Network Device can be found in 62443-NDR.

CR 1.7 – Strength of password-based authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: 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 cannot 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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

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

CR 1.7 (2) - Password lifetime restrictions for all users (human, software process or device)

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

The component shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.

Application Note: Non-human users that authenticate via username and password are not foreseen. Within the scope of IDS-evaluations, fulfilling CR 1.7(1) is therefore sufficient.

CR 1.8 – Public key infrastructure certificates

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.9 – Strength of public key-based authentication

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 1.10 – Authenticator feedback

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 1.11 – Unsuccessful login attempts

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 1.12 – System use notification

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

Application Note: The requirements for access via untrusted networks for the device type Network device can be found in 62443-NDR.

CR 1.14 – Strength of symmetric key-based authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

4.2 UC: Use Control

Application Note: 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 – Authorization enforcement

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

The component shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.

Application Note: For the Base Connector, this requirement cannot be technically enforced as it is expected to only support user accounts with admin privileges.

CR 2.1 (2) - Permission mapping to roles

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NOTE 1 This RE is applicable to software processes and devices as well.

CR 2.1 (3) - Supervisor override

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

The component shall support a supervisor manual override for a configurable time or sequence of events.
NOTE 2 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 2.1 (4) - Dual approval

- Base Security Profile: -
- Trust Security Profile: -
- Trust+ Security Profile: -

The component shall support dual approval when action can result in serious impact on the industrial process. Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.

CR 2.2 – Wireless use control

- Base Security Profile: (x)
- Trust Security Profile: (x)
- Trust+ Security Profile: (x)

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.

CR 2.3 – Use control for portable and mobile devices

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

There is no component level requirement associated with IEC 62443-3-3 SR 2.3.

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

Application Note: The use control requirements for mobile code for the device type Network device can be found in 62443-NDR.

CR 2.5 – Session lock

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.6 – Remote session termination

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 2.7 – Concurrent session control

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.8 – Auditable events

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

z) access control; aa) request errors; bb) control system events; cc) backup and restore event; dd) configuration changes; and ee) audit log events.

Individual audit records shall include:

ff) timestamp;

gg) source (originating device, software process or human user account); hh) category; ii) type; jj) event ID; and kk) event result.

CR 2.9 – Audit storage capacity

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.10 – Response to audit processing failures

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

CR 2.11 – Timestamps

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.11 (1) - Time synchronization

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.12 (2) - Protection of time source integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 2.12 – Non-repudiation

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 2.12 (1) - Non-repudiation for all users

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

4.3 SI: System integrity

CR 3.1 – Communication integrity

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 3.1 (1) - Communication authentication

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

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

Application Note: The protection from malicious code requirements for the device type Software Application can be found in 62443-NDR.

CR 3.3 – Security functionality verification

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

Components shall provide the capability to support verification of the intended operation of

security functions according to IEC 62443-3-3 SR3.3.

CR 3.3 (1) - Security functionality verification during normal operation

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

The component shall provide the capability to support verification of the intended operation of security functions during normal operations.

CR 3.4 – Software and information integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.4 (1) - Authenticity of software and information

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.4 (2) - Automated notification of integrity violations

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.5 – Input validation

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.6 – Deterministic output

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: 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

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.8 – Session integrity

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 3.9 – Protection of audit information

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 3.9 (1) - Audit records on write-once media

- Base Security Profile: -
- Trust Security Profile: -
- Trust+ Security Profile: -

Components shall provide the capability to store audit records on hardware-enforced write-once media.

Application Note: The requirements for support for updates for the device type Network device can be found in 62443-NDR.

Application Note: The requirements for physical tamper resistance and detection for the device type Network device can be found in 62443-NDR.

Application Note: The requirements for provisioning product supplier roots of trust for the device type Network device can be found in 62443-NDR.

Application Note: The requirements for provisioning asset owner roots of trust for the device type Network device can be found in 62443-NDR.

Application Note: The requirements for integrity of the boot process for the device type Network device can be found in 62443-NDR.

4.4 DC: Data confidentiality

CR 4.1 – Information confidentiality

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

CR 4.2 – Information persistence

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 4.2 (1) - Erase of shared memory resources

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NOTE: 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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 4.3 – Use of cryptography

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

4.5 RDF: Restricted data flow

CR 5.1 – Network segmentation

- Base Security Profile: x

- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: The requirements for zone boundary protection for the device type Network device can be found in 62443-NDR.

Application Note: The requirements for general person-to-person communication restrictions for the device type Network device can be found in 62443-NDR.

4.6 TRE: Timely response to events

CR 6.1 – Audit log accessibility

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 6.1 (1) - Programmatic access to audit logs

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 6.2 – Continuous monitoring

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

4.7 RA: Resource availability

CR 7.1 – Denial of service protection

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.1 (1) - Manage communication load from component

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.2 – Resource management

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.3 – Control system backup

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

CR 7.3 (1) - Backup integrity verification

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.4 – Control system recovery and reconstitution

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.6 – Network and security configuration settings

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

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

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.7 – Least functionality

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

CR 7.8 – Control system component inventory

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

4.8 NDR: Network device requirements

NDR 1.6 - Wireless Access Management

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 1.6 (1) - Unique identification and authentication

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 1.13 - Access via untrusted networks

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 1.13 (1) - Explicit access request approval

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 2.4 – Mobile code

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 2.13 - Use of physical diagnostic and test interfaces

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 2.13 (1) - Active monitoring

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

Application Note: If all debug interfaces are deactivated, monitoring is not needed

NDR 3.10 - Support for updates

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 3.10 (1) - Update authenticity and integrity

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 3.11 - Physical tamper resistance and detection

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

NDR 3.11 (1) - Notification of a tampering attempt

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 3.12 – Provisioning product supplier roots of trust

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 3.13 – Provisioning asset owner roots of trust

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 3.14 – Integrity of the boot process

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 3.14 (1) - Authenticity of the boot process

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

NDR 5.2 - Zone boundary protection

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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 risk-based zones and conduits model.

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

NDR 5.2 (1) - Deny all, permit by exception

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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).

NDR 5.2 (2) - Island mode

- Base Security Profile: -
- Trust Security Profile: x

- Trust+ Security Profile: x

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

NDR 5.2 (3) - Fail close

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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).

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

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

5 Development

5.1 D: Development Documentation

D_AD.1 - Secure initialisation

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

D_AD.2 - Tamper protection

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_AD.3 - Security-enforcing mechanisms

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

D_IS.1 - Interface purpose and usage

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_IS.2 - Interface parameters

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_IS.3 - Error messages

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

D_DD.1 - Subsystem structure

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_DD.2 - Module structure

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_DD.3 - Subsystem-Module mapping

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

D_DD.4 - Parameters, invocation conventions and return values

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

D_SC.1 - Source code

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

5.2 G: Guidance Documentation

G_AP.1 - Acceptance procedures

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

G_AP.2 - Installation procedures

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

G_OG.1 - Interface usage for each user role

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

G_OG.2 - Possible modes of operation

- Base Security Profile: x
- Trust Security Profile: x

- Trust+ Security Profile: x

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.

5.3 S: Secure Development

S_CM.1 - Unique component reference

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

The component shall be labelled with a unique reference.

S_CM.2 - Consistent usage of component reference

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

The component reference shall be used consistently.

S_CM.3 - Configuration management access control measures

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_CM.4 - Automated procedures for production

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_CM.5 - Component reflecting source code

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_CM.6 - Configuration list content

- Base Security Profile: x (a-b)
- Trust Security Profile: x (a-d)
- Trust+ Security Profile: x (a-d)

The configuration list shall include the following set of items:

a) the component itself;

b) the evaluation evidence required for the evaluation;

c) the source code;

d) 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).

S_CM.7 - Unique identification based on configuration list

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

The configuration list shall uniquely identify each configuration item.

S_CM.8 - Developer Information

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_DL.1 - Secure delivery

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

S_DS.1 - Operational security measures

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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.

S_FR.1 - Tracking of reported security flaws

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_FR.2 - Security flaw description

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_FR.3 - Status of corrective measures

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_FR.4 - Safeguards

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_FR.5 - Contact for user reports and enquires

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

S_LC.1 - Life-cycle model

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

5.4 T: Developer Testing

T_CA.1 - Test coverage analysis

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

T_CA.2 - Test procedures for subsystems

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

T_CA.3 - Test procedures for interfaces

- Base Security Profile: -
- Trust Security Profile: x
- Trust+ Security Profile: x

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

T_TD.1 - Test documentation

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

T_TD.2 - Test configuration

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

T_TD.3 - Ordering Dependencies

- Base Security Profile: x
- Trust Security Profile: x
- Trust+ Security Profile: x

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

6 Summary

For further details, see the spreadsheet Certification Criteria - Components v2.0.0 in Jive[1].

[1] https://industrialdataspace.jiveon.com/docs/DOC-2223

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

INTERNATIONAL DATA SPACES ASSOCIATION
IDSA WEBINAR
TRUST IN THE IDS BASED ON THE CERTIFICATION OF PARTICIPANTS AND CORE COMPONENTS

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

- A! Aalto University
- ADVANEO
- agmadata DIGITALE PROZESSE FÜR GUTE LEBENSMITTEL
- Allianz
- AtoS
- Audi
- bill-X Collect. Manage. Execute.
- Boehringer Ingelheim
- Brainport Industries
- bdr. BUNDESDRUCKEREI
- CAICT 中国信息通信研究院
- CANADA'S DIGITAL TECHNOLOGY SUPERCLUSTER
- CDQ SHARING DATA EXCELLENCE
- cea
- Cefriel POLITECNICO DI MILANO
- iti Information Technologies Institute
- CHALMERS UNIVERSITY OF TECHNOLOGY
- COSMOPlat
- Cybus
- CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
- DAIMLER
- DATAAHEAD
- DATATRONiQ
- DB SCHENKER
- Deloitte.
- Deutsche Bank
- DGZfP
- DHBW Duale Hochschule Baden-Württemberg Ravensburg
- DigitalGreen
- 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
- GERMAN EDGE CLOUD
- GESIS GESELLSCHAFT FÜR INFORMATIONSSYSTEME
- Google
- HITACHI Inspire the Next
- HUAWEI
- i2cat
- automotive engineering 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
- K
- KOMSA DIE BESSERE VERBINDUNG
- LOSEC LEADERS IN SECURITY
- Lobster
- Logata Digital Solutions
- LOGENIOS
- minnosphere
- .msg
- nexedi
- nicos AG Network of International Communication Solutions
- olmogo data ownership solutions

orbiter

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

pi-lar GmbH

POLITECNICO MILANO 1863

pwc

QuinScape

realworldsystems

RISE

REWE GROUP

RITTAL

SALZGITTER AG 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 Tunku Abdul Rahman University College

tecnalia Inspiring Business

IK4 TEKNIKER Research Alliance

T · ·

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

INTERNATIONAL DATA SPACES ASSOCIATION
REFERENCE ARCHITECTURE MODEL

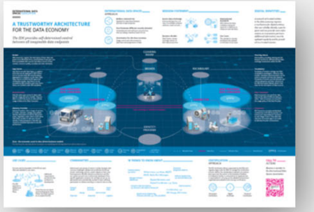
Reference Architecture Model

INTERNATIONAL DATA SPACES ASSOCIATION
SHARING DATA WHILE KEEPING DATA OWNERSHIP

Executive Summary

INTERNATIONAL DATA SPACES ASSOCIATION
INTERNATIONAL DATA SPACES (IDS)

Image Brochure



Infographic

INTERNATIONAL DATA SPACES ASSOCIATION
USE CASE OVERVIEW
INTERNATIONAL DATA SPACES
OUR USE CASES MAKE IT HAPPEN!
USE CASE OVERVIEW
INTERNATIONAL DATA SPACES
OUR USE CASES MAKE IT HAPPEN!
2019

Use Case Brochures

Study on Data Exchange

INTERNATIONAL DATA SPACES ASSOCIATION
Implementing the European Strategy on Data
Role of the International Data Spaces (IDS)

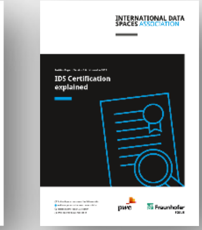
Position Paper Implementing the European Data Strategy

INTERNATIONAL DATA SPACES ASSOCIATION
GDPR Related Requirements and Recommendations for the IDS Reference Architecture Model
GDPR
Fraunhofer

Position Paper GDPR Requirements and Recommendations

INTERNATIONAL DATA SPACES ASSOCIATION
Usage Control in the International Data Space
Fraunhofer

Position Paper Usage Control in the IDS


INTERNATIONAL DATA SPACES ASSOCIATION
IDS Certification explained
pwc
Fraunhofer

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