Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B6, Version 2.0

Date:	30.09.2023
Status:	Mandatory
Subject:	Requirements for a TOE
Document Owner:	Certification body of BSI
Distribution:	BSZ-Licensed Evaluation Facilities (ITSEF)[1] BSI internal Website of the BSI

[1]All evaluators in the evaluation facilities licensed by the BSI for evaluations in accordance with the BSZ.

Document history

Version	*Date*	*Editor*	*Description*
1.0	2021-10-01	SZ 33	1st edition
1.1	2022-06-01	SZ 33	Specific references updated Updated wording of requirements: • "Has to" and "must" replaced by "shall" • Revision, clarification, and specification of requirements Updated numeration
1.2	2023-06-01	SZ 33	Change to the new BSI document template Update of requirements for re-authentication paragraph 12 and factory reset paragraph 23 Update of Background section with requirement regarding conformity checklists Editorial changes
2.0	2023-09-30	SZ 33	Added a new subsection 3.5 for the evaluation of software applications and applications in virtualised environments. Editorial changes

Table 1: history of changes

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: bsz@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Background 4
2 Specific references 5
3 Application notes and interpretation 6
3.1 Authentication and authorization 6
3.2 Logging 6
3.3 Services 7
3.4 Documentation 8
3.5 Additional requirements for software applications and applications in virtualised environments 8
4 Definitions 10
5 Reference documents 13

1 Background

1 This document defines requirements that each Target of Evaluation (TOE) shall fulfil for the BSZ. The requirements are based on international standards, in particular Part 4-2 of the IEC 62443 concerning cybersecurity in industrial communication networks [62443-4-2].

2 Sections of documents stating the conformity to the individual requirements of this AIS document shall be structured in tabular form.

2 Specific references

1 [BSZ-Prod] Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Produkte, BSI

2 [BSZ-Prüf] Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Prüfstellen, BSI

3 [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess, BSZ-EP, BSI

4 [AIS B1] Requirements for ST and IAR, BSI

5 [AIS B2] Requirements for the evaluation of cryptographic mechanisms according to the BSZ, BSI

6 [AIS B3] Requirements for user guidance, BSI

7 [AIS B4] Requirements for evaluation according to the BSZ, BSI

8 [AIS B5] Guideline for determining the efforts for a BSZ evaluation, BSI

9 [BSZ-ETR] BSZ – Vorlage für den Evaluierungsreport, BSI

10 [BSZ-ADA] BSZ - Agenda der Auftaktbesprechung, BSI

3 Application notes and interpretation

3.1 Authentication and authorization

3 The TOE shall identify and authenticate the user on each respective interface, before the user can access the services.
Note 1: Anonymous use may be possible if compromising the TOE is not possible and no critical configuration can be changed.
Note 2: In the Security Target (ST), the users of the TOE are mapped to assets they have access to and their respective kind of access. The TOE shall ensure that users can only access assets after successful authentication.

4 The TOE shall uniquely identify itself and be able to authenticate itself to the user.

5 The TOE shall not contain hard-coded passwords, cryptographic keys or other credentials that are shared by multiple products.

6 The TOE should allow administration of all existing user accounts.
Note: User administration can use local or centralized services, e.g., LDAP.

7 The TOE shall allow users to alter their own local authentication data, e.g. passwords and user names, and protect it from unauthorized access.

8 The TOE shall check for sufficient complexity and security of authentication data during creation or modification. The required configurable strength should be based on recognised security guidelines.

9 The TOE shall not leak or allow for inference about security relevant information as response to authentication.

10 The TOE shall limit authentication attempts to prevent brute force attacks.

11 The TOE should provide a role management for access to files and services. Access rights shall be assigned restrictively, also in default configuration.
Note 1: Role management is only required, if a function is provided in the TOE context.
Note 2: In the default configuration only the role of administrator with full permissions must be available.

12 The TOE shall request re-authentication after a defined time of inactivity or after a fixed time period.

3.2 Logging

13 The TOE shall as a minimum log the following events:

- Incorrect authentication
- Backup and backup restoring
- Configuration changes

14 For the events mentioned above, the TOE shall save the following information:

- Time stamp
- Event type
- Result of the action triggering the event

15 The TOE shall provide sufficient local storage for event logs.
Note: Event logging is not limited to local storage. Information can also be transmitted to other

systems. However, a sufficiently large memory for intermediate storage is absolutely necessary on the TOE to compensate for potential outages in the connection to the centralized instance.

16 The TOE shall preserve a secure state if insufficient storage space is available.

17 The TOE shall provide only authorized users the access to log files.
Note: Only valid for local storage, in the case of external event logging the documentation shall contain a description on how storage is implemented.

3.3 Services

18 The TOE shall respond robustly to incorrect or erroneous data of its services. The TOE shall not reach an undefined state at any time.

19 The TOE shall protect the integrity, authenticity and confidentiality of transmitted data according to the security properties.
Note 1: Deciding which transmitted data is worth protecting depends on the security functions.
Note 2: In cases, where resulting data is not confidential, protection measures may solely focus on integrity.

20 The TOE shall validate input and output before processing to avoid erroneous processing.
Note: The input and output data from the TOE itself or external interfaces shall be checked for syntax, length and content.

21 The TOE shall treat errors adequately.

22 The TOE shall not leak critical information in error messages.
Note: Error messages shall not contain information relevant to potential attackers. Log files shall not contain authentication data.

23 The TOE shall be able to be reset to factory settings. A function that securely and reliably deletes all user-specific data shall be available for this purpose.
Note 1: This function can also be security-critical and should be secured appropriately.
Note 2: Please provide a short technical description of the method used to delete the data.

24 The TOE should perform cryptographic operations in the default configuration in accordance to the requirements of the document [AIS B2].

25 The TOE shall provide means for backup and recovery of the current configuration.

26 In the default configuration, only services that are required to perform basic functions should be activated in the TOE. Users shall be provided with an option to deactivate services which are not required.
Note 1: In the default configuration as few services as possible should be active to minimize the attack surface in accordance with the principle of security by design.
Note 2: Basic functionality is defined by the functions included in the TOE's certification.
Note 3: The default configuration should only provide functions essential to the major purpose. Additional functions are e.g. comfort functions, which are only required under limited circumstances.

27 Only services and software required to provide the functions of the TOE shall be present on the TOE. Development information shall be removed.

28 The TOE shall provide the ability for updates after installation.

29 The TOE shall confirm the authenticity and integrity of update files before installation.
Note: Security updates serve the removal of flaws and errors critical to the safe and secure operation of the TOE.

30 Access to wireless networks shall be secured. If supported, the TOE should integrate access to wireless networks using the system usage control.

3.4 Documentation

31 The applicant shall provide a guidance documentation that describes the secure use of the TOE. This includes the installation, configuration, operation and decommissioning.
Further, the intended use and operational environment shall be described.
Note: This documentation is not limited to the Secure User Guidance and includes all user documentation for the product.

32 The applicant shall document the following features present in the default configuration:

- TOE's interfaces
- Users
- Roles
- Services and related functions
- Activation and deactivation status for the services

Note: The status of the features is not required to be provided in the documentation. Service information can also be provided using a designated service on the TOE.

33 The applicant shall provide advice for the secure operation of the TOE.
Note 1: Advice can be included in the documentation or be provided using a designated service on the TOE, e.g. displayed during configuration.
Note 2: The documentation or configuration advice must provide hints for possible security issues or implications.

3.5 Additional requirements for software applications and applications in virtualised environments

34 The hardware specification shall provide all necessary hardware information such that the TOE can perform its security function in this hardware environment, including but not limited to specific requirements for hardware architecture, network resources and system and storage requirements. Requirements for the system and storage shall be supplemented with minimum and, where appropriate, maximum requirements for necessary resources. For applications in virtualised environments, the information shall also cover virtual hardware components and resources used virtually. If the application requires the use of special hardware in the system environment, then the hardware shall be specified and the usage shall be described.
Note: The information in the hardware specification shall be sufficiently specific that a representative test environment can be selected by the ITSEF for the evaluation of the application.

35 A compatibility description is required in addition to the hardware specification if the TOE is to be used on divergent hardware such as different system architectures or substantially different variants of hardware. The compatibility description shall serve as a basis for the evaluation whether the TOE can perform its security in the specified conditions of the system environment or not. The description shall include the different design of the hardware component, whether it responds to different interfaces and how the behaviour of the hardware components differs.
Note: It is highly recommended to limit the hardware or virtualized environments considered for certification to a number that actually can be effectively evaluated within the allowed evaluation period of the BSZ. The actual number depends, amongst other things, on the number, complexity and diversity of the environments to be considered.

36 The software specification shall indicate the operating system used as well as additional software that is required by dependencies to run the application. This shall be supplemented by minimum and, if necessary, maximum required version number of the software or operating system used.

Note: The information for software may also be designed by means of release data. In this case, it shall be specified, which software versions ensure the secure operation of the application.

37 The indicated software in the software specification shall be provided with software security updates for the period of expected certificate validity.

38 The dependencies of the TOE on the system environment in the form of software packages, interfaces, libraries, links to databases, APIs or others shall be specified. All necessary dependencies shall be sufficiently specified for operators to decide which requirements for hardware and software are to be used for the secure operation of the TOE.
Note 1: The software packages used can be indicated as a list. All other dependencies require a description.
Note 2: Dependencies can also be communication channels such as emails, embedded forms or the user interface, as well as application navigation.
Note 3: Software package dependency lists can be created with the help of package management tools.

39 The TOE shall allow the retrieval of event logs by means of programmed access. Authorised human users should also have read access to event logs. Programmed access can be done via an API or by sending it to a central system.

40 If noise sources are used for, for example, random number generators, they shall be described as required in the document [AIS B2], paragraph “Noise source description”.
Note: There is a BSI study available addressing the use of random number generators in virtualised environments, see link [RNG].

4 Definitions

The following definitions are derived from IEC 62443 Part 1-1 [62443-1-1]:

Asset
Physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization.

Attack
Assault on a system that derives from an intelligent threat — i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
Note: There are different commonly recognized classes of attack:

- *An "active attack" attempts to alter system resources or affect their operation.*
- *A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.*
- *An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.*
- *An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.*

Authenticate
Verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission.

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authorization
Right or permission that is granted to a system entity to access a system resource.

Confidentiality
Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Cryptographic algorithm/operation
Algorithm based upon the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cryptographic key:
Input parameter that varies the transformation performed by a cryptographic algorithm.

Cybersecurity
Actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets.

Data confidentiality
Property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes.

Data integrity
Property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Default configuration
All settings are set to values defined by the developer and no user specific settings exist. Not to be confused with the secure configuration after installation of the TOE according to the Secure User Guidance [AIS B3]

Denial of service
Prevention or interruption of authorized access to a system resource or the delaying of system operations and functions.

Digital signature
Result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation.

Integrity
Quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

Interface
Physical or logical entry or exit point that provides access to the module for logical information flows.

Reliability
Ability of a system to perform a required function under stated conditions for a specified period of time.

Security

a. Measures taken to protect a system.
b. Condition of a system that results from the establishment and maintenance of measures to protect the system.
c. Condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.
d. Capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems.
e. Prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system.

Note: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

Security function
Function of a zone or conduit to prevent unauthorized electronic intervention that can impact or influence the normal functioning of devices and systems within the zone or conduit.

Security perimeter
Boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e., the boundary of the space in which security services protect system resources.

Security policy
Set of rules that specify or regulate how a system or organization provides security services to protect its assets.

Security service
Mechanisms used to provide confidentiality, data integrity, authentication, or no repudiation of information.

Service
Provides different functions using an interface. This might be for example a web server with corresponding web application for configuration.

System
Interacting, interrelated, or interdependent elements forming a complex whole.

User
Person, organization entity, or automated process (service) that accesses a system, whether authorized to do so or not.

5 Reference documents

1 [62443-4-2] IEC 62443 Industrial communication networks – Network and system security Part 4-2 Technical security requirements for IACS components, Edition1.0 2019-02

2 [62443-1-1] Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models, Edition 1.0 2009-07