Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B1, Version 2.0.1

Date:	17.11.2023
Status:	Mandatory
Subject:	Requirements for ST and further documentation
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	2022-05-25	SZ 33	Clarification regarding the publication of the ST Information added on where interfaces have to be listed and described Editorial changes (partly to keep this document consistent with AIS B2) Completed Section 2 and cryptographic references added in Section 5
1.2	2023-06-16	SZ 33	Change to the new BSI document template In Section 1, a sentence for the accessibility of ST documents has been added In Subsection 3.2.2, the title has been extended to include interfaces and the subsection has been better adapted for interfaces In Subsection 3.3.7, the heading has been changed and add that the mapping is required in the form of a table The contents of the previous Section 3.5 Appendix: Cryptographic Specification has been moved into a new Section 4 In Section 4, the heading and the content of Table 2 in Subsection 4.1.1 has been changed In Subsection 4.2.1, the connection to the AIS-31 for CC-certified RNG has been removed Editorial changes
2.0	2023-09-30	SZ 33	Requirements added for software applications and applications in virtualised environments in Subsections 3.1.2, 3.2.1, 3.2.4, 3.3.1, 3.3.6 and added a new Subsection 4.2.4. Reference added to additional requirements for different scopes of the BSZ Requirements added for SBOM in Section 6 Editorial changes
2.0.1	2023-11-17	SZ 33	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

1 The Security Target (ST) describes the security functionality, the interfaces, the threat model and the (expected) environment of the Target of Evaluation (TOE) as used in the BSZ. It shall follow the structure and provide the contents as laid out in Section 3 of this document. The BSI publishes the ST together with the issuance of the certificate. Therefore, it is advisable to prepare a final version of the ST without a version history or any information not intended for publication. The document shall comply with the accessibility requirements for publication on the BSI website. In principle, all personal metadata shall be removed from the final PDF version of the document. In addition, the document should be designed in accordance with the relevant German accessibility regulations [BITV 2.0]. The release version shall not have any change marks. If cryptographic mechanisms are part of any security functionality, they shall be included in the cryptographic specification as described in Section 4. If this specification is not intended to be published together with the ST, it may be provided in a separate document.

2 Specific scopes of the BSZ include additional requirements for the content of the security target.

3 All technical terms used in the ST document, which are not self-explanatory, shall be defined. Definitions can be given in the main section or by references to stable and accessible sources under public domain.

4 The description shall avoid company-specific terminology where possible. However, if certain company-specific terminology is used, a brief explanation shall be provided.

5 If a product was evaluated in a previous BSZ procedure, it is possible to reduce the evaluation effort for a new BSZ procedure. The applicant shall provide an Impact Analysis Report (IAR) for this, describing the changes to the TOE as well as modifications to any documents relevant to the certification. The IAR shall follow the structure and provide the contents as laid out in Section 5.

6 A Software Bill of Materials (SBOM) is a list of software components. An SBOM contains information on the elements (e.g. libraries) which are provided by the manufacturer himself, are created by third parties or are open source software components. Therefore, it is an important tool for transparent presentation of the software composition. It can be created automatically and shall be presented in the form of a machine readable file. The requirements for the content of SBOM is set out in Section 6.

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

5 [AIS B3] Requirements for user guidance, BSI

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

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

8 [AIS B6] Requirements for a TOE, BSI

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

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

3 Security Target

7 The following sections describe in detail how the Security Target shall be organised and which content is expected in the various sections. Where applicable, a subsection provides examples and further explanation.

8 Unless noted otherwise, the ST shall be written in a way that the expected end customer, i.e. the person who decides about the acquisition of the product, is capable of understanding its content. *Note: For some TOEs this might be a procurement officer while for other TOEs this might be a layperson. To facilitate the proper understanding, appropriate references to stable reference sources should be provided. The ST may be written in English or German with an approximate length of ten pages excluding the appendix.*

3.1 Introduction

3.1.1 Context of this document

Required content

9 This subsection shall describe why this document was created and how the content was derived.

10 It shall list (i.e. by name and function) or reference (i.e. only by function) the key personnel involved in the development of the ST.

3.1.2 Product identification

Required content

11 This subsection shall state, without ambiguity, the name and specific version of the TOE, including where applicable, the distinct version numbers of the software and the hardware. It shall also state how the expected end customer can unambiguously identify the product.

12 For integrated systems with hardware-related programming the name of the TOE shall be given as „{product category} [TOE name] – software version [X.X] from the company [company name]“.

13 For software applications or applications in virtualised systems, the name of the TOE shall be given as „[software application/virtualised application] [TOE name] – version [X.X]running on [name of the hardware platform with cpu model] from the company [company name] {for the system/the machine/self-chosen [device name]} in the product category [category name]“
Note: The content in the {} - brackets is optional. The slash (/) allows a selection.

3.1.3 References / acronyms

Required content

14 This subsection shall list all acronyms used.

15 This subsection shall contain all references, e.g. to implemented standards or to further documents of the vendor. If further documents of the vendor are referenced, they need to be available to all customers free of charge.

16 All content required by this document shall appear in the ST document itself and not in referenced documents, except for the cryptographic specification which shall be supplied separately.

3.2 Product description

3.2.1 General description

Required content

17 This subsection shall contain a general description of the TOE suitable for publications on websites or in product databases.

3.2.2 Features and interfaces

Required content

18 This subsection shall list and describe the features and interfaces of the TOE that are relevant to the BSZ evaluation. The terms used shall be defined if they are not self-explanatory. Definitions can be given in the main section or by references to stable and accessible sources under public domain.

19 The description shall avoid company specific terminology where possible.

20 Any communication interfaces shall be listed and described in this subsection.

21 Features and interfaces which are not accessible for testing shall be clearly marked as such.

3.2.3 Product usage

Required content

22 This subsection shall describe in natural language the intended product usage, which is specific for the intended target audience to decide whether the product is suitable for their intended purpose. The details of the operating environment shall be stated in the subsequent subsections.

3.2.4 Operating environment

Required content

23 This subsection shall state the required operating environment of the TOE, i.e. technical environment, expected users, expected threats.

24 Specific hardware or software required to operate the TOE shall be stated in this subsection.

25 If several environments are possible (e.g. several versions of some background systems or operating systems), it shall be clearly stated which version is to be used for evaluation.

For software applications and applications in virtualised environments

26 The system environment can be defined by concrete specifications for the hardware and software to be used or described by requirements and dependencies of the TOE according to the system environment.

27 If the applicant does not provide specific models or series of models for the TOE, minimum and, where necessary, maximum requirements for hardware and software for the secure operation of the TOE shall be specified and indicate in the hardware and software specification.
Note: Requirements for the system environment, which lead to potentially large combinations in the design of hardware and software, may require increased test effort and exceed the complexity limit or maximum test duration for a certification in the BSZ procedure.

28 If the design of the hardware can be realised by several different combinations of components, the hardware specification shall be extended by a compatibility description. This shall include a description of the required behaviour of specified hardware in terms of dependencies on the system environment.

29 For the certification, a specific selection of hardware and software as the representative test environment will be proposed in writing from the ITSEF before the kick-off meeting and will be defined in the kick-off meeting. The selection shall be based on the hardware and software specification provided by the applicant and shall be typical for the TOE.
Note: The test environment can represent more than one specific selection of the hardware and software specification for the evaluation of the TOE.

30 The system environment shall comply with the requirements for the application to be certified as listed in the document [AIS B6] under chapter 3.5.

3.3 Security perimeter

3.3.1 Users

Required content

31 This subsection shall describe the users or roles the TOE supports. The users or roles are not limited to those explicitly defined in the TOE. They might also be defined implicitly by the interface they act on (e.g. on a certain port of a firewall). This subsection shall describe the characteristics of each user or role, i.e. which kind of tasks it is associated with, if it has certain privileges in the TOE, if access is limited to certain ports etc.

32 For software applications and applications in virtualised environments, it is necessary to implement an appropriate role and authorisation concept for the operation of the TOE in the operational environment. The mandatory roles are the user of the TOE, the administrator of the TOE and the administrator of the operational environment:

- The user of the application is the user of the TOE and shall not have any administration rights.
- The application administrator have extended rights towards the TOE and shall be responsible for its administration and installation.
- The system administrator shall have the right to manage, install and administrate the system environment and may be extended by different authorised administrators depending on the set-up of the system environment.
- System administrator: The system administrator has physical access to the system environment and is responsible for management, administration and deployment of the system inside the environment. This is, for example, the management of domains and users.

Note: Depending on the complexity of the TOE or its operational environment, roles can also be implemented through different users. If the TOE also offers other internal roles, such as users of databases, this should be described in detail. When multiple roles are grouped into a single user, it is important that the access rights remain separate. I.e. the application software cannot be operated with the rights of an administrator.

3.3.2 Assumptions

Required content

33 The TOE might require a certain environment to fulfil its security properties. This environment may consist of personal attributes (e.g. required knowledge and skills of certain users), logical requirements (e.g. network topology), physical measures (e.g. physical access restrictions) organisational necessities (e.g. rights and roles) or IT-related assumptions (e.g. encryption used on network links). A brief colloquial rationale for the existence of these assumptions shall be provided in this subsection.

Note: This subsection shall be consistent with all other subsections, especially Subsection 3.2.3. For example, requiring certain knowledge of the user of the TOE is inconsistent with a product description, which claims that the product is intended for the general public.

34 Each assumption shall be uniquely identifiable.

3.3.3 Assets

Required content

35 This subsection shall list and describe the assets of the TOE or protected by the TOE, whose security properties (i.e. confidentiality, integrity or availability) are worthy of protection.

36 Each asset shall be uniquely identifiable.

3.3.4 Threat model: attackers

Required content

37 This subsection shall describe the attackers assumed in the threat model. They shall be the most likely expected attackers of the TOE in the intended environment.

38 Each attacker shall be uniquely identifiable.

3.3.5 Threat model: threats

Required content

39 This subsection shall describe the threats, which are countered by the security functions of the TOE.

40 Each threat shall be uniquely identifiable.

3.3.6 Security functions

Required content

41 This subsection shall contain a specification of the security related functions of the TOE. It shall reference where necessary the technical information (for example Layer 2, Protocol xy), where possible by referencing the appropriate and active standards. Stable online references should be used.

42 This subsection may refrain from using end customer language as long as technical terms suitable for average experts are used.

For software applications and applications in virtualised environments:

43 The TOE shall has sufficient own security functions that can be evaluated through external interfaces.

44 If the ST designates security functions that are fully or partially implemented by the system environment, they shall be specified in the document describing the dependencies to the system environment. The indication of a user for the security function from the role model is necessary if the TOE requires separate rights for the call or implementation of the security function. It shall be clearly described which parts of the security functionality are realised by the system environment and how these parts are integrated or used by the TOE to provide the security function to be tested.

45 In addition to the security functions provided by the TOE itself, security functions that are fully or partially implemented by the system environment shall also be indicated in the ST as security functions used. The designation of the security function shall clearly allow a distinction between those provided by the TOE itself and the security function implemented in the system environment.

3.3.7 Mapping

Required content

46 This subsection shall contain a table mapping of all threats to the associated attackers, the affected assets and the involved security functions. For complex relationships, it may contain a terse rationale.

3.4 Limits of evaluation

Required content

47 This subsection shall contain all features, functions, services and interfaces that are out of scope of this certification. The excluded items may not contradict the intended usage of the TOE.

48 If the TOE security functions require dynamic content to operate (e.g. from remote databases), the ST shall clearly state that the remote system providing the content is not part of the evaluation. However, the security function requiring the content shall be part of the evaluation.

4 Separate annex: cryptographic specification

49 The evaluation and certification require special attention if the ST includes any security functionality realised by cryptographic mechanisms or if the TOE provides cryptographic services (such as encryption routines, generation of hashes, generation of signatures, random number generation, key generation and communication protocols using encryption). To avoid any pitfalls due to conformity issues and to optimize the certification process, the applicant shall provide an overview of all included mechanisms and provided services, which are enabled in the secure configuration as described in the manual or secure user guidance, and which are in the scope of the evaluation.

4.1 List of cryptographic mechanisms

Required content

50 The applicant shall provide a cryptographic specification for the cryptographic mechanisms that are used to enforce the security functionality of the TOE. An overview of the cryptographic mechanisms used shall be presented in a table as shown in the example below.
Note: Cryptographic mechanisms may include but are not limited to (symmetric / asymmetric) encryption schemes, hash functions, message authentication codes, (password-based) key derivation functions, digital signature schemes, key establishment schemes, (symmetric / asymmetric) data origin authentication schemes, (symmetric / asymmetric) entity authentication schemes, authenticated encryption schemes, (password-)authenticated key establishment schemes, secret sharing schemes, cryptographic protocols, and deterministic random number generators.

51 Cryptographic mechanisms used by the TOE should be agreed algorithms from the SOG-IS catalogue [SCES-ACM]. Other mechanisms, in particular cryptographic protocols, shall be approved by the certification body before the start of the evaluation. Cryptographic protocols endorsed by the certification body comprise the recommendations of the Technical Guideline [BSI-TR-02102] (Parts 2 - 4).

52 The description of a cryptographic mechanism shall be categorized by interfaces and shall contain the following information:

- References to accessible standards that unequivocally define the mechanism, together with selected options or parameters (e.g. key lengths, domain parameters, etc.),
- The security functionality enforced by the mechanism (mapping to the security functions claimed in the security target),
- The security objective achieved by the mechanism (e.g. confidentiality, integrity, authenticity, etc.).

53 The definition of a cryptographic scheme or protocol usually requires the definition of several algorithms (e.g. encryption schemes require the definition of a key generation algorithm, an encryption algorithm, and a decryption algorithm).

Examples

1. Purpose	*2. Cryptographic Mechanism*	*3. Standard of Implementation*	*4. Key Size in Bit*
Trusted Channel to … via HTTPS with TLS 1.3 [RFC 8446]			
Authenticity	RSA-signature generation and verification (RSASSA-PSS) using SHA-256	[PKCS#1 v2.2] (RSA), [FIPS 180-4] (SHA)	Modulus length = 2048
Authentication	RSA signature generation and verification (for RSASSA-PSS)	[RFC 5246] (TLS) [RFC 3447] (PKCS#1 v2.1)	3072, 4096
Key Agreement	ECDHE curves: secp256r1, secp384r1	[RFC 5246] (TLS) [RFC 8422] (TLSECC) [IEEE P1363] (ECDH)	256, 384
Key Agreement	DHE groups: ffdhe3072, ffdhe4096	[RFC 5246] (TLS) [RFC 7919] (DHE)	3072, 4096
Confidentiality	AES in GCM mode	[RFC 5246] (TLS) [RFC 5288] (AESGCM) [RFC 5289] (AES-GCM) [FIPS 197] (AES) [SP800-38D] (GCM)	128, 256
Confidentiality	AES in CBC mode	[RFC 5246] (TLS) [FIPS 197] (AES) [SP800-38A] (CBC)	128, 256
Integrity	HMAC with SHA-2	[RFC 5246] (TLS) [FIPS 180-2] (SHA)	256, 384
Random Number Generator	Deterministic RNG DRG.3	[AIS-20]	

Table 2: Example of a table with cryptographic mechanisms

1. Purpose	*2. Cryptographic Mechanism*	*3. Standard of Implementation*	*4. Key Size in Bit*
Trusted Channel to Command Line Interface (CLI) with SSH [4251]			
Key Exchange (Agreement)	diffie-hellman-group15-sha512	[RFC 4253] (Key Exchange Methods) [RFC 8268] (more DH for SSH) [RFC 3526] (group specification)	3072
Authentication	Elliptic curve digital signature algorithm with SHA-256 and nistp256 (ecdsa-sha2-256)	[RFC 5656]	256

1. Purpose	***2. Cryptographic Mechanism***	***3. Standard of Implementation***	***4. Key Size in Bit***
Confidentiality	AES in CTR mode	[RFC 4344] (SSH Encryption Modes)	128, 192, 256
Integrity	HMAC with SHA-2 (hmac-sha2-256)	[RFC 4253] (SSH) [RFC 6668] (SHA-2 Integration) [RFC6234] (SHA-2 Definition)	256
Random Number Generator	/dev/urandom		

Table 3: Example of a table with cryptographic mechanisms

4.2 Noise source description

Required content

54 If the cryptographic specification contains random number generators, the applicant shall provide a noise source description as a chapter in the separate “crypto-annex” for the noise sources that are used for seeding.

55 The description of a noise source should contain information about its type (physical or non-physical) and operating principle.

56 If multiple noise sources are used, a justification should be given that the sources are independent.

57 The noise source description should contain a justification that random bits used for seeding have at least 125 bits of min-entropy. If a CC-certified physical random number generator is used, a reference to the certification ID is sufficient.

4.3 Key management description

Required content

58 The applicant shall provide a key management description as chapter in the separate “crypto-annex” containing information about cryptographic keys and parameters that are used by the TOE for cryptographic operations.

59 The description of a key should contain information about its type, generation, distribution, usage, storage, destruction, validity time period, and protection requirements.

60 The key management description shall also contain information on other relevant parameters including domain parameters, initialization vectors, counters, and tweaks.

61 The key management description shall highlight hierarchical relations between keys (e.g. whether a key is derived from another key, or whether a key is encrypted using another key).

4.4 Implementation representation

Required content

62 The applicant shall provide the ITSEF with an implementation representation for the cryptographic mechanisms that are used to enforce the security functionality of the TOE. If the applicant cannot provide the implementation representation for one or several cryptographic mechanisms, the ITSEF shall discuss the ability of the certification with the certification body before the start of the evaluation.

63 The implementation representation should consist of source code or pseudo code. If sourcecode is provided, it shall be the code that was used to build the TOE. If pseudocode is provided, it shall be at a level of detail that closely resembles the actual implementation (in particular, it shall include side-channel countermeasures if implemented).

64 The implementation representation shall cover the implementation of cryptographic functionality itself as well as the parts of the implementation where the cryptographic functionality is invoked.

65 If the implementation uses open-source cryptographic libraries, the implementation representation shall include information about their origin, version, and all changes applied by the applicant.

5 Impact Analysis Report

66 If a product has already been evaluated in a previous BSZ procedure, it is possible to reduce the evaluation effort for a new BSZ procedure. For this purpose, the applicant shall submit an Impact Analysis Report (IAR) together with application documents.

67 In the IAR, the applicant shall report the changes regarding the TOE as well as including a description of the modifications to the application documents. The IAR shall be sufficiently accurate to be understood by evaluators and certifiers. Any documentation not supporting the evaluation of the previously evaluated TOE but supporting the evaluation of the modified TOE shall be indicated.

68 The IAR does not replace the updating of the documentation. The applicant shall clearly indicate the changes to the documentation, e.g. by using change marks. A classification of the changes in the documentation is not required. If change marks are used, any unmarked content is valid for the previously evaluated TOE as well as for the modified/re-evaluated TOE, any marked content is either editorial or it concerns the modified TOE only.

5.1 Changes to the product compared to the previous evaluation

Required content

69 The IAR shall contain a summary describing all changes to the product. It shall explicitly address all issues from the last evaluation and all further changes (e.g. maintenance or product improvement, if any).

Examples

70 To address issue #5 (vulnerability to long input strings), library XYZ has been changed from version 1.0.1 to version 1.0.2. All other issues (#1-#4 and #6) have been addressed by explicit code changes. Further, this maintenance release fixes CVE 2020-06-23, CVE-2020-04-27 and CVE-2020-05-118 and deny-lists the new Unicode range to avoid potential security implications.

5.2 Description of modifications to the applicant documents

5.2.1 Changes to the Security Target

Required content

71 The applicant shall report whether the change is editorial (e.g. product name, version) or whether the change affects the content (e.g. description of the TOE, assumptions, threats or security requirements).

Examples

72 The Security Target was only updated with newer version numbers (TOE, Secure User Guidance).

5.2.2 Changes to the design and implementation of the product

Required content

73 The applicant shall report changes to the design and implementation with the objective of indicating the reference of the changes to the security functionality including the security architecture (e.g. new filtering libraries for handling input). Depending on the size and impact of the change, this might be a short reference to publicly accessible sources or some paragraphs describing the change.

Note: The objective of this description is to provide sufficient detail to allow an efficient re-evaluation. Depending on the size and complexity of a change, each description might be quite abstract, e.g. using a newer version of a library, or provide a more low-level description including source code or pseudocode excerpts.

Examples

74 *Updated network state machine to handle CVE 2020-06-23 by special casing it early in the processing, i.e. before processing the forwarding rules.*

75 *Updated OpenSSL to 1.1.1.g to address CVE-2020-04-27 and CVE-2020-05-118.*

76 *Updated filtering routine to also handle Unicode chars in the range …*

```
// Before any processing is done:
for each input string
for each unicode character
if unicode character in (updated) blacklist then replace character by
NULL character
```

77 *Updated library XYZ to version 1.02 to prevent overlong strings.*

5.2.3 Changes to the guidance documents

Required content

78 The applicant shall report the changes to the guidance documents (e.g. Secure User Guidance).

Examples

79 *Clarified that user names and password may not contain Unicode characters in the range (…).*

80 *Addressing the issue #7 from the previous evaluation in the Secure User Guidance that the password reset procedure is described confusingly/ambiguously.*

5.2.4 Changes to requirements for software applications and applications in virtualised environments

Required content

81 The submitter shall report any changes to the role- and authorisation concept that have an impact on the behaviour of the TOE in the operational environment. In case of re-certification, it is necessary to report whether existing functionalities have been outsourced to the system environment or added to it, as well as whether requirements or dependencies on the system environment have changed.

Example

82 *In the previous version 2.7.18 of the FooApp, the application still managed the user data itself and encrypted the data in a corresponding compiled user directory for each implemented user individually. With the new stable version 3.1.4 of FooApp, the user data management has been transferred to the operating system responsible for the creation of the user rights. Therefore, all user data under the file path X/y/z is forcibly stored in such a way that only the authenticated user can access their own dataised environments*

5.3 Discussion of the impact of changes

Required content

83 During the re-evaluation, the ITSEF is responsible for performing all necessary work to attest the trustworthiness of the modified product. Nevertheless, the discussion of the applicant will help the evaluator to estimate the required effort and facilitate the preparation of the kick-off with the certification body.

84 This IAR discussion needs to explicitly address every issue identified in the previous evaluation. In case not every issue is (fully) resolved by the applicant, a justification needs to be given as to why this does not lead to a security problem, e.g. implementation of further/other measures that prevent/mitigate the issue. The ITSEF has to assess this justification, which will require further testing efforts.
Note: This assessment has to take into account the state of the technology and also whether the justification is actually acceptable from an end user perspective.

Examples

1. *The change in the state machine concerns the corner case mentioned in CVE 2020-06-23 only. No further changes are applied and the corner case has been added to the default set of unit tests in several variations. Thus the impact on the correct processing of network packets is very low and only the corner case is changed.*
2. *OpenSSL 1.1.1g is a pure maintenance release only compared to the previously used 1.1.1f. It addresses 35 CVEs, for which only CVE-2020-04-27 and CVE-2020-05-118 are applicable to the TOE. OpenSSL has a good track record of clarifying changes and maintenance releases are strictly bound to fixing security issues (which are clearly described in the release notes). Also the results of all OpenSSL internal as well as product specific unit tests did not change and text cases for the aforementioned CVEs have been added. Thus the security impact on introducing new unknown security issues in the TOE is low.*
3. *The Unicode Consortium released a new version of Unicode with more characters. As these are most likely not relevant for production systems, the previous filter has been extended to deny-list these as well. As these only extends the deny-list, there is no further security impact from this change.*
4. *Issue #1 has been addressed by an explicit timing mechanism to make all responses time out at the same time, irrespective if the credential was (partial) correct. A new unit test covers this test case and the credential checking itself remains unchanged (which was not subject to any issue) thus the security impact of the change is low.*
5. *Issue #2 …*
6. *Issue #5 has been fixed by updating the library XYZ. Version 1.02 no longer accepts strings of arbitrary length at any place, throwing an error immediately which is duly handled in all instances in the code. Since this is the only change from Version 1.01 and unit tests both in library XYZ and for the TOE have been added, the impact of this change remedies the error stated in ETR in subsection X.Y.Z.*

6 Software Bill of Materials

85 The applicant shall provide a software bill of materials (SBOM) as defined in Section 6.1. For every component included in the TOE where the vendor of the TOE is the supplier, the applicant shall provide a corresponding SBOM entry.

86 For every third-party component that is directly used in a component for which the vendor of the TOE is the supplier, a corresponding SBOM entry shall be provided. Standard libraries of programming languages directly used in components for which the applicant is the supplier also fall under this stipulation. A software library A is considered to be directly used in a software library or application B if the source code of B contains calls to one or more procedures provided by A.

87 If the TOE consists of or includes multiple applications that must either run permanently (e.g., a webserver) or in response to one or more events (e.g., expiration of a timer) to provide one or more of the TOEs functionality, then an SBOM entry for each of these applications shall be provided.

88 If the TOE includes an operating system kernel, a corresponding SBOM entry shall be provided by the applicant, irrespective of whether the applicant is the supplier of the component.

89 If the supplier of a third-party component covered by the above conditions provides an official SBOM for this component that satisfies the definitions given in Section 6.1, then the official SBOM shall also be provided to the ITSEF. A corresponding entry for the third-party component in the SBOM for the TOE shall be omitted in this case.

90 Every SBOM entry shall correspond to the component that is actually included in the product. Components used for testing or debugging variants of the product shall not be included in the SBOM provided by the applicant.

91 If a specific component is included multiple times in the product (e.g., a specific version of a software library that is included in multiple applications running on the product), then only one corresponding entry in the SBOM is required. However, if multiple different versions of a particular component from a particular supplier are used in the product, then a separate entry shall be provided for each included version of the component.

6.1 Definition of SBOM

92 An SBOM is a list of entries that adheres to a specific format, where each entry contains identifying information about a single component and possibly further associated information. The format used for an SBOM should either be CycloneDX[2] (version 1.4 or above) or Software Package Data Exchange[3] (version 2.3 or above) in any representation supported by the respective format (e.g., JSON or XML).

93 In addition to the actual list of component entries, an SBOM shall include the following information:

Attribute	***Definition***	***Recommended format field***	***Remarks***
Author	The name of the entity that created the SBOM.	SPDX: Creator/Creators[4] CycloneDX: "authors" property of "metadata" element[5]	The name of the legal entity, e.g., the company name, is sufficient as author information.

[2] https://cyclonedx.org/specification/overview/

[3] https://spdx.dev/specifications/

[4] https://spdx.github.io/spdx-spec/v2.3/document-creation-information/#68-creator-field

[5] https://cyclonedx.org/docs/1.4/json/#metadata_authors

Attribute	*Definition*	*Recommended format field*	*Remarks*
Timestamp	Date and time when the SBOM was created by the author.	SPDX: Created[6] CycloneDX: "timestamp" property of "metadata" element[7]	The timestamp shall follow the format mandated by the chosen SBOM format (e.g., SPDX or CycloneDX).

Table 4: Minimum set of attributes required for SBOM description.

94 A component is a unit of software, e.g., in the form of an application, a software library, an operating system, or firmware, which consists of one or more files. The SBOM entry for each component shall include at least the following information:

Attribute	*Definition*	*Recommended format field*	*Remarks*
Supplier name	The name of the entity that created and/or maintains the component.	SPDX: PackageSupplier[8] CycloneDX: "supplier" property of object under "components"[9]	For proprietary components, the name of the legal entity, e.g., the company name, is sufficient as supplier name. For open source components, the name of the entity, project or service from which the component was obtained, either in a pre-compiled package or as source code, shall be provided as supplier name (e.g., Python Package Index, Debian, Ubuntu, Github).
Component name	The designation assigned to the component by the supplier.	SPDX: PackageName[8] CycloneDX: "name" property of object under "components"[9]	The value given for this field should describe the most common and recognizable title or name of the component
Version of the component	The identifier used by the supplier to specify a change in software from a previously identified version.	SPDX: PackageVersion[8] CycloneDX: "version" property of object under "components"[9]	Semantic versioning[10] should be used. If no official version identifier exists for the described component, then the identifier of the most recent version upon which the described component is based shall be provided. Furthermore, the applicant shall provide a summary of the changes between the most recent version upon which the described component is based and the one described by this SBOM entry in a separate document.

Table 5: Minimum set of attributes required per SBOM entry.

95 A component is called a "third-party component" if the applicant is not the supplier of the component.

96 Templates that may be used to create an SBOM according to the above definition are available upon request at the certification body. Those templates contain the minimum number of fields in each

[6] https://spdx.github.io/spdx-spec/v2.3/document-creation-information/#69-created-field
[7] https://cyclonedx.org/docs/1.4/json/#metadata_timestamp
[8] https://spdx.github.io/spdx-spec/v2.3/package-information/#75-package-supplier-field
[9] https://cyclonedx.org/docs/1.4/json/#components_items_name
[10] https://semver.org

SBOM representation necessary to comply with the above requirements as well as those mandated by the respective format. Each placeholder in the template shall be replaced with a correct entry that is conformant to the requirements of the corresponding format.

6.2 Optional vulnerability report

97 As a supplement to each SBOM given to the ITSEF, the applicant may provide a vulnerability report for one or more components listed in the SBOMs provided by the applicant. Each such vulnerability report should encompass vulnerabilities listed in the publicly available CVE dataset that apply to the respective component as well as vulnerabilities that are not publicly listed. It is advisable to submit a vulnerability report to speed up the evaluation, especially if it is known that components with vulnerabilities exist in the TOE.

98 For each vulnerability listed in the vulnerability report for the respective component, the applicant shall provide the following information:

Attribute	***Definition***	***Remarks***
Vulnerability identifier	A unique label or tracking ID used to identify the vulnerability.	If existing, the MITRE standard "Common Vulnerabilities and Exposures" (CVE) tracking number for this vulnerability shall be provided.
Vulnerability status	An assertion about the status of the vulnerability, which may either be "Fixed", "Not affected", "Affected" or "Under investigation".	The assertions carry the following meanings: • Fixed: The referenced vulnerability has been fixed in this version of the component. • Not affected: The referenced vulnerability cannot be exploited for the given TOE (e.g., due to remediations in other components or because the affected functionalities are disabled). • Affected: The referenced vulnerability can be exploited for the given TOE. • Under investigation: The applicant is currently unaware whether the vulnerability can be exploited for the given TOE.
Remarks	Explanations related to the status of the vulnerability.	If "Not affected" is reported as status for the vulnerability, a brief justification shall be provided. For other reported statuses, a brief justification may be provided.

Table 6: Set of attributes required for a vulnerability report

99 The format of the report may conform to the VEX Profile[11] of the "Common Security Advisory Framework" (version 2.0 or above) or to the "vulnerability" property[12].

[11] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#45-profile-5-vex External Link

[12] https://cyclonedx.org/docs/1.4/json/#vulnerabilities

7 Reference documents

1 [SCES-ACM] SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, current version

2 [BSI-TR-02102] Technischen Richtlinien der Serie BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI

3 [AIS-20] Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI

4 [BITV 2.0] Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0)