Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B2, Version 2.0

Date:	30.09.2023
Status:	Mandatory
Subject:	Requirements for the evaluation of cryptographic mechanisms according to the BSZ
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	2022-04-28	SZ 33	Update of structure: Section 4 Target of Evaluation is now Subsection 3.1.2 Numbering of paragraphs revised Clarification of submitter deliverables Further BSI guidance added to the recommended information sources Specified requirements for the identification of potential flaws Extended and specified requirements for penetration testing
1.2	2023-05-04	SZ 33	Change to the new BSI document template Updated rules for documentation provided by applicant Rules for certified RNGs updated Example for cryptographic specification in Section 4 updated Editorial changes
2.0	2023-09-30	SZ 33	Section 3.2: Evaluation Methodology based on EN 17640 Fixed-time cybersecurity evaluation methodology for ICT products [FiT CEM] 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 This document contains requirements for the evaluation of cryptographic mechanisms in the context of the BSZ and addresses evaluators of BSZ procedures. In order to provide a complete collection of the requirements for the evaluation of cryptographic mechanisms, some requirements in this document might also be found in other BSZ documents.

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-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 Application notes and interpretation

3.1 Input by the applicant

2 This section describes the input by the applicant, which is necessary for the evaluation of cryptographic mechanisms. The input consists of documentation and the Target of Evaluation (TOE).

3.1.1 Documentation

3 The applicant shall provide the documentation described in [BSZ-Prod], [AIS-B1], and [AIS-B3]. For the sake of completeness, all necessary applicant documents are listed in this subsection and the requirements for the cryptographic specification are listed in the exact manner as in [AIS-B1].

Security Target and Secure User Guidance

4 The applicant shall provide a Security Target (ST) (according to [AIS-B1]), a Secure User Guidance (SUG) (according to [AIS B3]), and the overview of the TOE architecture. In the case of a re-evaluation or re-certification, the applicant shall further provide an Impact Analysis Report (IAR) (in accordance with [AIS-B1]).

Cryptographic specification

5 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 Section 4. The cryptographic specification shall be provided as a separate document named "Crypto-Annex" and shall contain the contents mentioned in lines 6 to 8. It shall not be an appendix of the Security Target.
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.

6 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).

7 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.).

8 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).

Noise source description

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

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

11 If multiple noise sources are used, a justification that the sources are independent shall be provided.

12 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.

Key management description

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

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

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

16 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).

Implementation representation

17 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, this shall be discussed with the certification body before the start of the evaluation.

18 The implementation representation should consist of source code or pseudocode. If source code 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).

19 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.

20 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.

3.1.2 Target of Evaluation

21 The applicant shall provide the ITSEF with the TOE for the evaluation. This includes a configuration for the TOE and its operational environment that is suitable for testing.
Note: For details and further regulations see [BSZ-Prod], [BSZ-EP] and [AIS-B4].

22 The applicant may provide a simulator for the firmware of the TOE for testing.

3.2 Evaluation of implemented cryptographic functions

23 The BSZ cryptographic evaluation consists of conformity assessment, vulnerability analysis and penetration testing.

Conformity assessment and vulnerability analysis

24 The aim of conformity assessment in the context of BSZ cryptographic evaluation is to determine that the cryptographic mechanisms of the TOE are in accordance with SCES (SOG-IS Crypto Evaluation Scheme) and BSI policies and that the implementation of the TOE is compliant with the applicant documentation.

25 The aim of vulnerability analysis in the context of BSZ cryptographic evaluation is to determine that the cryptographic implementation does not contain exploitable implementation weaknesses. In order to identify potential flaws in the implementation, the evaluators should use their experience and all information at their disposal. In particular, the evaluators should already search for potential vulnerabilities during the conformity assessment activities.

26 The ITSEF shall report any detected nonconformity in the ETR.

27 The ITSEF shall execute work unit 1 from Section 6.12 [FiT CEM] (6.12.4.1).

28 The ITSEF shall examine the noise source description to determine that the entropy claim of the applicant is plausible.

29 The ITSEF shall execute work 2 from Section 6.12 [FiT CEM] (6.12.4.1).

30 Conformance testing should achieve a high coverage of the externally accessible cryptographic algorithms, schemes and protocols.

31 Standardized cryptographic protocols used for communication via external interfaces should be tested using automated test tools in order to save evaluation time for aspects that require human analysis.

32 The ITSEF should take the following publicly available sources of information into consideration:

- SCES guidance: [SCES-ACM],
- BSI guidance: [BSI-TR-02102], [BSI-RSA], [BSI-ECC], [BSI-TR-03116], [BSI-TR-03109],
- Security considerations in cryptographic standards,
- Academic literature,
- CVE entries, security advisories of CERTs or vendors, changelogs of cryptographic libraries, blogs of security researchers,
- Information on potential vulnerabilities provided by the certification body itself.

33 The ITSEF should take the following types of attack into consideration:

- Bypass of cryptographic functionality,
- Logical attacks,
- Reaction/oracle attacks,
- Timing attacks.

34 The ITSEF shall take the impact of the operational environment of the TOE on the identification of potential flaws into consideration.
Note: Vulnerabilities in cryptographic implementations may arise due to misuse of mechanisms, implementation weaknesses/errors, or side-channels. Whether a vulnerability or side-channel leads to

an attack depends, among other things, on the ability of the attacker to operate in the operational environment of the TOE. This might lead to might additional types of attacks, e.g.:

- *Side-channel attacks: power consumption, electromagnetic emanation, sound emanation, etc.,*
- *Fault attacks,*
- *Micro architectural attacks: cache attacks, branch prediction, speculative execution etc.,*
- *Cold boot attacks*.

Penetration testing

35 The aim of penetration testing is to determine that the cryptographic implementation resists attacks, i.e. the cryptographic implementation does not contain vulnerabilities that could be exploited by attackers with “enhanced basic” attack potential [FiT CEM] (5.4).

36 The ITSEF shall attempt to bypass or break the cryptographic security functionality. The evaluator shall set up a risk-based sampling strategy for this, taking into account the time allocated for this step. The testing strategy shall be based on the results previous steps of the evaluation, including the conformity assessment, the identification of potential flaws, and the evaluation steps described in [AIS-B4].

37 The testing strategy shall be continuously updated, especially when results (including those from the other steps) become available. If more time is needed for this step than initially allocated, the ITSEF shall record this fact and provide a rationale for this in the ETR.

4 Table of cryptographic mechanisms

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]	

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
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 2: Example of a table with cryptographic mechanisms

5 Reference documents

1 [FiT CEM] Fixed-time cybersecurity evaluation methodology for ICT products (FiT CEM), EN 17640:2022

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

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

4 [BSI-RSA] RSA-Leitfaden: Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_BSI_guidelines_SCA_RSA_V1_0_e_pdf.pdf?__blob=publicationFile&v=1

5 [BSI-ECC] ECC-Leitfaden: Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_ECCGuide_e_pdf.pdf?__blob=publicationFile&v=3

6 [BSI-TR-03116] Technischen Richtlinien der Serie BSI-TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung, BSI

7 [BSI-TR-03109] BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, BSI

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