Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B4, Version 2.0

Date:	30.09.2023
Status:	Mandatory
Subject:	Requirements for evaluation 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	2022-07-15	SZ 33	Evaluation added task concerning: AIS B6 conformance interfaces added Requirements for the ETR delivery clarified List of receivables updated: statement on conformance with [AIS B6] components of operational environment necessary to operate the TOE.
1.2	2023-06-16	SZ 33	Change to the new BSI document template Specified evaluation task concerning the evaluation of cryptographic functions and specification Minimum time between sending in the kick-off presentation and the kick-off specified Content of the Kick-Off presentation specified Content of the ETR concerning time used for the evaluation specified Editorial changes
2.0	2023-09-30	SZ 33	Sections 3.1.1, 3.1.5, 3.2.2.1, 3.3.2.1, 3.3.3.1, and 3.3.5: Added extra task for the evaluation of software applications and applications in virtualised environments. Evaluation Methodology based on EN 17640 Fixed-time cybersecurity evaluation methodology for ICT products [FiT CEM] This includes a new structure in the Sections 3.1 and 3.3. Structure of evaluation phases and steps aligned to structure of [BSZ-EP] 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 describes in detail requirements for a BSZ evaluation implementing the EN 17640 Fixed-time cybersecurity evaluation methodology for ICT products (FiT CEM) [FiT CEM]. The content of this document is mandatory for every BSZ ITSEF and every BSZ evaluation.

2 The document covers both, the initial BSZ evaluation and the re-certification or re-evaluation.

3 Specific scopes of the BSZ include additional tasks for the BSZ evaluation or refine tasks specified in this document. The scope specific documents provide the additional or modified requirements for the BSZ evaluation.

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-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 Phase 1 – Preparation for a BSZ

3 The objective of this phase is to ensure that the ITSEF is able to properly evaluate the TOE.

4 It is best performed before the application for the BSZ procedure is filed to allow the vendor to address possible issues in their documentation and to verify that the ITSEF has the tools, knowledge, and capacity to perform the evaluation.

5 If the ITSEF needs to acquire additional tools and knowledge to perform the evaluation, this shall be done before the kick-off in Phase 2 (Section 3.2).

3.1.1 Completeness check

6 The main objective of this part of the evaluation is to verify that all necessary documents and items are available. It implements the evaluation task “completeness check” from [FiT CEM] (6.1).

7 The ITSEF shall determine which scope of the BSZ is in effect for the TOE and execute the additional tasks and refined task at the appointed steps in the evaluation.

8 The ITSEF shall execute work unit 1 from Section 6.1 [FiT CEM] (6.1.4.1). The following items are required for every the BSZ evaluation:

- Security Target (ST)
- A brief overview of the principle design of the TOE
- A software bill of materials (SBOM)
- A brief technical description of the update mechanism
- Secure User Guidance (SUG)
- Statement and rationale that the TOE is compliant with requirements for the TOE in the scope in effect, e.g., [AIS-B6].
- Operational environment components necessary to operate the TOE

9 If the evaluated product is an embedded system the additional following items are required:

- If not otherwise specified in the scope in effect, 3 copies of the TOE (including the typical user documentation and manuals)
- A copy of the unencrypted firmware

10 If the evaluated product is software or virtualised product the additional following items are required (c.f. Section 3.5 [AIS B6]):

- Application installation package
- Hardware specification
- Software specification
- Description of the dependencies
- Compatibility description (if necessary)

11 The ITSEF shall check that all additional items required for the scope in effect are present.

12 The ITSEF shall execute work unit 3 from Section 6.1 [FiT CEM] (6.1.4.3)[2]. The items for the evaluation of cryptographic mechanisms are described in [AIS-B2].

13 In case of a re-certification or re-evaluation, the ITSEF shall check that the Impact Analysis Report (IAR) is present.

14 The ITSEF shall execute work unit 2 from Section 6.1 [FiT CEM] (6.1.4.2). The ITSEF may choose to execute this work unit later. It shall be completed before 3.3 Phase 2 – Step 2 Evaluation.

[2] The term white box cryptography used in 1 [FiT CEM] (6.1.4.3) means white box evaluation of the cryptographic implementation.

3.1.2 Security Target evaluation

15 The main objective of this part of the evaluation is to verify that the Security target is suitable as the basis for a BSZ. It implements the evaluation task “FIT Security Target Evaluation” from [FiT CEM] (6.4).

16 The ITSEF shall execute work unit 1a from Section 6.4 [FiT CEM] (6.4.4.1).
The structural requirements for the ST are stated in [AIS-B1]. For this work unit relevant security function means that the security functions are appropriate to counter the threats on the assets, every security function corresponds to at least one of the threats, and the assumptions are sensible and relevant.
The requirements and recommendations concerning the cryptographic algorithms are stated in [AIS-B2].

17 The ITSEF shall confirm that the TOE is identified unambiguously and comprehensibly to the reader with a version number in the ST (no placeholders or blanket statements).

18 The ITSEF shall confirm that the ST is not misleading in respect to the intended use case.

19 The ITSEF shall confirm that the list of assets is complete, given the remaining documentation provided with the TOE.

20 The ITSEF shall check that the list of interfaces of the TOE in the ST is complete and that all interfaces are named correctly.

21 The ITSEF shall confirm that the TOE based on the documents provided by the applicant is conformant to the TOE in the scope in effect, e.g., [AIS-B6].

22 The ITSEF shall verify that the security functions stated in the ST are testable.

3.1.3 Review of documentation for cryptographic functions

23 The main objective of this part of the evaluation is to verify that the documentation of cryptographic mechanisms is complete and to compile a first plan for the cryptographic evaluation.

24 If not already done in previous steps, the ITSEF shall verify that the cryptographic specification covers all security functions, services, and interfaces described in the ST that employ cryptographic mechanisms.

25 The ITSEF shall review the claimed cryptography and prepare a rough plan for the cryptography evaluation according to [AIS-B2]. This plan shall identify the intended sampling strategy.

3.1.4 Review of software bill of materials

26 The main objective of this part of the evaluation is to verify that SBOM is complete and conformant to the requirements stated in [AIS-B1], Section 6.

27 The ITSEF shall check that all entries listed in the SBOM are plausible, in particular with respect to statements and information provided in other TOE documents.

28 The ITSEF shall document any potential implausibility they have identified and wish to clarify during Kick-Off.

3.1.5 Impact Analysis Report evaluation

29 In case of a re-certification or re-evaluation, the ITSEF shall confirm that the Impact Analysis Report (IAR) follows the requirements described in [AIS-B1].

30 In case of a re-evaluation, the ITSEF shall check that the IAR addresses all issues identified in the Evaluation Report (ETR) from the previous evaluation in sufficient detail to enable an efficient re-

evaluation. If this is not the case, the ITSEF shall advise the applicant that the lack of detail will be compensated by a higher evaluation workload.

31 The ITSEF shall document any potential issue they have identified and wish to clarify during Kick-Off.

32 The ITSEF shall review whether there are any risks to impartiality for this BSZ procedure. If such risks are identified, the ITSEF shall document how it manages those risks.

33 If any of the above requirements fail, the ITSEF shall report the failure to the applicant and request an update of the ST or the respective missing TOE(s) or documentation. The ITSEF shall not provide consultancy on how to remedy the failure.

3.1.6 Additional tasks for software applications and applications in virtualised environments:

34 The ITSEF shall confirm that the necessary dependencies for the TOE are listed.

35 The ITSEF shall confirm that the hardware and software configurations stated in the applicant's hardware and software specification for the TOE allow for proper operation of all security functions of the TOE.

36 The ITSEF shall confirm that the hardware and software required for the evaluation can be provided either by the ITSEF itself or by the applicant.

37 The ITSEF shall confirm that it will be able to set up the hardware and software required for the evaluation, with or without the support of the applicant.

38 The ITSEF shall confirm that the required role and authorisation model in the ST follows the requirements described in [AIS B1].

39 The ITSEF shall evaluate, if necessary, whether the content described in the compatibility description is adequately described.

40 The ITSEF shall evaluate, if necessary, whether the specified security measures in the SUG (Secure User Guidance) document for the secure operation of the TOE in the system environment are adequately present and described.

3.1.7 Estimate the evaluation effort and duration

41 The main objective of this part of the evaluation is to estimate the workload necessary for the evaluation of the TOE, a time schedule for the evaluation, and to ensure that the ITSEF is capable to perform the evaluation.

42 The ITSEF shall verify that they have the required knowledge, systems, tools and enough capacity to perform the evaluation. The ITSEF shall document any deficit in tools or knowledge and the date of availability. If the ITSEF lacks either tools or knowledge, they shall acquire them. This includes tools made available by the applicant.

43 The ITSEF shall ensure that it is in possession of any additional software, systems or cryptographic material required for the operation of the TOE. This equipment shall be provided by the applicant and the provision shall be organised by the ITSEF. The ITSEF shall inform the certification body when the TOE is expected to be operational. If necessary, the applicant may support the ITSEF in setting up the operational environment.

44 The ITSEF shall estimate the number of person days required to perform a BSZ evaluation and document it along with a rationale. It shall use [AIS-B5] as a guideline.
Note: Specifically, this is only the time needed for the evaluation of the TOE. This includes the time needed to document and analyse the evaluation results and to compile the ETR. However, this neither

includes the time needed for the preparation for the kick-off and final interview nor the time needed for project management.

45 The ITSEF shall review internal resources to provide an initial time frame of the evaluation, i.e. a mapping of the estimated person days to calendar days, taking into account personnel availability, estimated time of tool execution, dependencies in the evaluation (e.g. possible parallelization), time required for preparation by the applicant and internal (e.g. training) and other factors influencing the progress of the BSZ. The ITSEF shall document the estimated date of completion of the evaluation.

46 In case of a re-evaluation, the ITSEF determines the expected evaluation period in person days necessary to verify that the issues addressed in the previous ETR are no longer present, including areas noted for further investigation in the previous interview. This evaluation time shall include a sufficient amount of regression testing, depending on the size of the changes and the details given in the IAR, e.g. covering further relevant changes at the TOE since the last evaluation (Hardware and Software).

47 In case of a re-certification, the ITSEF determines the expected evaluation period in person days necessary to test all functions that are affected by updates and changes described in the IAR and further relevant changes at the TOE since the last evaluation (Hardware and Software). This evaluation time shall include a sufficient amount of regression testing, depending on the size of the changes and the details given in the IAR.

48 In case of a re-certification or re-evaluation, the ITSEF shall review the previously performed evaluation. It shall verify whether the tests performed are still up-to-date and valid, or if the tests need to be repeated, and whether additional testing or a new method of testing is necessary. In the latter case the ITSEF shall include this in the evaluation time frame.

3.2 Phase 2 – Step 1 The kick-off

49 The objective of the kick-off is to create a solid basis for the BSZ procedure. A common understanding of the TOE and ST shall be achieved. All parties, i.e. applicant, ITSEF, and BSI, shall agree that the TOE can be certified based on the ST. Possible obstacles for the evaluation and certification process need to be identified and addressed.

50 For software applications and applications in virtualised environments, the ITSEF shall submit a proposal for the test environment to the certification body before the kick-off meeting e.g. together with the presentation for the kick-off meeting. When applicable, the suggested test environment should have the lowest possible performance levels of the hardware specification. The proposal shall be based on the applicant's hardware and software specification for the TOE.

51 Following discussion, the evaluation plan shall be agreed and the time schedule shall be fixed.

3.2.1 Preparation

52 The ITSEF shall prepare a high level presentation on the TOE and the evaluation, following the template for the kick-off agenda [BSZ-ADA] The presentation shall contain all required output of Phase 1. In particular, it shall include an overview and discussion of the users, attackers, threats and assumptions and how they interact in the intended usage, whether the chosen configuration is a typical configuration of the TOE (significant market relevance) and how the proposed extent of the evaluation (person days) was derived. The presentation shall include the version of all scheme documents and templates to be used, including the ETR template. In case of a re-certification or re-evaluation, the presentation shall include those results of the previously performed evaluation that are still up-to-date and valid and will therefore be reused for the re-evaluation.

53 The ITSEF shall provide the BSI with a copy of the prepared presentation at least five business days before the kick-off [BSZ-ADA].

54 The ITSEF together with the applicant shall verify that the application of the developer for a BSZ procedure has been accepted at the BSI.

55 The ITSEF shall support the applicant and the BSI in agreeing on dates for sending in the presentation and the kick-off.

56 In case of a re-certification or re-evaluation, the preparation shall focus on the IAR and its analysis, including a rationale for the evaluation time frame.

3.2.2 Participation in the kick-off

57 The ITSEF shall attend the kick-off with at least one evaluator. The evaluator(s) shall be able to present and discuss the results from Phase 1 using the output of Phase 2, Step 1. The evaluator(s) present at the kick-off shall be able to discuss possible testing strategies intended for the TOE including the cryptography evaluation.

58 The evaluator(s) present at the kick-off shall confirm the version of all scheme documents and templates to be used, including the ETR template.

59 The evaluator(s) present at the kick-off shall confirm that the ITSEF is capable of evaluating this TOE. This includes the treatment of any risks regarding impartiality.

60 The evaluator(s) present at the kick-off shall be authorised to agree the number of person days required for this BSZ procedure, the time schedule for the evaluation, and a date for ETR submission.

61 If, as a result of the kick-off, necessary changes to the ST are identified and agreed, the evaluator(s) present at the kick-off shall be able and authorised to assess the impact of those changes, both on the time frame as well as on the preparation required for the evaluation.

3.2.2.1 Additional tasks for software applications and applications in virtualised environments

62 During the kick-off meeting, the ITSEF shall present that the proposed test environment is representative for the TOE with respect to the applicant's hardware and software specification for the TOE and appropriate for the planned evaluation methods.

63 If the certification body follows the proposal of the ITSEF, the proposed test environment shall be considered as defined and shall be noted in writing for the evaluation.

3.3 Phase 2 – Step 2 Evaluation

64 The objective of this phase is to examine the TOE and the corresponding documentation to enable the ITSEF to reach a well-founded verdict on the evaluation.

65 The evaluation consists of four parts (Section 3.3.1, Section 3.3.2, Section 3.3.3 and Section 3.3.4) that are dedicated to the examination and testing of the TOE and a fifth part (Section 3.3.5) for compiling the evaluation report. It is expected that the evaluation starts with the first part and ends with the fifth part, but otherwise the steps may be executed in any order, even in parallel.

66 During the evaluation, the test strategy should be adjusted depending on previous findings. Additionally, the performed tests, test strategy, course of action, and actual time required for testing should be documented in order to enable the ITSEF to compile the report, present the evaluation results in the interview in Phase 4 (Section 3.4), and if necessary to answer enquiries by the BSI.

67 The ITSEF shall reject any query by the applicant after the evaluation has started. If, however, the ITSEF identifies issues where additional information from the applicant might be helpful to avoid significant evaluation efforts, it shall contact the applicant for clarification. This exchange shall be recorded in the ETR. At no time shall the ITSEF accept new versions of the TOE, any mandatory evidence or provide the applicant with intermediate results.

68 If the ITSEF identifies security relevant issues, which might be relevant for an entire group of products, possibly even from other vendors or critical issues for this product it shall inform BSI to discuss further actions.
Example
A vendor uses an unmodified version of a (wider used) library and the ITSEF finds a security vulnerability.

69 In case of a re-certification or re-evaluation, the evaluation shall be executed adapted to the changes according to the IAR. If no changes to the cryptography were required and the tests from the previous evaluation are still up-to-date, Part 4 (Section 3.3.4) may be omitted. The evaluators shall ensure that Part 3 (Section 3.3.3) includes the determination where the changes introduced new vulnerabilities.

3.3.1 Evaluation of the TOE installation

70 The main objective of this part of the evaluation is to verify that the TOE can be set up as described in the SUG. It implements the evaluation task “Evaluation of TOE Installation” from [FiT CEM] (6.6).

71 The ITSEF shall execute work unit 2 of Section 6.6 [FiT CEM] (6.6.4.2). The requirements for the SUG are defined in [AIS-B3]

72 The ITSEF shall execute work unit 1 of Section 6.6 [FiT CEM] (6.6.4.1).

73 The ITSEF shall execute work unit 3 of Section 6.6. [FiT CEM] (6.6.4.3)

74 If the TOE is **not** in the expected state, then the ITSEF shall use its general expert knowledge and the remaining information (besides the SUG) to set up the TOE in the state described in the ST. The ITSEF shall document the additional (or changed) steps compared to the SUG.

3.3.2 Conformance testing

75 The main objective of this part of the evaluation is to verify that the TOE provides the claimed security functions, is conformant to claimed standards and fulfils the requirements for the TOE in the scope in effect, e.g., [AIS-B6]. It implements the evaluation task “Conformance testing” from [FiT CEM] (6.7).

76 The ITSEF shall execute work unit 1 of Section 6.7 [FiT CEM] (6.7.4.1). For this, the ITSEF shall set up a test strategy covering all security functions described in the ST and all requirements for the TOE in the scope in effect, e.g., [AIS-B6]. The ITSEF shall take the time allocated for this step in account. Testing depth and effort may vary for each security function and requirement for the TOE.
The acceptance criteria from Annex C [FiT CEM] are not implemented in the BSZ.

77 The ITSEF shall execute work unit 2 of Section 6.7 [Fit CEM] (6.7.4.2).

78 The ITSEF shall execute work unit 3 of Section 6.7 [FiT CEM] (6.7.4.3).

79 The test 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.

80 The ITSEF shall ensure that the evaluator(s) who are present at the interview in Phase 4 (Section 3.4) are capable of explaining and justifying the test strategy and its updates, and if applicable, the rationale for allocating more time for this step.

81 If nonconformities, notable deviations from best practices, missing functions or items in the documentation (cf. paragraph 63) are detected, they shall be documented in the ETR (Section 3.3.5)

3.3.2.1 Additional tasks for software applications and applications in virtualised environments

82 The ITSEF shall evaluate that the chosen test environment conforms to the hardware and software specification for the TOE. If a compatibility description exists, then sample based tests shall be performed on a representative set of heterogeneous hardware.

83 The ITSEF shall evaluate the conformity for the specific set-up of the system environment that is necessary for the TOE to perform its security functionality. The set-up measures shall be formally evaluated on suitability for use and on proper function. The measures are considered to be formally robust if no security risks are known. The proper security functionality is achieved if no additional weakness exists after the configuration.

84 The ITSEF shall evaluate the conformity for the configuration of the TOE according to the Secure User Guidance (SUG). For this purpose, the ITSEF shall evaluate whether the TOE fulfils its self-provided security functions in the system environment after set-up in accordance with the SUG, or whether requirements are provided in the SUG that could compromise the security of the system environment..

3.3.3 Penetration testing

85 The main objective of this part of the evaluation is to determine that the TOE does not contain vulnerabilities that could be exploited by attackers. The considered attack potential corresponds to “Enhanced Basic” level and if the calculated value is 13 and below the attack is deemed possible, see [FiT CEM] (Annex F).

86 It implements the evaluation task “Penetration testing” from [FiT CEM] (6.10).

87 The ITSEF shall execute work unit 1 of Section 6.10 [FiT CEM] (6.10.4.1).

88 The ITSEF shall sufficiently evaluate the update mechanism.

89 If the TOE includes components developed by third parties that may have common vulnerabilities and exposures and no adequate optional vulnerability report was provided before, the ITSEF shall demand a detailed list of the vulnerabilities and exposures concerned and a detailed description or evidence from the developer about how the vulnerabilities and exposures are addressed or mitigated.

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

91 The ITSEF shall ensure that the evaluator(s) who are present at the interview (see Phase 4 below) are capable of explaining and justifying the test strategy, its updates and the sampling strategy used to search for publicly known vulnerabilities. If applicable, they shall be able to explain the rationale for allocating more time for this step.

92 The ITSEF shall execute work unit 2 of Section 6.10 [FiT CEM] (6.10.4.2).

93 If potential vulnerabilities or other notable deviations from best practices are found, they shall be documented in the ETR (Section 3.3.5).

94 If the applicant supplied modified versions of the TOE or additional information, e.g. a TOE with unencrypted firmware or source code, the ITSEF shall ensure that the (partial) vulnerability is also present in the unmodified TOE.

95 The ITSEF shall analyse the findings (cf. paragraph 87) of the evaluation considering possible attack paths based on the threat model of the ST. If a potential vulnerability is considered a residual vulnerability that will not hinder a positive verdict, the ITSEF shall estimate the quantum of resources an attacker would need to bypass or break the security functions. The estimate shall result in a score according to the principles used in Appendix F [FiT CEM] in conjunction with the table F.1 in the document.

96 The analysis of the findings shall be documented in the ETR. The ITSEF shall ensure that the evaluator(s) who are present at the interview (Section 3.4.2) are capable of explaining and justifying the analysis and its results.

97 If relevant for the TOE, the ITSEF shall determine if the TOE introduces vulnerabilities on its environment. If vulnerabilities are found the ITSEF shall analyse them, taking into account possible attack paths, based on the threat model of the ST.

3.3.3.1 Additional tasks for software applications and applications in virtualised environments

98 The ITSEF shall examine whether the role and authorisation concept is appropriate to protect the interfaces to the system environment from possible compromise.

99 The ITSEF shall analyse whether the TOE, after hardening and installation in accordance with the SUG protects against unauthorised access by other applications or users.

3.3.4 Evaluation of cryptographic functions

100 The main objective of this part of the evaluation is to verify that the TOE implements the claimed cryptographic mechanisms and protocols correctly and is conformant to claimed and required standards. It implements the evaluation task “Extended crypto analysis” from [FiT CEM] (6.12).

101 The ITSEF shall evaluate the cryptographic functions according to [AIS-B2].

102 The ITSEF shall ensure that the evaluator(s) who are present at the interview (Section 3.4.2) are capable of explaining and justifying the test strategy and its updates, and, where applicable, the rationale for allocating more or less time for this step.

103 If nonconformities, vulnerabilities or notable deviations from best practices are found, they shall be documented in the ETR (Section 3.3.5)

104 If insufficiencies in the cryptographic functions are found, they shall be treated as described in Step 3 (cf. paragraphs 90 and 91 for details).

3.3.5 Preparation of the evaluation report

105 The evaluation report shall follow the latest version of the ETR template as provided by the BSI before the kick-off.

106 The report shall include as a minimum:

- The identification of the TOE and its version, a description of the test environment used by the ITSEF and reference to the analysed documents
- A brief summary of the evaluation strategy and the evaluation tasks performed
- A documentation (cf. paragraphs 76, 87, and 97) and analysis (cf. paragraph 89) of all findings
- A documentation and analysis of all vulnerabilities introduced by the TOE on its environment, if any

107 The ITSEF shall describe each nonconformity, vulnerability, missing function or item in sufficient detail so that other security experts are able to reproduce it.

108 If there is a complete attack path for the TOE, the verdict is a Fail. If there are irregularities, insufficiencies or notable deviations from best practices in the implemented algorithms, cryptography, principles or in the underlying properties or nonconformities, that do not lead to a complete attack path, the ITSEF shall propose a verdict for the evaluation and a rationale for the verdict.

109 The ITSEF shall verify that the agreed evaluation time (number of days) has been fully used. The ITSEF shall include a table that contains all evaluation tasks, the time originally planned for the task, and the time actually spent. This includes the time for documentation and the compiling of the ETR.

110 The ITSEF shall verify that no pending results from Step 1 to Step 4 are remaining. If any pending evaluation step is identified, it shall be completed, even if this implies that the total number of days is exceeded.

111 If deemed necessary in Step 1 (cf. paragraph 60), the ITSEF shall document the information necessary for the correct secure configuration in the ETR and the applicant shall complement important steps in the SUG.

112 In the case of a re-certification or re-evaluation, the ETR shall refer to the ETR of the initial evaluation where necessary and appropriate. This should cover the focus of the re-evaluation (taking into account the IAR and issue list) and briefly describe what has already been tested in the previous evaluation and why these previous results are reusable and still valid.

113 The ITSEF shall assign an evaluator who has not written the ETR to review the ETR both for formal compliance with the scheme requirements and for obviously incorrect conclusions or missing content.

114 The responsible project manager or head of the ITSEF and the quality management representative of the ITSEF shall sign the ETR using a specific wording as given in [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ Evaluierungsprozess, BSZ-EP, BSI, cf. Section 3.1 paragraph 9.

115 The ITSEF shall send the encrypted ETR to bsz@bsi.bund.de.
Note: The encryption policies are stated in the [BSZ-Prod], cf. Section 5.2.

116 The ITSEF shall update the ETR based on the comments received from the BSI. All comments shall be answered. In some evaluations, this may require additional testing (e.g. from Step 1 – 4). All changes shall be clearly marked in the revised documents.

117 The ITSEF shall not disclose any results, including parts of the ETR, to the applicant in this phase.

3.4 Phase 2 – Step 3 Final interview

118 The objective of this phase is to review the evaluation performed by the ITSEF and to determine a final verdict on the TOE.

119 As a rule, the interview between the certification body and the ITSEF shall take place at one of the BSI offices. The office shall be determined by the BSI.

3.4.1 Preparation

120 After submission of the ETR, the ITSEF shall contact the BSI to arrange an appointment for the interview.

121 The ITSEF shall prepare a high level presentation on the evaluation. The presentation shall contain:

- All required output ("results") from phase 2 – Step 2(sec 3.3)
- A description of the relevant tests and tools (not only their name)
- The test strategy chosen and its development over the course of the evaluation
- The personnel involved (with a brief rationale)

- An overview of what was considered but not done (with some rationale)
- If potential vulnerabilities are found during step 3 and 4, the rating following Appendix F [FiT CEM]
- The overall verdict of the results with a rationale

122 The ITSEF shall select evaluator(s) who are able to explain and defend the entire evaluation (including the cryptographic part), the test strategy, the distribution of the allocated time, the selection of evaluators and the rating of the results.

123 Unless otherwise agreed, the ITSEF shall provide the BSI with a copy of the prepared presentation at least five business days before the interview.

3.4.2 Interview

124 The evaluator(s) present at the interview shall be able to present and defend the results from Phase 3, guided by the presentation prepared for the interview. The evaluator(s) shall be able to access additional information (this might include contacting other evaluators or accessing detailed logs made during the evaluation) to answer questions which may arise during the interview. Where possible, these logs shall be on the presentation machine of the evaluator(s) at the interview.

125 The evaluator(s) present at the interview shall record all open and unresolved issues and present them to the BSI at the end of the interview.

126 The ITSEF shall document the results of the interview in a protocol and send the encrypted protocol to bsz@bsi.bund.de
Note: The encryption policies are stated in the [BSZ-Prod], cf. Section 5.2.

3.4.3 Addendum

127 If necessary, the ITSEF shall perform an additional evaluation based on the open and unresolved issues from the interview and update the ETR accordingly. For this, they may follow the applicable requirements of Phase 3 (Section 3.3).

128 The ITSEF shall send the encrypted final ETR to bsz@bsi.bund.de.
Note: The encryption policies are stated in the [BSZ-Prod], cf. Section 5.2.

129 After BSI has acknowledged the receipt of the ETR, the ITSEF may inform the applicant on the results and any other details. In any event, the ITSEF shall provide the developer with a copy of the ETR.

130 Immediately after acceptance of the ETR by the certification body, the ITSEF shall send a signed version to the applicant and to the BSI (see [BSZ-EP], cf. Sections 2.5 and 3.1).

131 The ITSEF shall ensure that all relevant information on this BSZ evaluation is archived according to the requirements of the BSI scheme.

132 If problems are identified which could affect future evaluations (e.g. in terms of tools, test strategy, evaluator qualification), the ITSEF shall ensure that these are recorded and, if necessary, appropriate measures are taken from the next procedure onwards.

4 Definitions

See definitions in Chapter 3 in [FiT CEM].

5 Reference documents

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