Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B4, Version 2.0

Datum:	01.03.2024
Status:	Verbindlich
Thema:	Anforderungen an die Evaluierung gemäß BSZ
Herausgeber:	Zertifizierungsstelle des BSI
Verteiler:	Anerkannte BSZ-Prüfstellen (ITSEFs) [1] BSI-intern Webseite des BSI

[1]Alle Evaluatoren in den vom BSI für Prüfungen im Rahmen der BSZ anerkannten Prüfstellen.

Änderungshistorie

Version	*Datum*	*Herausgeber*	*Beschreibung*
2.0	01.03.2024	SZ 33	Deutsche Erstausgabe

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: bsz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Hintergrund

1 In diesem Dokument wird detailliert beschrieben, wie eine BSZ-Evaluierung durchgeführt werden muss. Der Inhalt dieses Dokuments ist für jede BSZ-Prüfstelle für IT-Sicherheit (kurz Prüfstelle) und jede BSZ-Evaluierung verbindlich.

2 Es umfasst sowohl die BSZ-Erstevaluierung als auch die Rezertifizierung oder Reevaluierung.

3 Spezifische Geltungsbereiche der BSZ umfassen zusätzliche Aufgaben für die BSZ-Evaluierung oder verfeinern die in diesem Dokument festgelegten Aufgaben. Die Dokumente der spezifischen Geltungsbereiche enthalten die zusätzlichen oder modifizierten Anforderungen für die BSZ-Evaluierung.

2 Spezifische Referenzen

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] Anforderungen an ST und IAR, BSI

5 [AIS-B2] Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ, BSI

6 [AIS-B3] Anforderungen an die Benutzeranleitung, BSI

7 [AIS-B5] Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung, BSI

8 [AIS-B6] Anforderungen an einen TOE, BSI

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

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

3 Anwendungshinweise und Interpretationen

3.1 Phase 1 – Vorbereitung auf eine BSZ

3 Das Ziel dieser Phase besteht darin, sicherzustellen, dass die Prüfstelle den TOE ordnungsgemäß evaluieren kann.

4 Diese Phase wird am besten vor Antragstellung auf ein BSZ-Verfahren durchgeführt. Die Antragstellerin hat somit noch die Möglichkeit, Probleme in ihren Dokumentationsunterlagen zu beseitigen und kann verifizieren, ob die Prüfstelle über die Werkzeuge, Kenntnisse und Kapazitäten zur Durchführung der Evaluierung verfügt.

5 Sollte die Prüfstelle zur Durchführung der Evaluierung zusätzliche Werkzeuge und Kenntnisse beschaffen müssen, sollte dies vor der Auftaktbesprechung in Phase 2 (Abschnitt 3.2) getan werden.

3.1.1 Vollständigkeitsprüfung

6 Das Hauptziel dieses Teils der Evaluierung ist die Verifizierung, dass alle erforderlichen Dokumente und Elemente verfügbar sind. Hierbei wird die Evaluierungsaufgabe "Vollständigkeitsprüfung" gemäß [FiT CEM] (6.1) umgesetzt.

7 Die Prüfstelle muss bestimmen, in welchen BSZ-Geltungsbereich der TOE fällt und die zusätzlichen Aufgaben sowie die verfeinerten Aufgaben in den festgelegten Schritten der Evaluierung durchführen.

8 Die Prüfstelle muss die Workunit 1 aus Abschnitt 6.1 [FiT CEM] (6.1.4.1) ausführen. Der Prüfstelle muss Folgendes vorgelegt werden:

- Das Dokument der Sicherheitsvorgaben (Englisch: Security Target, ST)
- Ein kurzer Überblick über den grundsätzlichen Aufbau des TOE
- Eine Softwarestückliste (Englisch: Software Bill of Materials, SBOM)
- Eine kurze technische Beschreibung des Update-Mechanismus
- Ein Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance, SUG)
- Eine Erklärung und Begründung zur Konformität des TOE zu den für den TOE geltungsbereichsspezifischen Anforderungen, bspw. [AIS-B6]
- Die für den Betrieb des TOE notwendigen Komponenten der Betriebsumgebung

9 Falls es sich beim TOE um ein eingebettetes System handelt, sind die folgenden zusätzlichen Eingaben erforderlich:

- Falls nicht anders im spezifischen Geltungsbereich festgelegt, 3 Exemplare des TOE (einschließlich der typischen Benutzerdokumentation und Handbücher)
- Eine Kopie der unverschlüsselten Firmware

10 Falls es sich beim TOE um eine Softwareanwendung oder eine virtualisierte Anwendung handelt, sind die folgenden zusätzlichen Eingaben erforderlich:

- Installationspaket der Anwendung
- Spezifikation der Hardware
- Spezifikation der Software
- Beschreibung der Abhängigkeiten

- Kompatibilitätsbeschreibung (falls erforderlich)

11 Die Prüfstelle muss prüfen, dass alle zusätzlichen Eingaben vorliegen, die für den spezifischen Geltungsbereich erforderlich sind.

12 Die Prüfstelle muss Workunit 3 aus Abschnitt 6.1 [FiT CEM] (6.1.4.3)[2] ausführen. Die Eingaben zur Evaluierung der kryptographischen Mechanismen werden in [AIS-B2] beschrieben.

13 Im Falle einer Rezertifizierung oder Reevaluierung muss die Prüfstelle überprüfen, dass der Impact Analysis Report (IAR) vorliegt.

14 Die Prüfstelle muss Workunit 2 aus Abschnitt 6.1 [FiT CEM] (6.1.4.2) ausführen. Die Prüfstelle kann wählen, diese Workunit später auszuführen. Dies muss jedoch vor Phase 2, Schritt 2 Evaluierung abgeschlossen werden.

3.1.2 Evaluierung der Sicherheitsvorgaben (Evaluierung des Security Targets)

15 Das Hauptziel dieses Teils der Evaluierung besteht in der Verifikation, dass das Dokument Sicherheitsvorgaben (ST) als Grundlage für eine BSZ geeignet ist. Hierbei wird die Evaluierungsaufgabe "FiT Security Target Evaluierung" gemäß [FiT CEM] (6.4) umgesetzt.

16 Die Prüfstelle muss Workunit 1a aus Abschnitt 6.4 [FiT CEM] (6.4.4.1) ausführen.
Die strukturellen Anforderungen an das ST sind in [AIS-B1] festgelegt. Für diese Workunit bedeutet relevante Sicherheitsfunktion, dass die Sicherheitsfunktionen zur Abwehr von Bedrohungen auf die Werte (Englisch: Assets) geeignet sind, sich jede Sicherheitsfunktion auf mindestens eine Bedrohung bezieht und die Annahmen sinnvoll und relevant sind.
Die Anforderungen und Empfehlungen bezüglich der kryptographischen Algorithmen sind in [AIS-B2] festgelegt.

17 Die Prüfstelle muss bestätigen, dass der TOE im ST eindeutig und verständlich für den Leser mit einer Versionsnummer identifiziert ist (keine Platzhalter oder pauschale Aussagen).

18 Die Prüfstelle muss bestätigen, dass das ST im Hinblick auf den beabsichtigten Anwendungsfall nicht irreführend ist.

19 Die Prüfstelle muss bestätigen, dass unter Berücksichtigung der verbleibenden mit dem TOE bereitgestellten Dokumentation die Liste der Werte vollständig ist.

20 Die Prüfstelle muss überprüfen, dass die Liste der Schnittstellen des TOE im ST vollständig ist und alle Schnittstellen korrekt benannt sind.

21 Die Prüfstelle muss auf Grundlage der von der Antragstellerin vorgelegten Unterlagen verifizieren, dass der dort beschriebene TOE mit dem tatsächlichen TOE im spezifischen Geltungsbereich konform ist, z. B. [AIS-B6].

22 Die Prüfstelle muss verifizieren, dass die im ST angegebenen Sicherheitsfunktionen testbar sind.

3.1.3 Überprüfung der Dokumentation für kryptographische Funktionen

23 Das Hauptziel dieses Teils der Evaluierung besteht in der Verifizierung der Vollständigkeit der Dokumentation der kryptographischen Mechanismen und in der Erstellung eines ersten Plans für die Kryptoanalyse.

24 Falls dies nicht bereits in früheren Schritten erfolgt ist, muss die Prüfstelle verifizieren, dass die kryptographische Spezifikation alle im ST beschriebenen Sicherheitsfunktionen, Dienste und Schnittstellen abdeckt, die kryptographische Mechanismen verwenden.

[2] Die in der Workunit 1 [FiT CEM] (6.1.4.3) verwendete Bezeichnung „White Box Kryptographie“ bezieht sich auf eine White Box Evaluierung der kryptographischen Implementation.

25 Die Prüfstelle muss die angegebene Kryptographie überprüfen und gemäß [AIS-B2] einen groben Plan für die Kryptoanalyse erstellen. Dieser Plan soll die beabsichtigte Stichprobenstrategie darlegen.

3.1.4 Überprüfung der Softwarestückliste (SBOM)

26 Das Ziel dieses Teils der Evaluierung besteht in der Verifizierung der Vollständigkeit und Konformität der SBOM zu den in [AIS-B1], Kapitel 6 beschriebenen Anforderungen.

27 Die Prüfstelle muss überprüfen, dass alle Einträge in der SBOM plausibel sind, insbesondere bezüglich der in den anderen TOE-Dokumenten bereitgestellten Aussagen und Informationen.

28 Die Prüfstelle muss alle potenziellen Unstimmigkeiten dokumentieren, die sie identifiziert hat und in der Auftaktbesprechung zu klären wünscht.

3.1.5 Evaluierung des Impact Analysis Reports

29 Im Falle einer Rezertifizierung oder Reevaluierung muss die Prüfstelle bestätigen, dass der Impact Analysis Report (IAR) den in [AIS-B1] beschriebenen Anforderungen entspricht.

30 Im Falle einer Reevaluierung muss die Prüfstelle überprüfen, dass der IAR alle im vorherigen Prüfbericht (ETR) identifizierten Probleme in ausreichender Detailtiefe anspricht, um eine effiziente erneute Evaluierung zu ermöglichen. Falls dies nicht der Fall ist, muss die Prüfstelle die Antragstellerin darauf hinweisen, dass der Mangel an Details durch einen höheren Evaluierungsaufwand kompensiert wird.

31 Die Prüfstelle muss alle potenziellen Probleme dokumentieren, die sie identifiziert hat und in der Auftaktbesprechung zu klären wünscht.

32 Die Prüfstelle muss überprüfen, ob für dieses BSZ-Verfahren Risiken für die Unparteilichkeit bestehen. Falls solche Risiken identifiziert werden, muss die Prüfstelle dokumentieren, wie sie diese Risiken handhabt.

33 Falls eine der oben genannten Anforderungen nicht erfüllt wird, muss die Prüfstelle das Versäumnis der Antragstellerin melden und eine Aktualisierung des ST oder die entsprechend fehlenden TOE(s) oder Dokumentation anfordern. Die Prüfstelle darf keine Beratung anbieten, wie das Versäumnis behoben werden kann.

3.1.6 Zusätzliche Aufgaben für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

34 Die Prüfstelle muss bestätigen, dass die für den TOE notwendigen Abhängigkeiten aufgeführt sind.

35 Die Prüfstelle muss bestätigen, dass die in der Hardware- und Softwarespezifikation der Antragstellerin für den TOE angegebenen Hardware- und Softwarekonfigurationen eine ordnungsgemäße Funktion aller Sicherheitsfunktionen des TOE ermöglichen.

36 Die Prüfstelle muss bestätigen, dass die für die Evaluierung erforderliche Hardware und Software entweder von der Prüfstelle selbst oder von der Antragstellerin bereitgestellt werden kann.

37 Die Prüfstelle muss bestätigen, dass sie in der Lage sein wird, die für die Evaluierung erforderliche Hardware und Software einzurichten, mit oder ohne Unterstützung der Antragstellerin.

38 Die Prüfstelle muss bestätigen, dass das im ST beschriebene erforderliche Rollen- und Berechtigungsmodell den in [AIS B1] beschriebenen Anforderungen entspricht.

39 Die Prüfstelle muss gegebenenfalls bewerten, ob die in der Kompatibilitätsbeschreibung ausgeführten Inhalte angemessen beschrieben sind.

40 Die Prüfstelle muss gegebenenfalls evaluieren, ob die im Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance, SUG) spezifizierten Sicherheitsmaßnahmen für den sicheren Betrieb des TOE in der Systemumgebung angemessen vorhanden und beschrieben sind.

3.1.7 Schätzung von Evaluierungsaufwand und -dauer

41 Das Ziel dieses Teils der Evaluierung besteht in der Schätzung des für die Evaluierung erforderlichen Arbeitsaufwands, der Zeitplanung für die Evaluierung und der Sicherstellung, dass die Prüfstelle zur Durchführung der Evaluierung in der Lage ist.

42 Die Prüfstelle muss verifizieren, dass sie über das erforderliche Wissen, die erforderlichen Systeme, Werkzeuge und über ausreichende Kapazität verfügt, um die Evaluierung durchzuführen. Die Prüfstelle muss etwaige Defizite bei Werkzeugen oder Kenntnisse sowie das Datum der Verfügbarkeit dokumentieren. Wenn der Prüfstelle Werkzeuge oder Kenntnisse fehlen, muss sie diese akquirieren. Dies inkludiert auch von der Antragstellerin bereitgestellte Werkzeuge.

43 Die Prüfstelle muss sicherstellen, dass sie im Besitz aller zusätzlicher Software, Systeme oder kryptografischen Materialien ist, die für den Betrieb des TOE erforderlich sind. Diese Ausrüstung muss von der Antragstellerin bereitgestellt und die Bereitstellung muss von der Prüfstelle auf Vollständigkeit kontrolliert werden. Die Prüfstelle muss die Zertifizierungsstelle darüber informieren, wann der TOE voraussichtlich betriebsbereit sein wird. Falls erforderlich, kann die Antragstellerin die Prüfstelle bei der Einrichtung der Betriebsumgebung unterstützen.

44 Die Prüfstelle muss die Anzahl der für die Durchführung der Evaluierung erforderlichen Personentage schätzen und dies zusammen mit einer Begründung dokumentieren. Dabei muss [AIS-B5] als Richtlinie verwendet werden.

Hinweis: Dies bezieht sich speziell nur auf die Zeit, die für die Evaluierung des TOE benötigt wird. Hierbei ist die Zeit für die Dokumentation und Analyse der Evaluierungsergebnisse und die Erstellung des ETR enthalten. Es sind jedoch weder die Zeit für die Vorbereitung der Auftaktbesprechung und des Abschlussinterviews noch die Zeit für das Projektmanagement inkludiert.

45 Die Prüfstelle muss ihre internen Ressourcen prüfen, um einen ersten Zeitrahmen für die Evaluierung bereitzustellen, d. h. eine Zuordnung der geschätzten Personentage zu Kalendertagen unter Berücksichtigung der Verfügbarkeit des Personals, der geschätzten Zeit für die Ausführung der Testprogramme, der Abhängigkeiten in der Evaluierung (z. B. mögliche Parallelisierung), der für die Vorbereitung durch die Antragstellerin benötigten Zeit sowie internen (z. B. Schulungen) und anderen Faktoren, die den Fortschritt der BSZ beeinflussen. Die Prüfstelle muss das voraussichtliche Abschlussdatum der Evaluierung dokumentieren.

46 Im Falle einer Reevaluierung bestimmt die Prüfstelle den erwarteten Evaluierungszeitraum in Personentagen, der erforderlich ist, um zu verifizieren, dass die in dem vorherigen ETR adressierten Probleme nicht mehr vorhanden sind. Das schließt Bereiche ein, die in dem vorherigen Abschlussinterview für weitere Untersuchungen vermerkt wurden. Diese Evaluierungszeit muss eine ausreichende Menge an Regressionstests beinhalten, abhängig vom Umfang der Änderungen und den Details im IAR, z. B. um weitere relevante Änderungen am TOE seit der letzten Evaluierung (Hardware und Software) abzudecken.

47 Im Falle einer Rezertifizierung bestimmt die Prüfstelle den erwarteten Evaluierungszeitraum in Personentagen, der erforderlich ist, um alle Funktionen zu testen, die von im IAR beschriebenen Updates und Änderungen sowie von weiteren relevanten Änderungen am TOE seit der letzten Evaluierung (Hardware und Software) betroffen sind. Diese Evaluierungszeit muss eine ausreichende Menge an Regressionstests enthalten, abhängig vom Umfang der Änderungen und den Details im IAR.

48 Im Falle einer Rezertifizierung oder einer Reevaluierung muss die Prüfstelle die zuvor durchgeführte Evaluierung überprüfen. Sie muss verifizieren, ob die durchgeführten Tests noch aktuell und gültig sind oder ob die Tests wiederholt werden müssen, und ob zusätzliche Tests oder eine neue Testmethode erforderlich sind. In letzterem Fall muss die Prüfstelle dies in den Zeitrahmen der Evaluierung aufnehmen.

3.2 Phase 2 – Schritt 1: Die Auftaktbesprechung

49 Ziel der Auftaktbesprechung ist es, eine belastbare Grundlage für das BSZ-Verfahren zu schaffen. Es soll ein gemeinsames Verständnis vom TOE und des ST erreicht werden. Alle Parteien, d. h. die Antragstellerin, die Prüfstelle und das BSI, müssen darin übereinstimmen, dass der TOE auf Grundlage des ST zertifiziert werden kann. Mögliche Hindernisse für den Evaluierungs- und Zertifizierungsprozess müssen identifiziert und beseitigt werden.

50 Für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen muss die Prüfstelle vor der Auftaktbesprechung einen Vorschlag für die Testumgebung bei der Zertifizierungsstelle einreichen, z. B. zusammen mit der Präsentation für die Auftaktbesprechung. Sofern anwendbar, soll die vorgeschlagene Testumgebung der niedrigsten Leistungsstufe der Hardware-Spezifikation entsprechen. Der Vorschlag muss auf der Hardware- und Softwarespezifikation der Antragstellerin für den TOE basieren.

51 Nach der Erörterung müssen der Evaluierungsplan vereinbart und der Zeitplan festgelegt werden.

3.2.1 Vorbereitung

52 Die Prüfstelle muss eine Überblickspräsentation zum TOE und der Evaluierung erstellen und sich dabei an die Vorlage für die Agenda der Auftaktbesprechung [BSZ-ADA] halten. Die Präsentation muss alle erforderlichen Ergebnisse der Phase 1 enthalten. Insbesondere muss darin ein Überblick und eine Erörterung zu den Nutzern, Angreifern, Bedrohungen und Annahmen und deren Interaktionen im Rahmen der beabsichtigten Verwendung sowie zu den Fragen enthalten sein, ob die gewählte Konfiguration eine typische Konfiguration des TOE ist (wesentliche Marktrelevanz) und wie der vorgeschlagene Umfang der Evaluierung (Personentage) davon abgeleitet wurde. Die Präsentation muss die Version aller zu verwendenden Schemadokumente und Vorlagen einschließlich der ETR-Vorlage enthalten. Im Falle einer Rezertifizierung oder Reevaluierung müssen die Ergebnisse der zuvor durchgeführten Evaluierung, die noch aktuell und gültig sind und daher im Rahmen der Reevaluierung wiederverwendet werden, in die Präsentation aufgenommen werden.

53 Die Prüfstelle stellt dem BSI spätestens 5 Werktage vor der Auftaktbesprechung eine Kopie der vorbereiteten Präsentation für die Auftaktbesprechung zur Verfügung.

54 Die Prüfstelle muss gemeinsam mit der Antragstellerin verifizieren, dass der Antrag auf ein BSZ-Verfahren beim BSI angenommen wurde.

55 Die Prüfstelle muss die Antragstellerin und das BSI bei der Vereinbarung von Terminen für die Einsendung der Präsentation und die Auftaktveranstaltung unterstützen.

56 Im Falle einer Rezertifizierung oder Reevaluierung muss das Hauptaugenmerk bei der Vorbereitung auf dem IAR und seiner Analyse liegen, einschließlich der Begründung für den Zeitrahmen der Evaluierung.

3.2.2 Teilnahme an der Auftaktbesprechung

57 Die Prüfstelle muss mit mindestens einem Evaluator oder einer Evaluatorin an der Auftaktbesprechung teilnehmen. Der oder die Evaluatoren müssen in der Lage sein, die Ergebnisse aus Phase 1 anhand der Ergebnisse von Phase 2, Schritt 1 zu präsentieren und zu erörtern. Die bei

der Auftaktbesprechung anwesenden Evaluatorinnen und Evaluatoren müssen in der Lage sein, mögliche Teststrategien für den TOE einschließlich der kryptographischen Evaluierung zu besprechen.

58 Die bei der Auftaktbesprechung anwesenden Evaluatorinnen und Evaluatoren bestätigen die Version aller zu verwendenden Schemadokumente und Vorlagen, einschließlich der ETR-Vorlage.

59 Die bei der Auftaktbesprechung anwesenden Evaluatorinnen und Evaluatoren bestätigen, dass die Prüfstelle in der Lage ist, den entsprechenden TOE zu bewerten. Dazu gehört auch die Auseinandersetzung mit etwaigen Risiken der Unparteilichkeit.

60 Die bei der Auftaktbesprechung anwesenden Evaluatorinnen und Evaluatoren müssen befugt sein, die Anzahl der für dieses BSZ-Verfahren erforderlichen Personentage, den Zeitplan für die Evaluierung und einen Termin für die ETR-Einreichung zu vereinbaren.

61 Wenn infolge der Auftaktbesprechung notwendige Änderungen am ST festgestellt und vereinbart werden, müssen die bei der Auftaktbesprechung anwesenden Evaluatorinnen und Evaluatoren in der Lage und befugt sein, die Auswirkungen dieser Änderungen auf den Zeitrahmen sowie auf die für die Evaluierung erforderliche Vorbereitung zu beurteilen.

3.2.2.1 Zusätzliche Aufgaben für Softwareanwendungen und Anwendung in virtualisierten Umgebungen

62 Während der Auftaktbesprechung muss die Prüfstelle zeigen, dass die vorgeschlagene Testumgebung hinsichtlich der Hardware- und Softwarespezifikation der Antragstellerin für den TOE repräsentativ und für die geplanten Evaluierungsmethoden geeignet ist.

63 Wenn die Zertifizierungsstelle dem Vorschlag der Prüfstelle folgt, gilt die vorgeschlagene Testumgebung als festgelegt und muss schriftlich für die Evaluierung festgehalten werden.

3.3 Phase 2 – Schritt 2: Die Evaluierung

64 Ziel dieser Phase ist, den TOE und die zugehörigen Dokumentationsunterlagen zu prüfen, damit die Prüfstelle ein fundiertes Urteil im Rahmen der Evaluierung fällen kann.

65 Die Phase setzt sich aus vier Teilen zusammen (Unterabschnitt 3.3.1, Unterabschnitt 3.3.2, Unterabschnitt 3.3.3 und Unterabschnitt 3.3.4), die die Untersuchung und Prüfung des TOE zum Inhalt haben, sowie einem fünften Teil (Unterabschnitt 3.3.5) zur Erstellung des Evaluierungsreports. Die Evaluierung sollte mit Teil 1 beginnen und mit Teil 5 enden, abgesehen davon können die Schritte in beliebiger Reihenfolge und auch parallel ausgeführt werden.

66 Im Rahmen der Evaluierung sollte die Teststrategie abhängig von den bisherigen Ergebnissen angepasst werden. Darüber hinaus sollten die durchgeführten Prüfungen, die Teststrategie, die Vorgehensweise und die tatsächlich für die Prüfungen erforderliche Zeit dokumentiert werden, damit die Prüfstelle in der Lage ist, den Bericht zu erstellen, die Evaluierungsergebnisse im Rahmen des Gesprächs in Phase 4 (Abschnitt 3.4) vorzulegen und bei Bedarf Anfragen des BSI zu beantworten.

67 Die Prüfstelle muss jede Anfrage der Antragstellerin nach Beginn der Evaluierung ablehnen. Sollte die Prüfstelle jedoch Probleme feststellen, bei denen zusätzliche Informationen der Antragstellerin hilfreich sein könnten um einen erheblichen Evaluierungsaufwand zu vermeiden, muss die Prüfstelle die Antragstellerin zur Klärung kontaktieren. Dieser Austausch muss im ETR vermerkt werden. Die Prüfstelle darf zu keinem Zeitpunkt neue Versionen des TOE oder obligatorische Nachweise akzeptieren oder der Antragstellerin Zwischenergebnisse zur Verfügung stellen.

68 Sollten von der Prüfstelle sicherheitsrelevante Probleme, die für eine ganze Produktgruppe (möglicherweise auch anderer Anbieter) von Bedeutung sein könnten, oder kritische Probleme für das betreffende Produkt festgestellt werden, muss sie das BSI informieren, um anschließend das

weitere Vorgehen zu besprechen.
Beispiel:
Ein Anbieter verwendet eine unveränderte Version einer (weit verbreiteten) Bibliothek und die Prüfstelle entdeckt eine Sicherheitslücke.

69 Im Falle einer Rezertifizierung oder Reevaluierung muss die Evaluierung an die Änderungen gemäß dem IAR angepasst werden. Für den Fall, dass an der Kryptographie keine Änderungen erforderlich waren und die Prüfungen aus der vorherigen Evaluierung weiterhin aktuell sind, kann Teil 4 (Unterabschnitt 3.3.4) entfallen. Die Evaluatoren müssen sicherstellen, dass in Teil 3 (Unterabschnitt 3.3.3) bestimmt wird, durch welche Änderungen neue Schwachstellen entstanden sind.

3.3.1 Evaluierung der TOE-Installation

70 Das Ziel dieses Teils der Evaluierung besteht in der Verifizierung, dass der TOE wie im SUG beschrieben eingerichtet werden kann. Dies implementiert die Evaluierungsaufgabe "Evaluierung der TOE-Installation" aus [FiT CEM] (6.6).

71 Die Prüfstelle muss Workunit 2 von Abschnitt 6.6 [FiT CEM] (6.6.4.2) ausführen. Die Anforderungen für den SUG sind in [AIS-B3] definiert.

72 Die Prüfstelle muss Workunit 1 von Abschnitt 6.6 [FiT CEM] (6.6.4.1) ausführen.

73 Die Prüfstelle muss Workunit 3 von Abschnitt 6.6 [FiT CEM] (6.6.4.3) ausführen.

74 Wenn der TOE **nicht** im erwarteten Zustand ist, muss die Prüfstelle ihr allgemeines Fachwissen und die verbleibenden Informationen (abseits des SUG) nutzen, um den TOE gemäß dem im ST beschriebenen Zustand einzurichten. Die Prüfstelle muss die zusätzlichen (oder geänderten) Schritte im Vergleich zum SUG dokumentieren.

3.3.2 Konformitätsprüfung

75 Das Ziel dieses Teils der Evaluierung besteht in der Verifizierung, dass der TOE die angegebenen Sicherheitsfunktionen bereitstellt, den angegebenen Standards entspricht und die Anforderungen für den TOE im wirksamen Geltungsbereich erfüllt, z. B. [AIS-B6]. Dies implementiert die Evaluierungsaufgabe "Konformitätsprüfung" aus [FiT CEM] (6.7).

76 Die Prüfstelle muss Workunit 1 von Abschnitt 6.7 [FiT CEM] (6.7.4.1) ausführen. Dafür muss die Prüfstelle eine Teststrategie entwickeln, die alle im ST beschriebenen Sicherheitsfunktionen und alle Anforderungen für den TOE im spezifischen Geltungsbereich abdeckt, z. B. [AIS-B6]. Die Prüfstelle muss die für diesen Schritt zugewiesene Zeit berücksichtigen. Testtiefe und Aufwand können für jede Sicherheitsfunktion und Anforderung für den TOE variieren. Die Akzeptanzkriterien aus Anhang C [FiT CEM] werden in der BSZ nicht umgesetzt.

77 Die Prüfstelle muss Workunit 2 von Abschnitt 6.7 [FiT CEM] (6.7.4.2) ausführen.

78 Die Prüfstelle muss Workunit 3 von Abschnitt 6.7 [FiT CEM] (6.7.4.3) ausführen.

79 Die Teststrategie muss fortlaufend aktualisiert werden, insbesondere wenn Ergebnisse (einschließlich der Ergebnisse aus den anderen Schritten) verfügbar werden. Sollte für diesen Schritt mehr Zeit benötigt werden als ursprünglich vorgesehen, muss die Prüfstelle dies dokumentieren und entsprechend begründen.

80 Die Prüfstelle stellt sicher, dass der bzw. die beim Gespräch in Phase 4 (Abschnitt 3.4) anwesende(n) Evaluator(en) in der Lage ist bzw. sind, die Teststrategie und ihre Aktualisierungen zu erläutern und zu begründen und gegebenenfalls die Gründe für die Bereitstellung von zusätzlicher Zeit für diesen Schritt anzugeben.

81 Bei Feststellung von Nichtkonformitäten, auffälligen Abweichungen von Best Practices, fehlenden Funktionen oder Punkten in den Dokumentationsunterlagen (vgl. Abs. 63) müssen diese im ETR (Unterabschnitt 3.3.5) dokumentiert werden.

3.3.2.1 Zusätzliche Aufgaben für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

82 Die Prüfstelle muss evaluieren, dass die gewählte Testumgebung mit der Hardware- und Software-Spezifikation für den TOE übereinstimmt. Falls eine Kompatibilitätsbeschreibung vorhanden ist, sollten Stichprobenprüfungen an einem repräsentativen Satz heterogener Hardware durchgeführt werden.

83 Die Prüfstelle muss die Konformität für die spezifische Einrichtung der Systemumgebung evaluieren, die für den TOE zur Ausführung seiner Sicherheitsfunktionen erforderlich ist. Die Einrichtungsmaßnahmen müssen formal auf ihre Eignung zur Verwendung und auf ordnungsgemäße Funktion hin evaluiert werden. Die Maßnahmen gelten als formal robust, wenn keine Sicherheitsrisiken bekannt sind. Die ordnungsgemäße Sicherheitsfunktionalität wird erreicht, wenn nach der Konfiguration keine zusätzliche Schwachstelle existiert.

84 Die Prüfstelle muss die Konformität der Konfiguration des TOE gemäß des Handbuches zur sicheren Benutzung (SUG) evaluieren. Zu diesem Zweck muss die Prüfstelle evaluieren, ob der TOE nach der Einrichtung gemäß des SUG seine selbst bereitgestellten Sicherheitsfunktionen in der Systemumgebung erfüllt oder ob Anforderungen in der SUG bereitgestellt werden, die die Sicherheit der Systemumgebung gefährden könnten.

3.3.3 Penetrationstests

85 Das Ziel dieses Teils der Evaluierung besteht in der Bestimmung, ob der TOE von Angreifern ausnutzbare Schwachstellen enthält. Das betrachtete Angriffspotenzial entspricht dem „erweitert einfach“-Niveau (englisch „enhanced-basic“) und wenn der berechnete Wert 13 oder weniger beträgt, gilt der Angriff als möglich, siehe [FiT CEM] (Anhang F).

86 Dies implementiert die Evaluierungsaufgabe "Penetrationstests" aus [FiT CEM] (6.10).

87 Die Prüfstelle muss Workunit 1 von Abschnitt 6.10 [FiT CEM] (6.10.4.1) ausführen.

88 Die Prüfstelle muss den Update-Mechanismus ausreichend bewerten.

89 Sollten im TOE Komponenten enthalten sein, die von Dritten entwickelt wurden und möglicherweise häufige Sicherheitsrisiken und Sicherheitslücken (Englisch: Common Vulnerabilities and Exposures, CVE) aufweisen, für die zuvor kein adäquater optionaler Schwachstellenbericht bereitgestellt worden ist, muss die Prüfstelle eine detaillierte Liste der betreffenden Schwachstellen und Sicherheitsrisiken sowie eine detaillierte Beschreibung oder einen Nachweis vom Entwickler darüber verlangen, wie die Schwachstellen und Sicherheitsrisiken beseitigt oder gemindert werden.

90 Die Teststrategie muss fortlaufend aktualisiert werden, insbesondere, wenn Ergebnisse (einschließlich der Ergebnisse aus den anderen Schritten) verfügbar werden. Sollte für diesen Schritt mehr Zeit benötigt werden als ursprünglich vorgesehen, muss die Prüfstelle dies dokumentieren und entsprechend begründen.

91 Die Prüfstelle stellt sicher, dass der bzw. die beim Gespräch (siehe Phase 4 unten) anwesende(n) Evaluator(en) bzw. Evaluatorin(nen) in der Lage ist bzw. sind, die Teststrategie, ihre Aktualisierungen und die Stichprobenstrategie zur Suche nach öffentlich bekannten Schwachstellen zu erläutern und zu begründen. Gegebenenfalls müssen sie in der Lage sein, die Gründe für die Einräumung von zusätzlicher Zeit für diesen Schritt zu erläutern.

92 Die Prüfstelle muss Workunit 2 von Abschnitt 6.20 [Fit CEM] (6.10.4.2) ausführen.

93 Werden potenzielle Schwachstellen oder andere auffällige Abweichungen von Best Practices festgestellt, müssen diese im ETR (Unterabschnitt 3.3.5) dokumentiert werden.

94 Sollte die Antragstellerin geänderte Versionen des TOE oder zusätzliche Informationen vorlegen, z. B. einen TOE mit unverschlüsselter Firmware oder unverschlüsseltem Quellcode, muss die Prüfstelle sicherstellen, dass die Schwachstelle (oder der Teil einer Schwachstelle) auch im unveränderten TOE vorhanden ist.

95 Die Prüfstelle muss die Befunde (vgl. Abs. 73) der Evaluierung unter Berücksichtigung möglicher Angriffspfade auf Basis des Bedrohungsmodells des ST analysieren. Wenn eine potenzielle Schwachstelle als residuale Schwachstelle betrachtet wird, die einem positiven Urteil nicht im Wege steht, muss die Prüfstelle die Ressourcenmenge abschätzen, die ein Angreifer benötigen würde, um die Sicherheitsfunktionen zu umgehen oder zu durchbrechen. Aus der Schätzung ergibt sich eine Punktzahl gemäß den Grundsätzen im Anhang F [Fit CEM] in Verbindung mit der Tabelle F.1 [Fit CEM]

96 Die Analyse der Ergebnisse muss im ETR dokumentiert werden. Die Prüfstelle stellt sicher, dass der bzw. die beim Gespräch anwesende(n) Evaluator(en) (Unterabschnitt 3.4.2) in der Lage ist bzw. sind, die Analyse und ihre Ergebnisse zu erläutern und zu begründen.

97 Sofern dies für den TOE relevant ist, muss die Prüfstelle bestimmen, ob der TOE Schwachstellen in seiner Umgebung verursacht. Für den Fall, dass Schwachstellen gefunden werden, muss die Prüfstelle diese unter Berücksichtigung möglicher Angriffspfade auf Basis des Bedrohungsmodells des ST analysieren.

3.3.3.1 Zusätzliche Aufgaben für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

98 Die Prüfstelle muss überprüfen, ob das Rollen- und Autorisierungskonzept geeignet ist, um die Schnittstellen zur Systemumgebung vor möglichen Kompromittierungen zu schützen.

99 Die Prüfstelle muss analysieren, ob der TOE nach der Härtung und Installation gemäß des SUG vor unbefugtem Zugriff durch andere Anwendungen oder Benutzer schützt.

3.3.4 Evaluierung kryptographischer Funktionen

100 Das Ziel dieses Teils der Evaluierung ist die Verifizierung, dass der TOE die angegebenen kryptografischen Mechanismen und Protokolle korrekt implementiert und den angegebenen und geforderten Standards entspricht. Dies implementiert die Bewertungsaufgabe "Erweiterte Kryptoanalyse" gemäß [FiT CEM] (6.12).

101 Die Prüfstelle muss die kryptographischen Funktionen gemäß [AIS-B2] evaluieren.

102 Die Prüfstelle muss sicherstellen, dass der bzw. die beim Gespräch (Unterabschnitt 3.4.2) anwesende(n) Evaluator(en) bzw. Evaluatorin(nen) in der Lage ist bzw. sind, die Teststrategie und ihre Aktualisierungen zu erläutern und zu begründen und gegebenenfalls die Gründe für die Allokation von mehr oder weniger Zeit für diesen Schritt anzugeben.

103 Werden Nichtkonformitäten, Schwachstellen oder auffällige Abweichungen von Best Practices festgestellt, müssen diese im ETR (Unterabschnitt 3.3.5) dokumentiert werden.

104 Sollten in den kryptographischen Funktionen Unzulänglichkeiten festgestellt werden, müssen diese gemäß den Angaben in Schritt 3 (siehe Absatz 90 und 91 für weitere Informationen) behandelt werden.

3.3.5 Erstellung des Evaluierungsreports

105 Der Evaluierungsreport muss sich an der neuesten Version der ETR-Vorlage orientieren, die das BSI vor der Auftaktbesprechung veröffentlicht hat.

106 Der Bericht muss mindestens Folgendes enthalten:

- Die Identifizierung des TOE und seiner Version, eine Beschreibung der von der Prüfstelle verwendeten Testumgebung und eine Referenz auf die analysierten Dokumente.
- Eine kurze Zusammenfassung der Evaluierungsstrategie und der durchgeführten Evaluierungsaufgaben.
- Die Dokumentationsunterlagen (vgl. Abs. 76, 87 und 97) und die Analyse (vgl. Abs. 89) aller Erkenntnisse.
- Die Dokumentationsunterlagen und die Analyse aller vom TOE in seiner Umgebung eingeführten Schwachstellen, sofern zutreffend.

107 Die Prüfstelle beschreibt jede Nichtkonformität, Schwachstelle, fehlende Funktion oder jedes Element so detailliert, dass andere Sicherheitsexperten sie reproduzieren können.

108 Bei Vorliegen eines vollständigen Angriffspfades für den TOE lautet das Urteil „Nicht bestanden“. Treten in den implementierten Algorithmen, der Kryptographie, den Prinzipien oder in den zugrunde liegenden Eigenschaften oder Nichtkonformitäten Unregelmäßigkeiten, Unzulänglichkeiten oder auffällige Abweichungen von Best Practices auf, die nicht zu einem vollständigen Angriffspfad führen, empfiehlt die Prüfstelle ein Urteil für die Evaluierung und eine Begründung für das Urteil.

109 Die Prüfstelle verifiziert, ob die vereinbarte Evaluierungszeit (Anzahl der Tage) vollständig genutzt wurde. Die Prüfstelle stellt eine Tabelle bereit, die alle Evaluierungsaufgaben, die ursprünglich für die Aufgabe vorgesehene Zeit und die tatsächlich aufgewendete Zeit enthält. Darin enthalten ist die Zeit für die Dokumentation und die Erstellung des ETR.

110 Die Prüfstelle verifiziert, dass keine Ergebnisse aus den Schritten 1–4 ausstehend sind. Sollte ein noch ausstehender Evaluierungsschritt festgestellt werden, muss dieser abgeschlossen werden, auch wenn dies zur Folge hat, dass die Gesamtzahl der Tage überschritten wird.

111 Sofern in Schritt 1 (vgl. Abs. 60) als notwendig erachtet, dokumentiert die Prüfstelle die für die korrekte sichere Konfiguration erforderlichen Informationen im ETR und die Antragstellerin ergänzt wichtige Schritte im SUG.

112 Im Falle einer Rezertifizierung oder Reevaluierung bezieht sich der ETR, soweit erforderlich und angemessen, auf den ETR der Erstevaluierung. Dieser sollte den Schwerpunkt der Reevaluierung abdecken (unter Berücksichtigung des IAR und der Problemliste) und kurz beschreiben, was in der vorherigen Evaluierung bereits geprüft wurde und warum diese bereits vorliegenden Ergebnisse wiederverwendbar und weiterhin gültig sind.

113 Die Prüfstelle beauftragt einen Evaluator, der den ETR nicht verfasst hat, damit, den ETR sowohl auf formelle Einhaltung der Schema-Anforderungen als auch auf offensichtlich falsche Schlussfolgerungen oder fehlende Inhalte zu prüfen.

114 Der verantwortliche Projektleiter bzw. Leiter der Prüfstelle und der Qualitätsmanagementbeauftragte der Prüfstelle unterzeichnen den ETR unter Verwendung eines bestimmten Wortlauts gemäß [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ Evaluierungsprozess, BSZ-EP, BSI, vgl. Abschnitt 3.1 Abs. 9.

115 Die Prüfstelle sendet den verschlüsselten ETR an bsz@bsi.bund.de.
Hinweis: Die Verschlüsselungsrichtlinien sind im [BSZ-Prod] angegeben, vgl. Abschnitt 5.2.

116 Die Prüfstelle aktualisiert den ETR auf Grundlage der vom BSI erhaltenen Kommentare. Auf alle Kommentare muss eingegangen werden. Bei einigen Evaluierungen kann dies zusätzliche Prüfungen erfordern (z. B. aus den Schritten 1–4). Alle Änderungen müssen in den überarbeiteten Dokumenten deutlich gekennzeichnet sein.

117 Die Prüfstelle darf in dieser Phase gegenüber der Antragstellerin keine Ergebnisse, einschließlich Teile des ETR, offenlegen.

3.4 Phase 2 – Schritt 3: Abschlussinterview

118 Ziel dieser Phase besteht darin, die von der Prüfstelle durchgeführte Evaluierung zu bewerten und ein endgültiges Urteil über den TOE zu fällen.

119 Das Gespräch zwischen der Zertifizierungsstelle und der Prüfstelle findet in der Regel in einer der BSI-Geschäftsstellen statt. Die Geschäftsstelle muss vom BSI bestimmt werden.

3.4.1 Vorbereitung

120 Nach Übermittlung des ETR kontaktiert die Prüfstelle das BSI, um einen Termin für das Gespräch zu vereinbaren.

121 Die Prüfstelle erstellt eine Überblickspräsentation zur Evaluierung. Die Präsentation muss Folgendes enthalten:

- Alle erforderlichen Ergebnisse aus Phase 2, Schritt 2 (Abschnitt 3.3)
- Eine Beschreibung der relevanten Prüfungen und Werkzeuge (nicht nur deren Name)
- Die gewählte Teststrategie und deren Weiterentwicklung im Verlauf der Evaluierung
- Das beteiligte Personal (mit einer kurzen Begründung)
- Ein Überblick darüber, was zwar in Erwägung gezogen, aber letztlich nicht unternommen wurde (mit einer Begründung)
- Für den Fall, dass im Rahmen der Schritte 3 und 4 potenzielle Schwachstellen gefunden wurden, die Bewertung nach Anhang F [FiT CEM]
- Das Gesamturteil der Ergebnisse einschließlich einer Begründung

122 Die Prüfstelle muss einen oder mehrere Evaluator(en) bzw. Evaluatorin(nen) auswählen, der bzw. die in der Lage ist/sind, die gesamte Evaluierung (einschließlich des kryptographischen Teils), die Teststrategie, die Verteilung der zugewiesenen Zeiten, die Auswahl der Evaluatoren und die Bewertung der Ergebnisse zu erläutern und zu verteidigen.

123 Sofern nicht anders vereinbart, muss die Prüfstelle dem BSI mindestens 5 Werktage vor dem Gespräch eine Kopie der vorbereiteten Präsentation vorlegen.

3.4.2 Interview

124 Der bzw. die beim Gespräch anwesende(n) Evaluator(en) bzw. Evaluatorin(nen) muss bzw. müssen in der Lage sein, die Ergebnisse aus Phase 3 anhand der für das Gespräch vorbereiteten Präsentation zu präsentieren und zu verteidigen. Der bzw. die Evaluator(en) bzw. Evaluatorin(nen) muss bzw. müssen auf zusätzliche Informationen zugreifen können (dazu kann die Kontaktaufnahme zu anderen Evaluatoren oder der Zugriff auf detaillierte Protokolle gehören, die während der Evaluierung erstellt wurden), um Fragen zu beantworten, die während des Gesprächs auftreten können. Soweit möglich, müssen diese Protokolle während des Gesprächs auf dem Präsentationsgerät des Evaluators bzw. der Evaluatoren gespeichert sein.

125 Der bzw. die beim Gespräch anwesende(n) Evaluator(en) bzw. Evaluatorin(nen) muss bzw. müssen alle offenen und ungeklärten Fragen auf und legt (legen) diese am Ende des Gesprächs dem BSI vornehmen.

126 Die Prüfstelle muss die Ergebnisse des Gesprächs in einem Bericht dokumentieren und den verschlüsselten Bericht an bsz@bsi.bund.de senden.

Hinweis: Die Verschlüsselungsrichtlinien sind im [BSZ-Prod] angegeben, vgl. Abschnitt 5.2.

3.4.3 Nachtrag

127 Bei Bedarf muss die Prüfstelle eine zusätzliche Evaluierung auf Grundlage der offenen und ungelösten Fragen aus dem Gespräch durchführen und den ETR entsprechend aktualisieren. Hierzu kann sie sich an die geltenden Anforderungen aus Phase 3 (Abschnitt 3.3) halten.

128 Die Prüfstelle muss den verschlüsselten finalen ETR an bsz@bsi.bund.de übermitteln.

Hinweis: Die Verschlüsselungsrichtlinien sind im [BSZ-Prod] angegeben, vgl. Abschnitt 5.2.

129 Nachdem das BSI den Erhalt des ETR bestätigt hat, kann die Prüfstelle die Antragstellerin über die Ergebnisse und weitere Einzelheiten informieren. In jedem Fall muss die Prüfstelle dem Entwickler eine Kopie des ETR zur Verfügung stellen.

130 Unmittelbar nach Abnahme des ETR durch die Zertifizierungsstelle muss die Prüfstelle eine unterzeichnete Version an die Antragstellerin und an das BSI (siehe [BSZ-EP], vgl. Abschnitte 2.5 und 3.1) senden.

131 Die Prüfstelle muss sicherstellen, dass alle relevanten Informationen zu dieser BSZ-Evaluierung gemäß den Anforderungen des BSI-Schemas archiviert werden.

132 Bei Feststellung von Problemen, die Auswirkungen auf künftige Evaluierungen haben könnten (z. B. hinsichtlich Werkzeuge, Teststrategie, Evaluatorenqualifikation), muss die Prüfstelle sicherstellen, dass diese erfasst werden und gegebenenfalls ab dem darauffolgenden Verfahren entsprechende Maßnahmen ergriffen werden.

4 Definitionen

1 Vgl. Definitionen in Kapitel 3 in [Fit `CEM].

5 Referenzdokumente

1 [FiT CEM] Fixed-time cybersecurity evaluation methodology for ICT products (FiT CEM), EN 17640:2022 bzw.
Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte; Deutsche Fassung EN 17640:2022