

DIN EN 17640

ICS 35.030

**Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für
IKT-Produkte;
Deutsche Fassung EN 17640:2022**

Fixed-time cybersecurity evaluation methodology for ICT products;
German version EN 17640:2022

Méthode d'évaluation de la cybersécurité pour produits TIC;
Version allemande EN 17640:2022

Gesamtumfang 60 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 17640:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-04-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 62443-4-1:2018	siehe	DIN EN IEC 62443-4-1:2018-10
ISO 62443-4-2:2019	siehe	DIN EN IEC 62443-4-2:2019-12

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN IEC 62443-4-1:2018-10, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1:2018); Deutsche Fassung EN IEC 62443-4-1:2018*

DIN EN IEC 62443-4-2:2019-12, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019*

Deutsche Fassung

Zeitlich festgelegte
Cybersicherheitsevaluationsmethodologie für
IKT-Produkte

Fixed-time cybersecurity evaluation methodology for
ICT products

Méthode d'évaluation de la cybersécurité pour
produits TIC

Diese Europäische Norm wurde vom CEN am 15. August 2022 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

	Seite
Europäisches Vorwort	5
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Konformität	10
5 Allgemeine Konzepte	13
5.1 Anwendung dieser Methodologie	13
5.2 Wissen über den TOE	13
5.3 Evaluierung des Entwicklungsprozesses	13
5.4 Angriffspotential	14
5.5 Aufbau von Wissen	14
6 Evaluierungsaufgaben	15
6.1 Vollständigkeitsprüfung	15
6.1.1 Ziel	15
6.1.2 Evaluierungsmethode	15
6.1.3 Kompetenz des Evaluators	15
6.1.4 Workunits der Evaluatoren	15
6.2 Evaluierung des FIT-Schutzprofils	15
6.2.1 Ziel	15
6.2.2 Evaluierungsmethode	16
6.2.3 Kompetenz des Evaluators	16
6.2.4 Workunits der Evaluatoren	16
6.3 Überprüfung der Sicherheitsfunktionalitäten	17
6.3.1 Ziel	17
6.3.2 Evaluierungsmethode	17
6.3.3 Kompetenz des Evaluators	17
6.3.4 Workunits der Evaluatoren	17
6.4 Evaluierung der FIT-Sicherheitsvorgabe	17
6.4.1 Ziel	17
6.4.2 Evaluierungsmethode	18
6.4.3 Kompetenz des Evaluators	18
6.4.4 Workunits der Evaluatoren	18
6.5 Entwicklungsdokumentation	19
6.5.1 Ziel	19
6.5.2 Evaluierungsmethode	19
6.5.3 Kompetenz des Evaluators	19
6.5.4 Workunits	20
6.6 Evaluierung der TOE-Installation	20
6.6.1 Ziel	20
6.6.2 Evaluierungsmethode	20
6.6.3 Kompetenz des Evaluators	20
6.6.4 Workunits der Evaluatoren	20
6.7 Konformitätsprüfung	21
6.7.1 Ziel	21

6.7.2	Evaluierungsmethode.....	21
6.7.3	Kompetenz des Evaluators.....	21
6.7.4	Workunits der Evaluatoren.....	21
6.8	Schwachstellenprüfung.....	23
6.8.1	Ziel	23
6.8.2	Evaluierungsmethode.....	23
6.8.3	Kompetenz des Evaluators.....	23
6.8.4	Workunits der Evaluatoren.....	24
6.9	Erweiterte Schwachstellenprüfung	24
6.9.1	Ziel	24
6.9.2	Evaluierungsmethode.....	25
6.9.3	Kompetenz des Evaluators.....	25
6.9.4	Workunits der Evaluatoren.....	25
6.10	Penetrationsprüfung.....	27
6.10.1	Ziel	27
6.10.2	Evaluierungsmethode.....	27
6.10.3	Kompetenz des Evaluators.....	28
6.10.4	Workunits der Evaluatoren.....	28
6.11	Grundlegende Kryptoanalyse	29
6.11.1	Ziel	29
6.11.2	Evaluierungsmethode.....	29
6.11.3	Kompetenz des Evaluators.....	30
6.11.4	Workunits der Evaluatoren.....	30
6.12	Erweiterte Kryptoanalyse	31
6.12.1	Ziel	31
6.12.2	Evaluierungsmethode.....	31
6.12.3	Kompetenz des Evaluators.....	31
6.12.4	Workunits der Evaluatoren.....	31
Anhang A (informativ) Beispiel für die Struktur einer FIT-Sicherheitsvorgabe (FIT-ST).....		34
A.1	Allgemeines	34
A.2	Beispiel für die Struktur	34
A.3	Typische Inhalte einer FIT-ST.....	35
Anhang B (normativ) Das Konzept eines FIT-Schutzprofils (FIT-PP)		36
B.1	Allgemeines	36
B.2	Ziel und Grundlagen eines FIT-PP	36
B.3	Anleitung für Schemata zur Implementierung des FIT-PP-Konzepts	36
Anhang C (informativ) Annahmekriterien.....		37
C.1	Einleitung	37
C.2	Identifizierung, Authentifizierungskontrolle und Zugriffskontrolle.....	37
C.3	Sicherer Systemstart (Secure Boot).....	40
C.4	Kryptographie	40
C.5	Sicherer Zustand nach Ausfall	41
C.6	Geringste Funktionalität.....	43
C.7	Aktualisierungsmechanismus	43
Anhang D (informativ) Anleitung für die Integration der Methodologie in ein Schema.....		45
D.1	Allgemeines	45
D.1.1	Einleitung	45
D.1.2	Durchführen einer Risikobeurteilung, Überprüfung der zu betrachtenden vertikalen Domäne	45
D.1.3	Zuordnen des Angriffspotentials zu den CSA-Vertrauenswürdigkeitsstufen	45
D.1.4	Auswählen der für diese CSA-Vertrauenswürdigkeitsstufe erforderlichen Evaluierungsaufgaben	45
D.1.5	Überprüfen und Festlegen der Parameter für die Arbeitsaufgaben	45

D.1.6	Mögliche Auswahl von zusätzlichen oder höherwertigen Arbeitsaufgaben.....	46
D.1.7	Überprüfen und Festlegen der Parameter für die zusätzlichen Arbeitsaufgaben.....	46
D.1.8	Erstellen und Pflegen weiterer Schemaanforderungen und -leitlinien	46
D.2	Beispiel.....	47
Anhang E (informativ) Parameter der Methodologie und der Evaluierungsaufgaben.....		50
E.1	Allgemeines	50
E.2	Parameter der Methodologie	50
E.3	Parameter der Evaluierungsaufgaben.....	50
E.3.1	Parameter für 6.1 „Vollständigkeitsprüfung“	50
E.3.2	Parameter für 6.2 „Evaluierung des FIT-Schutzprofils“	50
E.3.3	Parameter für 6.3 „Überprüfung der Sicherheitsfunktionalitäten“	50
E.3.4	Parameter für 6.4 „Evaluierung der Sicherheitsvorgabe“	50
E.3.5	Parameter für 6.5 „Entwicklungsdokumentation“	50
E.3.6	Parameter für 6.6 „Evaluierung der TOE-Installation“	51
E.3.7	Parameter für 6.7 „Konformitätsprüfung“	51
E.3.8	Parameter für 6.8 „Schwachstellenprüfung“	51
E.3.9	Parameter für 6.9 „Erweiterte Schwachstellenprüfung“	51
E.3.10	Parameter für 6.10 „Penetrationsprüfung“	51
E.3.11	Parameter für 6.11 „Grundlegende Kryptoanalyse“	51
E.3.12	Parameter für 6.12 „Erweiterte Kryptoanalyse“	51
Anhang F (normativ) Berechnung des Angriffspotentials.....		52
F.1	Allgemeines	52
F.2	Faktoren für das Angriffspotential	52
F.3	Numerische Faktoren für das Angriffspotential	52
F.3.1	Allgemeines	52
F.3.2	Standardbewertungstabelle	53
F.3.3	Anpassung der Bewertungstabelle	54
Anhang G (normativ) Berichterstattung über die Ergebnisse einer Evaluierung		56
G.1	Allgemeines	56
G.2	Schriftliche Berichterstattung	56
G.3	Mündliche Verteidigung der erzielten Ergebnisse.....	56
Literaturhinweise.....		58

Europäisches Vorwort

Dieses Dokument (EN 17640:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2023, und etwaige entgegenstehende nationale Normen müssen bis April 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die Grundlage für eine fundierte Produktzertifizierung ist eine zuverlässige, transparente und wiederholbare Evaluationsmethodologie. Es gibt mehrere produkt- oder systemabhängige Evaluationsmethodologien. Der Rechtsakt zur Cybersicherheit (CSA, en: Cybersecurity Act) [1] wird zur Schaffung neuer Schemata führen, die wiederum (neue) Methodologien zur Evaluierung der Cybersicherheitsfunktionalitäten von Produkten erfordern. Diese neuen Methodologien werden benötigt, um die im CSA definierten Evaluierungsaufgaben zu beschreiben. Diese Methodologie fügt auch ein Konzept hinzu, das unabhängig von den Anforderungen der CSA ist, nämlich die Evaluierung innerhalb einer festen Zeit. Bestehende Evaluationsmethodologien zur Cybersicherheit (z. B. EN ISO/IEC 15408 in Kombination mit EN ISO/IEC 18045) sind nicht ausdrücklich zum Einsatz innerhalb einer festen Zeit ausgelegt.

Schemaentwickler werden ermutigt, die Evaluationsmethodologie in ihren Schemata umzusetzen. Dies kann bei Schemata für allgemeine Zwecke oder bei speziellen (vertikalen) Schemata durch die Auswahl von Aspekten für die Selbstbewertung auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“ oder für Bewertungen durch Dritte geschehen. Die Selbstbewertung darf auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“, die Drittparteien-Evaluierungen dürfen auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“, „mittel“ oder „hoch“ durchgeführt werden. Und die Evaluierungskriterien sowie die Methodologie unterliegen möglicherweise einer zusätzlichen Anpassung je nach den Anforderungen des einzelnen Schemas. Diese Evaluationsmethodologie für die Cybersicherheit deckt alle diese Anforderungen ab. Diese Methodologie wurde so gestaltet, dass sie an die Anforderungen des jeweiligen Schemas angepasst werden kann (und muss).

Schemaentwickler werden ermutigt, die Evaluationsmethodologie für den vorgesehenen Verwendungszweck des Schemas umzusetzen, die für allgemeine Zwecke oder in speziellen (vertikalen) Domänen anwendbar ist, indem sie die Aspekte auswählen, die für die Selbstbewertung auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“ oder die Drittparteien-Evaluierung auf jeder vom Schema geforderten CSA-Vertrauenswürdigkeitsstufe erforderlich sind.

Dieses Dokument enthält das Mindestmaß an Evaluierungsaufgaben, die im CSA definiert sind, um die gewünschte CSA-Vertrauenswürdigkeitsstufe zu erreichen, sowie optionale Arbeitsaufgaben, die im Rahmen des Schemas erforderlich sein könnten. Die Auswahl der verschiedenen optionalen Arbeitsaufgaben wird von Leitlinien begleitet, damit die Schemaentwickler die Auswirkungen ihrer Entscheidungen abschätzen können. Eine weitere Anpassung an die Risikosituation im Schema kann durch die Auswahl der verschiedenen in der Methodologie definierten Evaluierungsaufgaben oder durch die Verwendung der Parameter der Evaluierungsaufgaben, z. B. die Anzahl der Tage für die Durchführung bestimmter Arbeitsaufgaben, erreicht werden.

Wenn Schemaentwickler Arbeitsaufgaben wählen, die nicht in dieser Evaluationsmethodologie definiert sind, liegt es in der Verantwortung des Schemaentwicklers, eine Reihe begleitender Anforderungen zu definieren oder eine anwendbare Evaluationsmethodologie wiederzuverwenden.

Nichtsdestotrotz wird erwartet, dass die einzelnen Schemata die allgemeinen Anforderungen, die in dieser Evaluationsmethodologie dargelegt sind, instanziiieren und den Herstellern (und allen anderen Parteien) umfassende Leitlinien zu den konkreten Anforderungen, die innerhalb des Schemas zu erfüllen sind, geben.

Evaluatoren, Prüfer und Zertifizierer können diese Methodologie verwenden, um die Beurteilung, Prüfung oder Evaluierung der Produkte durchzuführen und die eigentliche Evaluierung/Zertifizierung nach den von einem bestimmten Schema aufgestellten Anforderungen durchzuführen. Es sind auch Anforderungen an den Qualifikations- und Wissensstand der Evaluatoren enthalten, und daher wird das Schema auch von **Akkreditierungsstellen** oder **nationalen Zertifizierungsstellen für Cybersicherheit** bei der Akkreditierung oder ggf. Befugniserteilung und Überwachung von Konformitätsbewertungsstellen verwendet.

Hersteller und **Entwickler** finden die allgemeine Art von Nachweisen, die für jede Evaluierungsaufgabe erforderlich sind, in der Evaluationsmethodologie aufgeführt, um sich auf die Beurteilung oder Bewertung vorzubereiten. Die Nachweis- und Evaluierungsaufgaben sind unabhängig davon, ob die Evaluierung durch den Hersteller/Entwickler (d. h. Erstpartei) oder durch eine andere Person (Zweit-/Drittpartei) durchgeführt wird.

Benutzer von zertifizierten Produkten (Regulierungsbehörden, Benutzerverbände, Regierungen, Unternehmen, Verbraucher usw.) dürfen dieses Dokument ebenfalls nutzen, um sich über die Vertrauenswürdigkeit zu informieren, die sich aus bestimmten Zertifikaten ergibt, die diese Bewertungsmethode verwenden. Auch hier wird erwartet, dass die Schemaentwickler zusätzliche, auf die Domäne des Schemas zugeschnittene Informationen über die durch Evaluierungen/Beurteilungen nach dieser Methodologie gewonnene Vertrauenswürdigkeit bereitstellen.

Darüber hinaus ist diese Methodologie dazu gedacht, Schemaentwickler in die Lage zu versetzen, Schemata zu erstellen, die versuchen, den Aufwand für den Hersteller so weit wie möglich zu reduzieren (was einen zusätzlichen Aufwand für das Prüflabor und die Zertifizierungsstelle bedeutet).

ANMERKUNG In diesem Dokument wird der Begriff „Konformitätsbewertungsstelle“ (KBS) für KBS, die die Evaluierung durchführen, verwendet. Andere mögliche Rollen für KBS werden in diesem Dokument nicht berücksichtigt.

Es sollte beachtet werden, dass dieses Dokument nicht „eigenständig“ verwendet werden kann. Jede Domäne (Schema) muss domänenspezifische Cybersicherheitsanforderungen („technische Spezifikationen“) für die zu evaluierenden/zertifizierenden Objekte bereitstellen. Diese Methodologie ist dazu gedacht, in Verbindung mit den betreffenden technischen Spezifikationen verwendet zu werden, die solche Cybersicherheitsanforderungen enthalten. Die Beziehung zwischen der in diesem Dokument dargestellten Methodologie und den Aufgaben in der Produktkonformitätsbewertung ist in Bild 1 dargestellt.

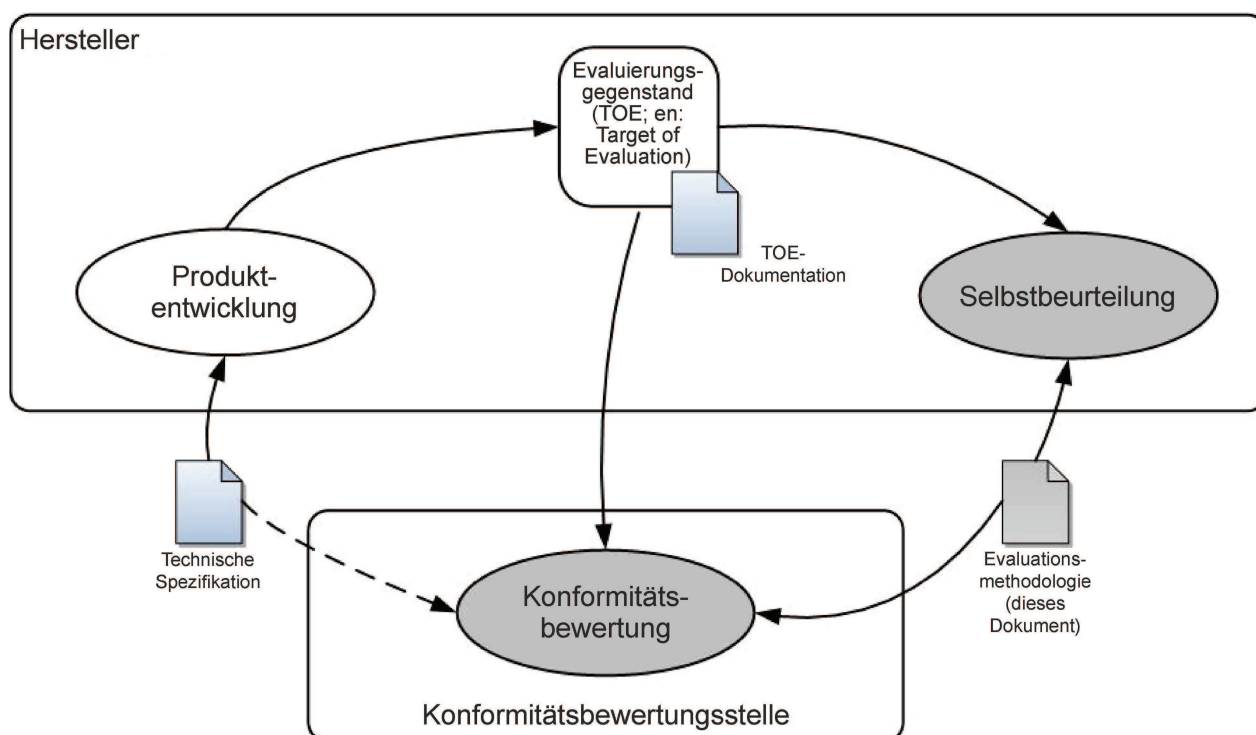


Bild 1 — Beziehung dieses Dokuments zu den Aufgaben in der Produktkonformitätsbewertung

1 Anwendungsbereich

Dieses Dokument beschreibt eine Methodologie zur Evaluierung der Cybersicherheit von IKT-Produkten, die mit vorab festgelegten Ressourcen für Zeit und Arbeitsaufwand durchgeführt werden kann. Es ist für die Anwendung aller drei im CSA definierten Vertrauenswürdigkeitsstufen (d. h. niedrig, mittel und hoch) vorgesehen.

Die Methodologie umfasst verschiedene Evaluierungsblöcke mit Bewertungsaufgaben, die den Evaluierungsanforderungen des CSA für die genannten drei Vertrauenswürdigkeitsstufen entsprechen. Gegebenenfalls kann sie sowohl bei der Drittparteien- als auch bei der Selbstbewertung angewendet werden.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 Evaluator

Einzelperson, die eine Evaluierung durchführt

Anmerkung 1 zum Begriff: Im Rahmen der Akkreditierung wird der Begriff „Prüfer“ für diese Einzelperson verwendet.

3.2 Auditor

Einzelperson, die ein Audit durchführt

3.3 Zertifizierungsfunktion

Person oder Gruppe von Personen, die für die Entscheidung über die Zertifizierung verantwortlich ist

Anmerkung 1 zum Begriff: Je nach Schema darf die Zertifizierungsfunktion Nachweise außerhalb des ETR (3.13) als eine Grundlage für die Zertifizierungsentscheidung verwendet werden.

3.4 Schemaentwickler

Person oder Organisation, die für ein Konformitätsbewertungsschema verantwortlich ist

Anmerkung 1 zum Begriff: Bei Schemata, die im Rahmen des CSA entwickelt werden, hilft die so genannte „Ad-hoc-Gruppe“ dem Schemaentwickler.

Anmerkung 2 zum Begriff: Diese Definition basiert auf der Definition von „Programmeigner“ in EN ISO/IEC 17000 und ist an diese angeglichen.

3.5

bestätigen

<Evaluationsverb> erklären, dass etwas detailliert und mit einer unabhängig bestimmten Angemessenheit geprüft wurde

[QUELLE: ISO/IEC 18045:2022, 3.2, modifiziert — Anmerkung zum Begriff wurde entfernt]

3.6

verifizieren

<Evaluationsverb> streng, detailliert und mit einer unabhängig bestimmten Angemessenheit prüfen

Anmerkung 1 zum Begriff: Siehe auch „bestätigen“. Dieser Begriff hat eine strengere Bedeutung. Der Begriff „verifizieren“ wird im Zusammenhang mit Evaluatorenaktionen verwendet, wenn ein unabhängiger Aufwand durch den Evaluator erforderlich ist.

[QUELLE: ISO/IEC 18045:2022, 3.22]

3.7

bestimmen

<Evaluationsverb> eine bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse mit dem Ziel bestätigen, eine bestimmte Schlussfolgerung zu erreichen

Anmerkung 1 zum Begriff: Die Verwendung dieses Begriffs setzt eine wirklich unabhängige Analyse voraus, in der Regel, ohne dass eine vorhergehende Analyse durchgeführt wurde. Vergleiche die Begriffe „bestätigen“ oder „verifizieren“, welche voraussetzen, dass bereits eine Analyse durchgeführt wurde, welche überprüft werden muss.

[QUELLE: ISO/IEC 18045:2022, 3.5]

3.8

IKT-Produkt

Produkt mit Informations- und/oder Kommunikationstechnik

Anmerkung 1 zum Begriff: IKT umfasst jedes Produkt, das digitale Informationen elektronisch in digitaler Form speichert, abrufen, verarbeitet, überträgt oder empfängt (z. B. Personal Computer, Smartphones, digitales Fernsehen, E-Mail-Systeme, Roboter).

3.9

Evaluierungsgegenstand

TOE, en: target of evaluation

Produkt (oder Teile davon, wenn das Produkt nicht vollständig evaluiert wird) mit einer klaren Abgrenzung, das der Evaluierung unterliegt

3.10

FIT-Sicherheitsvorgabe

FIT-ST

dokumentierte Informationen, die die Sicherheitseigenschaften und die Betriebsumgebung des *TOE* (3.9) beschreiben

Anmerkung 1 zum Begriff: Die FIT-ST kann je nach CSA-Vertrauenswürdigkeitsstufe unterschiedliche Inhalte, Strukturen und Größen haben.

3.11

FIT-Schutzprofil

FIT-PP

implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen TOE-Typ

[QUELLE: ISO/IEC 15408-1:2022, 3.68]

3.12

Handbuch zur sicheren Benutzung

SUG, en: secure user guide

dokumentierte Informationen, die beschreiben, welche Schritte notwendig sind, um den *TOE* (3.9) in den vorgesehenen *sicheren Zustand* (3.16) zu versetzen

3.13

technischer Evaluierungsbericht

ETR, en: evaluation technical report

dokumentierte Information, die die Ergebnisse der Evaluierung beschreibt

3.14

schemaspezifische Prüfliste

Liste von Elementen, die den erforderlichen Detaillierungsgrad und Grad der Granularität der Dokumentation definieren, die durch das Schema festgelegt sind

3.15

Wissen

Fakten, Informationen, Wahrheiten, Grundsätze oder Erkenntnisse, die durch Erfahrung oder Bildung erworben wurden

Anmerkung 1 zum Begriff: Ein Beispiel für Wissen ist die Fähigkeit, die verschiedenen Teile einer Informations-vertrauenswürdigkeitsnorm zu beschreiben.

Anmerkung 2 zum Begriff: Dieses Konzept unterscheidet sich vom Konzept „Wissen über den TOE“.

[QUELLE: ISO/IEC TS 17027:2014, 2.56, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt aus ISO/IEC 19896-1:2018, Anmerkung 2 zum Begriff ist neu]

3.16

sicherer Zustand

Zustand, in dem alle Daten in Bezug auf die Sicherheitsfunktionalität des *TOE* (3.9) korrekt sind und die Sicherheitsfunktionalität erhalten bleibt

3.17

Selbstbewertung

Konformitätsbewertungsaufgabe, die von der Person oder Organisation durchgeführt wird, die den *TOE* (3.9) bereitstellt oder die Gegenstand der Konformitätsbewertung ist

[QUELLE: EN ISO/IEC 17000:2020, 4.3, modifiziert — Anmerkungen zum Begriff und Beispiele wurden entfernt]

3.18

Parameter der Evaluierungsaufgabe

Parameter, der bei Verwendung dieses Dokuments angegeben werden muss, um festzulegen, wie die Evaluierungsaufgabe vom *Evaluator* (3.1) ausgeführt werden muss

4 Konformität

Die folgende Tabelle 1 dient als Verweisung darauf, wie die Evaluierungsaufgaben für ein bestimmtes Schema für die verschiedenen Vertrauenswürdigkeitsstufen des CSA ausgewählt werden sollten:

Tabelle 1 — Evaluierungsaufgaben gegenüber Konformitätsforderung der CSA-Vertrauenswürdigkeitsstufe

Evaluierungsaufgaben	Verweisung	Konformitätsforderung der CSA-Vertrauenswürdigkeitsstufe		
		niedrig	mittel	hoch
Vollständigkeitsprüfung	6.1	erforderlich	erforderlich	erforderlich
Überprüfung der Sicherheitsfunktionalitäten	6.3	erforderlich		
Evaluierung der FIT-Sicherheitsvorgabe	6.4		erforderlich	erforderlich
Entwicklungsdokumentation ^a	6.5	erforderlich	erforderlich	erforderlich
Evaluierung der TOE-Installation	6.6	empfohlen	erforderlich	erforderlich
Konformitätsprüfung	6.7	empfohlen	erforderlich	erforderlich
Schwachstellenprüfung	6.8	empfohlen	erforderlich (oder mit 6.9 erfüllt)	
Erweiterte Schwachstellenprüfung	6.9		empfohlen	
Penetrationsprüfung	6.10			erforderlich
Grundlegende Kryptoanalyse	6.11	empfohlen	empfohlen ^b	
Erweiterte Kryptoanalyse	6.12			erforderlich
^a Die schemaspezifische Prüfliste darf für ein bestimmtes Schema leer sein, so dass diese Evaluierungsaufgaben nicht anwendbar sind. ^b Wenn die Kryptofunktionalität zum Kern des Produkts gehört, ist es sinnvoll, dass die Schemaentwickler sie einbeziehen, z. B. durch die Definition entsprechender Produktklassen.				

ANMERKUNG 1 Die Evaluierung des FIT-Schutzprofils ist ein eigenständiger Prozess und nicht Teil der Evaluierung eines TOE. Während das FIT-PP festlegt, für welche CSA-Vertrauenswürdigkeitsstufe es anwendbar ist, ist die Evaluierung eines FIT-PP diesbezüglich agnostisch.

Um die Methodologie für ein bestimmtes Schema umzusetzen, müssen folgende Schritte durchgeführt werden:

1. Der Schemaentwickler muss eine Risikobeurteilung (der Domäne) durchführen, die die zu betrachtende Domäne überprüft.
2. Der Schemaentwickler muss jeder im Schema verwendeten Vertrauenswürdigkeitsstufe des CSA das Angriffspotential (vgl. 5.4 und Anhang F) zuordnen.
3. Für jede CSA-Vertrauenswürdigkeitsstufe muss der Schemaentwickler diejenigen Evaluierungsaufgaben auswählen, die für diese Stufe erforderlich sind; diese sind in Tabelle 1 grau markiert.
4. Für jede gewählte Aufgabe müssen die Schemaentwickler die Parameter für diese Evaluierungsaufgabe überprüfen und auf der Grundlage der Risikobeurteilung und des ermittelten Angriffspotentials angemessen festlegen. Für die Evaluierungsaufgabe „Entwicklungsdokumentation“ beinhaltet dies die Erstellung einer schemaspezifischen Prüfliste (die möglicherweise leer ist).

5. Für jede CSA-Vertrauenswürdigkeitsstufe muss der Schemaentwickler die für diese Stufe empfohlenen Evaluationsaufgaben überprüfen, wenn eine Einbeziehung sinnvoll ist; diese Aufgaben sind in Tabelle 1 mit dem Wort „empfohlen“ gekennzeichnet.
6. Für jede CSA-Vertrauenswürdigkeitsstufe muss der Schemaentwickler überprüfen, ob diese Evaluierungsaufgaben auf der Grundlage des ermittelten Angriffspotentials für das Schema ausreichend sind. Wenn dies nicht der Fall ist, muss der Schemaentwickler zusätzliche Evaluierungsaufgaben (z. B. aus der gleichen CSA-Vertrauenswürdigkeitsstufe), Arbeitsaufgaben aus einer höheren CSA-Vertrauenswürdigkeitsstufe oder zusätzliche, in dieser Methodologie nicht festgelegte Arbeitsaufgaben auswählen. Diese ersetzen möglicherweise bereits ausgewählte Arbeitsaufgaben.
7. Für jede neu gewählte oder aktualisierte Arbeitsaufgabe müssen die Schemaentwickler die Parameter für diese Arbeitsaufgabe überprüfen und auf der Grundlage der Risikobeurteilung und des Angriffspotentials angemessen festlegen.

Wenn die Schemaentwickler die Evaluierung/Beurteilung des Entwicklungsprozesses einbeziehen wollen, gibt es eine zusätzliche Arbeitsaufgabe für das Schema: Der Schemaentwickler muss über die Gültigkeit der Ergebnisse der Prozessevaluierung/-beurteilung für zukünftige Produktevaluierungen entscheiden. Das bedeutet, dass die entwicklungsbezogenen Arbeitsaufgaben einmal durchgeführt werden dürfen und die Ausgabe dieser Arbeitsaufgaben anschließend in mehreren Produktevaluierungen verwendet wird (z. B. als Voraussetzung). Optional dürfen die Auditoren eine Liste von Artefakten definieren, die bei jeder nachfolgenden Produktevaluierung vorzulegen sind, um zu zeigen, dass die auditierten Prozesse noch funktionsfähig sind.

Bei der Absicht, diesen Mechanismus zur Wiederverwendung von Evaluierungen/Beurteilungen des Entwicklungsprozesses einzubeziehen, müssen die Schemata sicherstellen, dass die Wiederverwendung auf Fälle beschränkt ist, in denen der Entwicklungsprozess in allen Evaluierungen oder Beurteilungen gleich ist, d. h. der/die Standort(e), das Wissen der Mitarbeiter und die tatsächlichen Prozesse sind identisch oder gleichwertig. Um dies zu erreichen, darf die anfängliche Evaluierung oder Beurteilung breiter angelegt werden (d. h. einen größeren Bereich der Entwicklung abdecken). Zusätzlich muss das Schema die maximale Dauer begrenzen, in der die Ergebnisse annehmbar sein sollen.

BEISPIEL Ein übliches Höchstalter für diese Ergebnisse ist zwei Jahre. Das bedeutet, wenn die Evaluierung/Beurteilung mehr als zwei Jahre nach den Ergebnissen der Evaluierung des Entwicklungsprozesses erfolgt, muss der Entwicklungsprozess neu beurteilt/neu evaluiert werden. Wird ein bestehendes SDL-Zertifikat (en: software development lifecycle certificate) verwendet, ist dessen Gültigkeit eine weitere Möglichkeit für die Gültigkeit dieses Nachweises.

Für einige Evaluierungsaufgaben kann das Schema zusätzliche Eingaben des Entwicklers erfordern, z. B. eine Architekturübersicht. Dieser zusätzliche Aufwand sollte so weit wie möglich begrenzt werden, insbesondere wenn diese Dokumentation in der Regel nur für die Beurteilung oder Evaluierung erstellt wird, d. h. für den TOE ohnehin nicht ohne weiteres verfügbar ist.

ANMERKUNG 2 Das Erfordernis von Designinformationen schließt möglicherweise einige Produkte von der Beurteilung oder Zertifizierung aus, da diese Informationen aufgrund der Tatsache, dass einige Komponenten von Drittanbietern, einschließlich der Hardware, proprietär und diese Designinformationen somit unzugänglich sein könnten, möglicherweise nicht verfügbar sind. Dies ist im Allgemeinen nicht zutreffend, wenn White-Box-Tests durchgeführt werden (wenn dies eine Option im Schema ist). Eine weitere Zusammensetzung von zertifizierten Teilen ist eine Möglichkeit, dieses Problem zu verringern.

Ein Beispiel für die Integration dieser Methodologie in ein Schema ist in Anhang D angegeben.

5 Allgemeine Konzepte

5.1 Anwendung dieser Methodologie

Abschnitt 5 beschreibt Elemente einer Evaluationsmethodologie für zeitlich festgelegte Sicherheitszertifizierung und Selbstbewertung.

Um eine spezifische Evaluationsmethodologie auf der Grundlage dieser generischen Methodologie zu instanziierten, werden die erforderlichen Evaluierungsaufgaben in Abhängigkeit von der beabsichtigten CSA-Vertrauenswürdigkeitsstufe nach dem CSA ausgewählt. Je nach Domäne sind bestimmte Evaluierungsaufgaben erforderlich, während andere optional sind (siehe Abschnitt 4). Bei probenbasierten Evaluierungsaufgaben muss das Schema den Probenumfang und die Probenstrategie sowie das absolute oder relative Gewicht, d. h. die Anzahl der Personentage oder den prozentualen Anteil an der gesamten Evaluierungszeit, festlegen. Es können zusätzliche Einschränkungen für die Probenahme vorgesehen werden, z. B. für die Grenzen der Probenahme in Abhängigkeit von der CSA-Vertrauenswürdigkeitsstufe.

Um diese Methodologie anzuwenden, ist es nicht notwendig, alle in Abschnitt 6 beschriebenen Evaluierungsaufgaben für jede CSA-Vertrauenswürdigkeitsstufe zu verlangen. Zum Beispiel könnte ein Schema, das für die CSA-Vertrauenswürdigkeitsstufe „mittel“ ausgelegt ist, eine Evaluierungsaufgabe „Grundlegende Kryptoanalyse“ erfordern oder diese weglassen und stattdessen möglicherweise die erforderlichen Teile in die Arbeitsaufgabe „Konformitätsprüfung“ integrieren.

ANMERKUNG Dieses Dokument und das sich daraus ergebende Schema definieren nicht die genaue Struktur der von der Evaluierung verwendeten oder erstellten Dokumente, z. B. der FIT-ST oder des ETR. Diese sind schemaabhängig.

5.2 Wissen über den TOE

Für das Schema werden verschiedene Gruppen von Informationen oder Informationen mit unterschiedlichen Detaillierungsgraden benötigt. Dies hängt zum einen von der geforderten Vertrauenswürdigkeit ab, zum anderen könnten zusätzliche Informationen bestimmte Evaluierungsaufgaben beschleunigen.

Im Allgemeinen muss der Entwickler eine FIT-Sicherheitsvorgabe und ein Handbuch zur sicheren Benutzung bereitstellen. Letzteres ist unter Umständen nicht erforderlich, wenn der TOE automatisch in den sicheren Zustand nach FIT-ST geht, d. h. keine weitere Benutzerführung notwendig ist.

Das Schema kann zusätzliche Informationen für bestimmte Aufgaben erfordern. Dies ist ggf. in den jeweiligen Evaluierungsaufgaben angegeben.

Der Evaluator muss Zugang zu Informationen (wie Normen, Protokollspezifikationen) bezüglich der im TOE implementierten Techniken haben, sofern diese Informationen öffentlich zugänglich sind.

ANMERKUNG Öffentlich zugänglich bedeutet nicht kostenlose Bereitstellung.

5.3 Evaluierung des Entwicklungsprozesses

Diese Methodologie befasst sich mit der Evaluierung von IKT-Produkten, und ein Schema könnte seine Evaluierungsaufgaben auf rein IKT-produktbezogene Aufgaben beschränken. Die Erfahrung bei der Zertifizierung von IKT-Produkten hat jedoch gezeigt, dass es sinnvoll und wertvoll ist, auch den Entwicklungsprozess zu evaluieren. Dies betrifft sowohl die anfängliche Entwicklung (z. B. in Bezug auf die Sicherheit während des Designs und der Konstruktion des Produkts, einschließlich der Standortsicherheit) als auch Aspekte nach der Auslieferung des Produkts, z. B. Schwachstellen und Aktualisierungsmanagementprozesse. Um die Nutzung der Auditergebnisse in zukünftigen Produktevaluierungen zu verbessern, darf der Auditor einen Satz von Artefakten (z. B. Besprechungsprotokolle, Auflistung von Konfigurationsmanagementsystemen, ausgefüllten Prüflisten) definieren, die dann in jeder nachfolgenden Produktevaluierung angefordert werden, um zu verifizieren, dass die auditierten Prozesse in diesem Fall eingehalten wurden.

Generische Normen für die Evaluierung von Entwicklungsprozessen sollten wiederverwendet werden, wo dies möglich, anwendbar oder verfügbar ist.

5.4 Angriffspotential

Um die notwendigen Evaluierungsaufgaben und deren Parameter zu bestimmen, ist es notwendig, den erwarteten Bedrohungsagenten zu definieren, der mit einer bestimmten Stärke gekennzeichnet ist, die auch Angriffspotential genannt wird. Die Arbeitsaufgabe des Evaluators bei der Schwachstellenanalyse darf Penetrationsprüfungen unter Annahme des Angriffspotentials des Bedrohungsagenten umfassen. In diesem Dokument wird von den folgenden Stufen des Angriffspotentials ausgegangen, wobei die Kategorisierung auf [2] und [5] basiert.

- Einfach
- Erweitert einfach
- Moderat
- Hoch

ANMERKUNG 1 Die Angriffspotentiale moderat und hoch sind wahrscheinlich nicht in einem zeitlich festgelegten Evaluierungsschema adressierbar: Die systematische Verfügbarkeit von detaillierter Dokumentation wird wahrscheinlich notwendig sein, um Evaluatoren zu ermöglichen, auf Augenhöhe mit Bedrohungsagenten hoher Stufe zu sein.

Der CSA [1] definiert drei Vertrauenswürdigkeitsstufen: niedrig, mittel und hoch. Jeder Stufe ist ein implizit definiertes Angriffsszenario zugeordnet. Den Schemaentwicklern wird geraten, die Definitionen im CSA zu überprüfen, um die Vertrauenswürdigkeitsstufen des CSA (wie für ihre Domäne zutreffend) mit dem in dieser Methodologie verwendeten Angriffspotential abzugleichen.

ANMERKUNG 2 Die im Zusammenhang mit dem Angriffspotential verwendeten Begriffe werden so verwendet, wie sie in diesem Dokument definiert sind, und weichen von der Bedeutung ähnlicher, im CSA verwendeter Begriffe ab.

Am Ende bewerten die Evaluatoren, ob ein Bedrohungsagent, der ein bestimmtes Angriffspotential besitzt, in der Lage ist, die Sicherheitsfunktionalität des TOE zu umgehen oder zu brechen.

Die Berechnung des Angriffspotentials ist Anhang F zu entnehmen.

5.5 Aufbau von Wissen

Um sicherzustellen, dass jede Evaluierungsaufgabe zu den erwarteten Ergebnissen führt, müssen die Evaluatoren über bestimmtes Wissen und Kompetenzen verfügen. Dieses Wissen wird bei jeder Evaluierungsaufgabe kurz beschrieben und muss bei Einrichtung des Schemas präzisiert werden.

Um sicherzustellen, dass eine Gesamtevaluierung die erwarteten Ergebnisse liefert, müssen die kompetenten Evaluatoren im Team gut zusammenarbeiten. Insbesondere die Evaluatoren, die an den Dokumententeilen der Evaluierung arbeiten, müssen sehr eng mit denjenigen Evaluatoren zusammenarbeiten, die die eigentlichen Prüfungen durchführen; im Idealfall handelt es sich dabei um dieselbe(n) Person(en), insbesondere wenn die Gesamtdauer der Evaluierung kurz ist.

6 Evaluierungsaufgaben

6.1 Vollständigkeitsprüfung

6.1.1 Ziel

Das Ziel dieser Evaluierungsaufgabe ist es, zu verifizieren, dass alle für die Evaluierung erforderlichen Nachweise erbracht wurden.

6.1.2 Evaluierungsmethode

Diese Evaluierungsaufgabe ist eine Vollständigkeitsprüfung der vom Schema geforderten Nachweise. Es ist kein Zugriff auf interne Dokumente erforderlich. Je nach TOE kann der Zugriff auf öffentlich zugängliche Spezifikationen oder andere Dokumente, die mit dem TOE verteilt oder von ihm in Bezug genommen werden, erforderlich sein.

6.1.3 Kompetenz des Evaluators

Die Evaluatoren müssen die Anforderungen des Schemas bezüglich der Nachweise kennen.

6.1.4 Workunits der Evaluatoren

6.1.4.1 Workunit 1

Die Evaluatoren müssen prüfen, ob alle für die Evaluierung erforderlichen Nachweise vorhanden sind. Dazu gehört eine ausreichende Anzahl von TOEs.

Möglicherweise sind mehrere Instanzen der TOEs erforderlich, z. B. weil ein TOE während der Prüfung komplett ausfallen oder durch einige Prüfungen unbrauchbar werden kann, oder weil parallele Prüfungen (zur Beschleunigung) durchgeführt werden.

6.1.4.2 Workunit 2

Der Evaluator muss überprüfen, ob der Hersteller die für die Durchführung der Evaluierungsaufgaben des TOE erforderliche Prüfumgebung zur Verfügung gestellt hat, falls dies für die Prüfaufgaben und den TOE zutreffend ist.

6.1.4.3 Workunit 3

Wenn White-Box-Kryptographie Teil der Evaluierung ist, müssen die Evaluatoren überprüfen, ob der vorgelegte Nachweis die in der FIT-ST festgelegte Kryptographie und die Anforderungen an den Nachweis der zutreffenden kryptographischen Workunits abdeckt.

Dies kann geschehen, indem alle Sicherheitsfunktionen identifiziert werden, die Kryptographie enthalten (wie in der FIT-ST angegeben), und überprüft wird, ob der entsprechende Nachweis für den kryptographischen Teil vorhanden ist.

ANMERKUNG Der Nachweis ist in der Regel ein Quellcode, Pseudocode oder Schaltplan und die Kryptobeschreibung/Spezifikation, die in der FIT-ST oder in einem separaten Dokument bereitgestellt wird.

6.2 Evaluierung des FIT-Schutzprofils

6.2.1 Ziel

Das Ziel dieser Evaluierungsaufgabe ist es, zu verifizieren, dass das FIT-PP gut aufgebaut, konsistent und als Grundlage für zukünftige FIT-ST geeignet ist.

ANMERKUNG Die Hintergrundinformationen für das FIT-PP-Konzept sind in Anhang B enthalten.

6.2.2 Evaluierungsmethode

Diese Evaluierungsaufgabe ist eine vollständige Überprüfung des Schutzprofils. Es ist kein Zugriff auf einen tatsächlichen TOE erforderlich. Je nach FIT-PP kann der Zugriff auf öffentlich zugängliche Spezifikationen (z. B. Normen) für die im FIT-PP beschriebene Technik erforderlich sein.

6.2.3 Kompetenz des Evaluators

Die Evaluatoren müssen die typischen TOEs kennen, die das FIT-PP implementieren. Sie müssen in der Lage sein, Dokumentationen wie Normen oder Nutzungsszenarien zu überprüfen.

6.2.4 Workunits der Evaluatoren

6.2.4.1 Workunit 1

Die Evaluatoren müssen prüfen, ob das FIT-PP die im Schema festgelegten strukturellen Anforderungen erfüllt.

Die Evaluatoren müssen verifizieren, dass die im FIT-PP enthaltenen Informationen frei von Widersprüchen/Diskrepanzen und Inkonsistenzen sind.

Die Evaluatoren müssen bestätigen, dass das FIT-PP die wirklichen Sicherheitseigenschaften der Klasse von TOEs beschreiben, insbesondere, dass es in Bezug auf die Sicherheitseigenschaften nicht „irreführend“ ist.

Die Evaluatoren müssen bestätigen, dass das FIT-PP die für die bestimmungsgemäße Verwendung relevanten Sicherheitseigenschaften beschreibt.

Die Evaluatoren müssen verifizieren, dass die Sicherheitsfunktionen im FIT-PP für den bestimmungsgemäßen Anwendungsfall relevant sind.

Die Evaluatoren müssen bestätigen, dass die im FIT-PP angegebenen Annahmen realistische Annahmen für den bestimmungsgemäßen Anwendungsfall der Klasse von TOEs sind.

Die Evaluatoren müssen bestätigen, dass die Gruppe der Bedrohungsagenten unter Berücksichtigung des bestimmungsgemäßen Anwendungsfalls der Klasse von TOEs realistisch ist.

Die Evaluatoren müssen bestätigen, dass die Grenzen der Klasse von TOEs und die Grenzen der Evaluierung im FIT-PP klar und unmissverständlich definiert sind.

Wenn das Schema die kryptographischen Anforderungen für die vorgesehene CSA-Vertrauenswürdigkeitsstufe und Produktklasse pflegt, muss der Evaluator die im FIT-PP enthaltene kryptographische Spezifikation untersuchen, um festzustellen, ob die kryptographischen Mechanismen geeignet sind, ihr im FIT-PP angegebenes Sicherheitsziel zu erreichen.

Die Evaluatoren müssen verifizieren, dass das FIT-PP für die potentiellen Endkunden verständlich ist. „Verständlichkeit“ bedeutet in diesem Zusammenhang, dass die Sprache und die Beschreibungstiefe des FIT-PP dem Wissen des erwarteten Endkunden angemessen sind, einschließlich der erwarteten Kenntnis über Begriffe und Konzepte.

Die Evaluatoren müssen bestätigen, dass die im FIT-PP angegebene Sicherheitsfunktionalität mit den geltenden Anforderungen übereinstimmt, z. B. mit den im Schema angegebenen Anforderungen.

Die Evaluatoren müssen prüfen, ob alle zusätzlichen (später vom FIT-ST-Autor zu instanziiierenden) Aktionen, die im FIT-PP eingeführt werden (sogenannte Operationen), geeignet gekennzeichnet sind.