

DIN EN 17640

ICS 35.030

Einsprüche bis 2021-08-18

Entwurf**Cybersicherheitsevaluationsmethodologie für IKT-Produkte;
Deutsche und Englische Fassung prEN 17640:2021**

Fixed time cybersecurity evaluation methodology for ICT products;
German and English version prEN 17640:2021

Méthode d'évaluation de la cybersécurité pour produits TIC;
Version allemande et anglaise prEN 17640:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-06-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 116 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17640:2021) wurde vom Technischen Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

IEC 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 62443-4-2, *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

- Entwurf -

2021-07

prEN 17640:2021

Titel de: Cybersicherheitsevaluationsmethodologie für IKT-Produkte
Titel en: Fixed time cybersecurity evaluation methodology for ICT products
Titel fr: Méthode d'évaluation de la cybersécurité pour produits TIC

Inhalt

	Seite
Europäisches Vorwort	5
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Konformität	10
5 Allgemeine Begriffe	12
5.1 Anwendung dieser Methodologie	12
5.2 Wissen über den TOE	12
5.3 Evaluierung des Entwicklungsprozesses	13
5.4 Angriffspotential	13
5.5 Aufbau von Wissen	14
6 Evaluierungsarbeitsaufgaben	14
6.1 Vollständigkeitsprüfung	14
6.1.1 Ziel	14
6.1.2 Evaluierungsverfahren	14
6.1.3 Qualifikation des Evaluators	14
6.1.4 Workunits der Evaluatoren	14
6.2 Evaluierung des Schutzprofils	15
6.2.1 Ziel	15
6.2.2 Evaluierungsverfahren	15
6.2.3 Qualifikation des Evaluators	15
6.2.4 Workunits der Evaluatoren	15
6.3 Evaluierung der Sicherheitsvorgabe	16
6.3.1 Ziel	16
6.3.2 Evaluierungsverfahren	16
6.3.3 Qualifikation des Evaluators	16
6.3.4 Workunits der Evaluatoren	16
6.4 Überprüfung der Sicherheitsfunktionalitäten	18
6.4.1 Ziel	18
6.4.2 Evaluierungsverfahren	18
6.4.3 Qualifikation des Evaluators	18
6.4.4 Workunits der Evaluatoren – Workunit 1	18
6.5 Entwicklungsdokumentation	18
6.5.1 Ziel	18
6.5.2 Evaluierungsverfahren	18
6.5.3 Qualifikation des Evaluators	19
6.5.4 Workunits	19
6.6 Evaluierung der TOE-Installation	19
6.6.1 Ziel	19
6.6.2 Evaluierungsverfahren	19
6.6.3 Qualifikation des Evaluators	19
6.6.4 Workunits der Evaluatoren	19
6.7 Konformitätsprüfung	20
6.7.1 Ziel	20

6.7.2	Evaluierungsverfahren.....	20
6.7.3	Qualifikation des Evaluators.....	20
6.7.4	Workunits der Evaluatoren.....	21
6.8	Anfälligkeitsüberprüfung.....	22
6.8.1	Ziel	22
6.8.2	Evaluierungsverfahren.....	22
6.8.3	Qualifikation des Evaluators.....	22
6.8.4	Workunits der Evaluatoren.....	23
6.9	Anfälligkeitsprüfung	23
6.9.1	Ziel	23
6.9.2	Evaluierungsverfahren.....	24
6.9.3	Qualifikation des Evaluators.....	24
6.9.4	Workunits der Evaluatoren.....	24
6.10	Penetrationstest	26
6.10.1	Ziel	26
6.10.2	Evaluierungsverfahren.....	26
6.10.3	Qualifikation des Evaluators.....	27
6.10.4	Workunits der Evaluatoren.....	28
6.11	Grundlegende Kryptoanalyse	28
6.11.1	Ziel	28
6.11.2	Evaluierungsverfahren.....	29
6.11.3	Qualifikation des Evaluators.....	29
6.11.4	Workunits der Evaluatoren.....	29
6.12	Erweiterte Kryptoanalyse	30
6.12.1	Ziel	30
6.12.2	Evaluierungsverfahren.....	30
6.12.3	Qualifikation des Evaluators.....	30
6.12.4	Workunits der Evaluatoren.....	31
Anhang A (informativ) Beispiel für die Struktur einer Sicherheitsvorgabe.....		33
A.1	Allgemeines	33
A.2	Beispiel für die Struktur	33
A.3	Typische Inhalte einer ST.....	34
Anhang B (normativ) Der Begriff eines Schutzprofils		35
B.1	Allgemeines	35
B.2	Ziel und Grundlagen eines Schutzprofils (PP)	35
B.3	Leitlinien für Schemata zur Implementierung des PP-Begriffs.....	35
Anhang C (informativ) Annahmekriterien.....		36
C.1	Einleitung	36
C.2	Identifizierung, Authentifizierungskontrolle und Zugriffskontrolle.....	36
C.3	Sicherer Systemstart (Secure Boot).....	39
C.4	Kryptographie	40
C.5	Sicherer Zustand nach Ausfall	41
C.6	Geringste Funktionalität.....	42
C.7	Aktualisierungsmechanismus	43
Anhang D (informativ) Leitlinien für die Integration der Methodologie in ein Schema.....		44
D.1	Allgemeines	44
D.1.1	Einleitung	44
D.1.2	Durchführen einer Risikobeurteilung, Überprüfung der zu betrachtenden vertikalen Domäne	44
D.1.3	Zuordnen des Angriffspotentials zu den CSA-Stufen	44
D.1.4	Auswählen der für diese Stufe erforderlichen Evaluierungsarbeitsaufgaben	44
D.1.5	Überprüfen und Festlegen der Parameter für die Arbeitsaufgaben	44
D.1.6	Mögliche Auswahl von zusätzlichen oder übergeordneten Arbeitsaufgaben.....	45

D.1.7	Überprüfen und Festlegen der Parameter für die zusätzlichen Arbeitsaufgaben.....	45
D.1.8	Erstellen und Pflegen weiterer Schemaanforderungen und -leitlinien	45
D.2	Beispiel	46
Anhang E (informativ) Parameter der Methodologie und der Evaluierungsarbeitsaufgaben		49
E.1	Allgemeines	49
E.2	Parameter der Methodologie	49
E.3	Parameter der Evaluierungsarbeitsaufgaben.....	49
E.3.1	Parameter für 6.1 „Vollständigkeitsprüfung“	49
E.3.2	Parameter für 6.2 „Evaluierung des Schutzprofils“	49
E.3.3	Parameter für 6.3 „Evaluierung der Sicherheitsvorgabe“	49
E.3.4	Parameter für 6.4 „Überprüfung der Sicherheitsfunktionalitäten“	49
E.3.5	Parameter für 6.5 „Entwicklungsdokumentation“	49
E.3.6	Parameter für 6.6 „Evaluierung der TOE-Installation“	50
E.3.7	Parameter für 6.7 „Konformitätsprüfung“	50
E.3.8	Parameter für 6.8 „Anfälligkeitsüberprüfung“	50
E.3.9	Parameter für 6.9 „Anfälligkeitsprüfung“	50
E.3.10	Parameter für 6.10 „Penetrationstest“	50
E.3.11	Parameter für 6.11 „Grundlegende Kryptoanalyse“	50
E.3.12	Parameter für 6.12 „Erweiterte Kryptoanalyse“	50
Anhang F (normativ) Berechnung des Angriffspotentials.....		51
F.1	Allgemeines	51
F.2	Faktoren für das Angriffspotential	51
F.3	Numerische Faktoren für das Angriffspotential	51
F.3.1	Standardbewertungstabelle	52
F.3.2	Anpassung der Bewertungstabelle	53
Anhang G (normativ) Berichterstattung über die Ergebnisse einer Evaluierung		55
G.1	Allgemeines	55
G.2	Schriftliche Berichterstattung	55
G.3	Mündliche Verteidigung der erzielten Ergebnisse.....	55
Literaturhinweise.....		57

Europäisches Vorwort

Dieses Dokument (prEN 17640:2021) wurde vom Technischen Komitee CEN/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

Die Grundlage für eine fundierte Produktzertifizierung ist eine zuverlässige, transparente und wiederholbare Evaluationsmethodologie. Es gibt mehrere produkt- oder schemaabhängige Evaluationsmethodologien, doch mit dem Aufkommen des Rechtsakts zur Cybersicherheit (CSA, en: Cybersecurity Act) [1] benötigen neue Schemata neue Methodologien, um die Cybersicherheitsfunktionalitäten von Produkten zu evaluieren. Diese neuen Methodologien werden benötigt, um die im CSA definierten Evaluierungsarbeitsaufgaben zu beschreiben (z. B. Überprüfung der technischen Dokumentation, Vergleich mit bekannten Anfälligkeiten). Hinzu kommt, dass bestehende Evaluationsmethodologien zur Cybersicherheit (z. B. EN ISO/IEC 15408 und EN ISO/IEC 18045) nicht zum Einsatz innerhalb einer festen Zeit ausgelegt sind, d. h. die Dauer der Evaluierung kann während der Durchführung erheblich verlängert werden.

Der CSA ermöglicht es Schemaentwicklern, sowohl eine Selbstbeurteilung als auch Fremdevaluierungen zu berücksichtigen. Die Selbstbeurteilung darf auf der Vertrauenswürdigkeitsstufe „niedrig“, die Fremdevaluierungen dürfen auf der Vertrauenswürdigkeitsstufe „niedrig“, „mittel“ oder „hoch“ durchgeführt werden. Und je nach den Anforderungen des einzelnen Schemas unterliegen die Evaluierungskriterien und die Methodologie möglicherweise einer zusätzlichen Anpassung. 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 die bestimmungsgemäße Verwendung des Schemas umzusetzen, die für allgemeine Zwecke oder in speziellen (vertikalen) Bereichen anwendbar ist, indem sie die Aspekte auswählen, die für die Selbstbeurteilung auf der Stufe „niedrig“ oder die Fremdevaluierung auf jeder vom Schema geforderten Stufe notwendig sind.

Dieses Dokument enthält das Mindestmaß an Evaluierungsaufgaben, die im CSA definiert sind, um die gewünschte 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 Evaluierungsarbeitsaufgaben oder durch die Verwendung der Parameter der Evaluierungsarbeitsaufgaben, 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 erneut zu verwenden.

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

Evaluatoren, Tester 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/Tester enthalten, und daher wird das Schema auch von **Akkreditierungsstellen** oder **nationalen Zertifizierungsstellen für Cybersicherheit** bei der Akkreditierung oder ggf. Autorisierung und Überwachung von Konformitätsbewertungsstellen verwendet.

Hersteller und **Entwickler** erhalten in der Evaluationsmethodologie die für jede Evaluierungsarbeitsaufgabe erforderliche generische Art von Nachweisen zur Vorbereitung auf die Beurteilung oder Evaluierung. Die Nachweis- und Evaluierungsarbeitsaufgaben sind unabhängig davon, ob die Evaluierung durch den Hersteller/Entwickler (d.h. erste Seite) oder durch eine andere Person (zweite/dritte Seite) 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 aus bestimmten Zertifikaten unter Anwendung dieser Evaluationsmethodologie gezogen wird. Auch hier wird erwartet, dass die Schemaentwickler zusätzliche, auf den Bereich des Schemas zugeschnittene Informationen über die durch Evaluierungen/Beurteilungen nach dieser Methodologie gewonnene Vertrauenswürdigkeit bereitstellen.

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

ANMERKUNG In diesem Dokument wird der Begriff „Konformitätsbewertungsstelle“ (KBS) für KBS, die die Bewertung 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. Jeder Bereich (Schema) muss domänenspezifische Cybersicherheitsanforderungen für die zu evaluierenden/zertifizierenden Objekte bereitstellen. Diese Methodologie soll in Verbindung mit Spezifikationen verwendet werden, die solche Cybersicherheitsanforderungen enthalten.

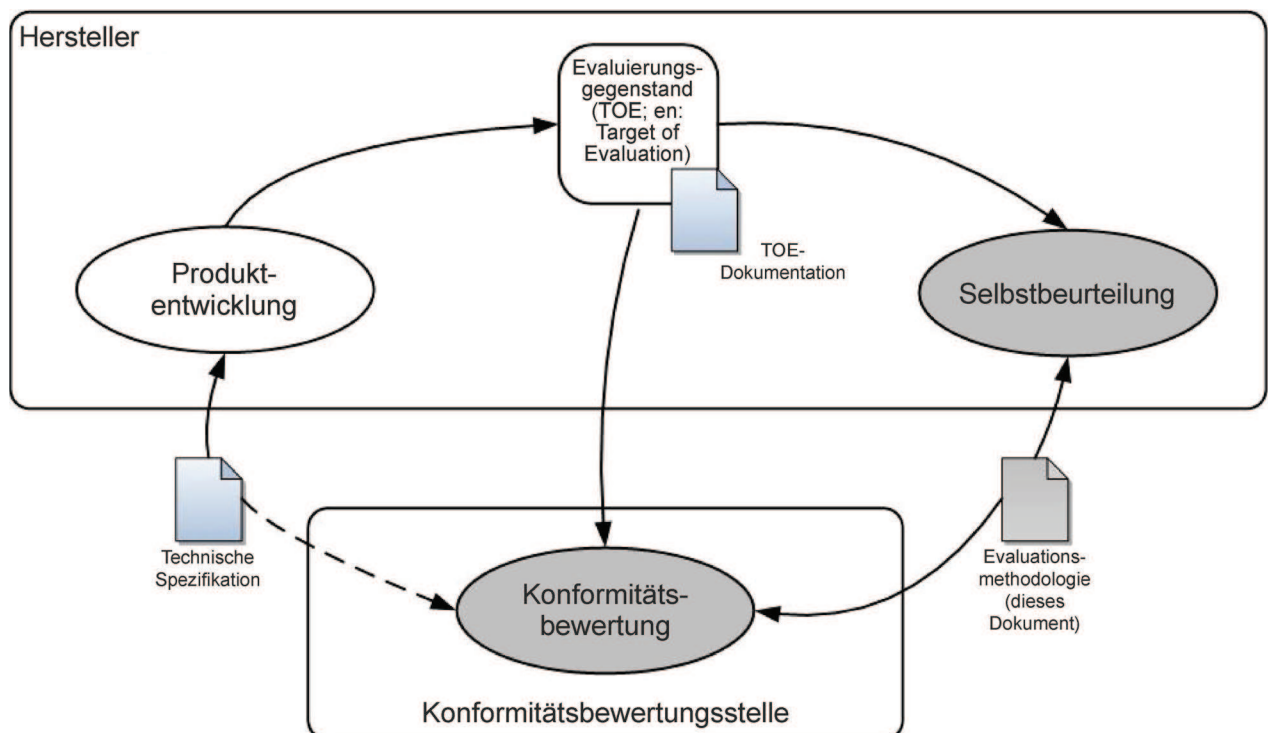


Bild 1 — Beziehung dieses Dokuments zu den Aufgaben in der Produktkonformitätsbewertung

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 soll für alle drei im CSA definierten Vertrauenswürdigkeitsstufen (d. h. niedrig, mittel und hoch) anwendbar sein.

Die Methodologie umfasst verschiedene Evaluierungsblöcke mit Bewertungsaufgaben, die den Evaluierungsanforderungen des CSA für die genannten drei Vertrauenswürdigkeitsstufen entsprechen.

Gegebenenfalls kann sie sowohl bei der Fremd- als auch bei der Selbstbeurteilung 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 <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 bestätigen

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

[QUELLE: EN ISO/IEC 15408-1:2009, Definition 3.1.4; ANMERKUNG entfernt]

3.2 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 als Grundlage für die Zertifizierungsentscheidung verwenden.

3.3 bestimmen

<Evaluationsverb> eine bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse bestätigen mit dem Ziel, 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: EN ISO/IEC 15408-1:2009, Definition 3.1.22]

3.4 Parameter der Evaluierungsarbeitsaufgabe

Parameter, der bei Verwendung dieses Dokuments angegeben werden muss, um festzulegen, wie die Evaluierungsarbeitsaufgabe vom Evaluator ausgeführt werden muss

3.5

Technischer Evaluierungsbericht

ETR, en: evaluation technical report

dokumentierte Information, die die Ergebnisse der Evaluierung beschreibt

3.6

Evaluator

Einzelperson, die eine Evaluierung durchführt

3.7

IKT-Produkt

Produkt mit Informations- und/oder Kommunikationstechnik

3.8

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 Informationsvertrauenswürdigkeitsnorm zu beschreiben.

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

3.9

Schutzprofil

PP, en: protection profile

implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen *TOE* (4.16)-Typ

[QUELLE: ISO/IEC EN 15408:2009, Definition 3.1.52]

3.10

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.

3.11

schemaspezifische Checkliste

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

3.12

sicherer Zustand

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

3.13

sicheres Benutzerhandbuch

dokumentierte Informationen, die beschreiben, welche Schritte notwendig sind, um den *TOE* (4.16) in den vorgesehenen sicheren Zustand zu versetzen

3.14

Sicherheitsvorgabe

ST, en: security target

dokumentierte Informationen, die die Sicherheitseigenschaften und die Betriebsumgebung des TOE (4.16) beschreiben

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

3.15

Selbstbeurteilung

Konformitätsbewertungsaufgabe, die von der Person oder Organisation durchgeführt wird, die die Konformitätsbewertung bereitstellt oder die Gegenstand der Konformitätsbewertung ist

[QUELLE: EN ISO/IEC 17000:2020, Definition 4.3; ANMERKUNGEN und BEISPIELE entfernt]

3.16

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

3.17

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 eine unabhängige Anstrengung durch den Evaluator erforderlich ist.

[QUELLE: EN ISO/IEC 15408-1:2009, Definition 3.1.84]

4 Konformität

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

Tabelle 1 — Evaluierungsarbeitsaufgaben gegenüber Konformitätsanspruch der CSA-Stufe

	Konformitätsanspruch der CSA-Stufe		
Evaluierungsarbeitsaufgaben	niedrig	mittel	hoch
Vollständigkeitsprüfung	muss	muss	muss
Evaluierung des Schutzprofils	entfällt	entfällt	entfällt
Überprüfung der Sicherheitsfunktionalitäten	muss		
Evaluierung der Sicherheitsvorgabe		muss	muss
Entwicklungsdokumentation	muss	muss	muss
Evaluierung der TOE-Installation	sollte	muss	muss
Konformitätsprüfung	sollte	muss	muss
Anfälligkeitsüberprüfung	sollte	muss (oder mit 6.9 erfüllt)	muss (oder mit 6.9 erfüllt)
Anfälligkeitsprüfung		sollte	sollte

	Konformitätsanspruch der CSA-Stufe		
Penetrationstest			muss
grundlegende Kryptoanalyse	sollte	sollte	
erweiterte Kryptoanalyse			sollte

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

ANMERKUNG 2 „Muss“ bedeutet, dass der CSA diese Evaluierungsarbeitsaufgabe für eine bestimmte Vertrauenswürdigkeitsstufe anfordert oder dass es notwendig ist, das Schema mit dieser Evaluationsmethodologie umzusetzen. „Sollte“ bedeutet, dass empfohlen wird, die Evaluierungsarbeitsaufgabe auszuwählen, dies aber nicht verpflichtend ist.

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

- 1) Der Schemaentwickler muss eine Risikobeurteilung durchführen, die den zu betrachtenden Bereich 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-Stufe muss der Schemaentwickler diejenigen Evaluierungsarbeitsaufgaben 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 Evaluierungsarbeitsaufgabe überprüfen und auf der Grundlage der Risikobeurteilung und des ermittelten Angriffspotentials angemessen festlegen.
- 5) Für jede CSA-Stufe muss der Schemaentwickler überprüfen, ob diese Evaluierungsarbeitsaufgaben auf der Grundlage des ermittelten Angriffspotentials für das Schema ausreichend sind. Wenn dies nicht der Fall ist, muss der Schemaentwickler zusätzliche Evaluierungsarbeitsaufgaben (z. B. aus der gleichen Stufe), Arbeitsaufgaben aus einer höheren Stufe oder zusätzliche, in dieser Methodologie nicht festgelegte Arbeitsaufgaben auswählen. Dies ersetzt möglicherweise bereits ausgewählte Arbeitsaufgaben.
- 6) 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 beabsichtigt ist, dass das Schema die Evaluierung/Beurteilung des Entwicklungsprozesses einschließt, 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 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, kann die anfängliche Evaluierung oder Beurteilung breiter angelegt werden (d. h. einen größeren Bereich der Entwicklung abdecken). Zusätzlich muss das Schema die Höchstdauer begrenzen, in der die Ergebnisse annehmbar sein sollen.

BEISPIEL Ein übliches Höchstalter für diese Ergebnisse ist 2 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.

Für einige Evaluierungsarbeitsaufgaben 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 3 Das Erfordernis von Gestaltungsinformationen 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 Gestaltungsinformationen somit unzugänglich sein könnten, möglicherweise nicht verfügbar sind. Dies ist im Allgemeinen nicht anwendbar, 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 ist in Anhang D aufgeführt.

5 Allgemeine Begriffe

5.1 Anwendung dieser Methodologie

Abschnitt 5 beschreibt Elemente einer Evaluationsmethodologie für die zeitlich begrenzte Sicherheitszertifizierung und Selbstbeurteilung.

Um eine spezifische Evaluationsmethodologie auf der Grundlage dieser generischen Methodologie zu instanziierten, werden die erforderlichen Evaluationsarbeitsaufgaben in Abhängigkeit von der beabsichtigten Vertrauenswürdigkeitsstufe nach dem CSA ausgewählt. Je nach Bereich sind bestimmte Evaluierungsarbeitsaufgaben erforderlich, während andere optional sind (siehe Abschnitt 2 dieses Dokuments). Bei probenbasierten Evaluierungsarbeitsaufgaben muss das Schema den Probenumfang und die Probenstrategie sowie das absolute oder relative Gewicht, d. h. die Anzahl der Manntage 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-Stufe.

Um diese Methodologie anzuwenden, ist es nicht notwendig, alle in Abschnitt 6 beschriebenen Evaluierungsarbeitsaufgaben für jede Vertrauenswürdigkeitsstufe zu verlangen. Zum Beispiel könnte ein Schema, das für die CSA-Vertrauenswürdigkeitsstufe „mittel“ ausgelegt ist, eine Evaluierungsarbeitsaufgabe „Grundlegende Kryptoanalyse“ erfordern oder diese weglassen und stattdessen 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 ST oder des TOE. 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 Evaluierungsarbeitsaufgaben beschleunigen.

Im Allgemeinen muss der Entwickler eine Sicherheitsvorgabe und ein sicheres Benutzerhandbuch bereitstellen. Letzteres mag überflüssig sein, wenn der TOE automatisch in den gewünschten Zustand geht, d. h. keine weitere Benutzerführung notwendig ist.

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

Der Evaluator muss Zugang zu Informationen (wie Normen, Protokollspezifikationen) bezüglich der im TOE implementierten Technologie 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 Evaluierungsarbeitsaufgaben 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 der Gestaltung und Konstruktion des Produkts, einschließlich der Sicherheit vor Ort) als auch Aspekte nach der Auslieferung des Produkts, z. B. Anfälligkeit und Aktualisierungsmanagementprozesse. Um die Nutzung der Auditergebnisse in zukünftigen Produktevaluierungen zu verbessern, kann der Auditor einen Satz von Artefakten (z. B. Besprechungsprotokolle, Auflistung von Konfigurationsmanagementsystemen, ausgefüllte Checklisten) 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 Evaluierungsarbeitsaufgaben und deren Parameter zu bestimmen, ist es notwendig, den erwarteten Bedrohungsagenten zu definieren, der mit einer bestimmten Stärke, auch Angriffspotential genannt, gekennzeichnet ist. Die Arbeitsaufgabe des Evaluators bei der Anfälligkeitsanalyse kann Penetrationstests unter Annahme des Angriffspotentials des Bedrohungsagenten umfassen. In diesem Dokument wird von den folgenden Stufen des Angriffspotentials ausgegangen, die Kategorisierung basiert auf [2] und [5]:

- einfach
- erweitert einfach
- moderat
- hoch

ANMERKUNG Angriffspotential moderat und hoch sind wahrscheinlich nicht in einem zeitlich begrenzten 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 empfohlen, die Definitionen im CSA zu überprüfen, um die Vertrauenswürdigkeitsstufen des CSA (wie für ihren Bereich zutreffend) mit dem in dieser Methodologie verwendeten Angriffspotential abzugleichen.

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

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

6 Evaluierungsarbeitsaufgaben

6.1 Vollständigkeitsprüfung

6.1.1 Ziel

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

6.1.2 Evaluierungsverfahren

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

6.1.3 Qualifikation 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

Der Evaluator muss prüfen, ob alle für die Evaluierung erforderlichen Nachweise vorhanden sind. Dazu gehört eine ausreichende Anzahl von TOEs.

ANMERKUNG Mehrere Proben der TOEs sind möglicherweise erforderlich, z. B. weil ein TOE während der Prüfung komplett ausfallen und durch einige Prüfungen unbrauchbar gemacht werden kann, oder parallele Prüfungen (zur Beschleunigung) werden durchgeführt.

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 ST festgelegte Kryptographie und die Anforderungen an den Nachweis der zutreffenden kryptographischen Workunits abdeckt.

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

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

6.2 Evaluierung des Schutzprofils

6.2.1 Ziel

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

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

6.2.2 Evaluierungsverfahren

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

6.2.3 Qualifikation des Evaluators

Die Evaluatoren müssen die PP-Domäne kennen. 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

Der Evaluator muss prüfen, ob das PP die im Schema festgelegten strukturellen Anforderungen erfüllt.

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

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

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

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

Die Evaluatoren müssen bestätigen, dass die im 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 PP klar und unmissverständlich definiert sind.

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

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

Die Evaluatoren müssen bestätigen, dass die im 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 ST-Autor zu instanziiierenden) Aktionen, die im PP eingeführt werden (sogenannte Operationen), geeignet gekennzeichnet sind.

ANMERKUNG „Geeignete Kennzeichnung“ bedeutet, dass die Operationen leicht gefunden werden können und mögliche Werte (einschließlich Freitext) für jede Variable, die in einer bestimmten Operation definiert ist, angegeben sind.

Die Evaluatoren müssen verifizieren, dass PP-Operationen mit bereitgestellten Werten bei keinem der bereitgestellten Werte zu einem Widerspruch mit den Sicherheitszielen führen.

6.3 Evaluierung der Sicherheitsvorgabe

6.3.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu verifizieren, dass die ST gut aufgebaut, konsistent und als Grundlage für eine weitere Evaluierung geeignet ist.

6.3.2 Evaluierungsverfahren

Diese Evaluierungsarbeitsaufgabe ist eine vollständige Überprüfung der Sicherheitsvorgabe. Es ist kein Zugriff auf den TOE erforderlich. Der Zugriff auf alle für die Evaluierung bereitgestellten Dokumente ist erforderlich. Je nach TOE könnte der Zugriff auf öffentlich verfügbare Spezifikationen erforderlich sein.

Wenn Kryptographie Teil der Evaluierung ist, muss die kryptographische Spezifikation ebenfalls als Teil des Nachweises betrachtet werden.

6.3.3 Qualifikation des Evaluators

Die Evaluatoren müssen die TOE-Domäne kennen. Sie müssen in der Lage sein, Dokumentationen zu überprüfen.

6.3.4 Workunits der Evaluatoren

6.3.4.1 Workunit 1a

Diese Workunit ist anwendbar, wenn die ST nicht auf einem PP basiert.

Der Evaluator muss prüfen, ob die ST die im Schema festgelegten strukturellen Anforderungen erfüllt.

ANMERKUNG Anhang A enthält einen Leitfaden zu den typischen Inhalten von STs.

Die Evaluatoren müssen verifizieren, dass die in der ST enthaltenen Informationen frei von Widersprüchen und Inkonsistenzen sind.

Die Evaluatoren müssen verifizieren, dass die Informationen in der ST frei von Widersprüchen zu anderen Informationen sind, die entlang des TOE zur Verfügung gestellt werden, insbesondere zum sicheren Benutzerhandbuch und anderen (gestaltungsrelevanten) Dokumenten, die durch das Schema vorgeschrieben sind (falls vorhanden).

Die Evaluatoren müssen bestätigen, dass die ST die wirklichen Sicherheitseigenschaften des TOE beschreiben, insbesondere, dass sie in Bezug auf die Sicherheitseigenschaften nicht „irreführend“ sind.

Die Evaluatoren müssen verifizieren, dass die ST die für die bestimmungsgemäße Verwendung relevanten Sicherheitseigenschaften beschreibt.

Die Evaluatoren müssen verifizieren, dass die Sicherheitsfunktionen in der ST für den bestimmungsgemäßen Anwendungsfall relevant sind.

Die Evaluatoren müssen bestätigen, dass die in der ST angegebenen Annahmen realistische Annahmen für den bestimmungsgemäßen Anwendungsfall des TOE sind.

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

Die Evaluatoren müssen bestätigen, dass der Anwendungsbereich und die Grenzen des TOE klar und unmissverständlich in der ST definiert sind.

Wenn das Schema kryptographische Anforderungen für die vorgesehene Vertrauenswürdigkeitsstufe und Produktklasse aufrechterhält, dann müssen die Evaluatoren überprüfen, ob die in der ST aufgeführten kryptographischen Algorithmen in der Menge der vom Schema genehmigten kryptographischen Algorithmen enthalten sind.

Der Evaluator muss die kryptographische Spezifikation bestätigen, um festzustellen, ob die kryptographischen Mechanismen geeignet sind, ihre Sicherheitszielsetzung zu erreichen.

Die Evaluatoren müssen überprüfen, ob die ST für die potentiellen Endkunden verständlich ist. „Verständlichkeit“ bedeutet in diesem Zusammenhang, dass die Sprache und die Beschreibungstiefe der ST dem Wissen des erwarteten Endkunden angemessen sind, einschließlich des erwarteten Wissens über Begriffe und Konzepte.

Die Evaluatoren müssen bestätigen, dass die in der ST angegebene Sicherheitsfunktionalität mit den geltenden Anforderungen, z. B. den in den Schutzprofilen angegebenen oder mit den im Schema angegebenen Anforderungen, übereinstimmt.

6.3.4.2 Workunit 1b

Diese Workunit ist anwendbar, wenn die ST auf einem PP basiert.

Die Evaluatoren müssen bestätigen, dass allen Vorgängen, die im PP angegeben sind, in der ST Werte zugeordnet sind.

Die Evaluatoren müssen verifizieren, dass die Informationen in der ST frei von Widersprüchen zu anderen Informationen sind, die entlang des TOE zur Verfügung gestellt werden, insbesondere zum sicheren Benutzerhandbuch und anderen (gestaltungsrelevanten) Dokumenten, die durch das Schema vorgeschrieben sind (falls vorhanden).

6.4 Überprüfung der Sicherheitsfunktionalitäten

6.4.1 Ziel

Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu überprüfen, ob die Sicherheitsfunktionalitäten solide sind und keine offensichtlichen Widersprüche und Lücken im Vergleich zu den bewährten Verfahren, wie sie im Schema definiert sind, bestehen.

ANMERKUNG Diese Arbeitsaufgabe des Evaluators ist das Gegenstück zur ST-Evaluierung für die Stufe „niedrig“.

6.4.2 Evaluierungsverfahren

Diese Evaluierungsarbeitsaufgabe ist eine vollständige Überprüfung der Sicherheitsvorgabe. Es ist kein Zugriff auf den TOE oder interne Dokumente erforderlich. Je nach TOE könnte der Zugriff auf öffentlich verfügbare Quellen erforderlich sein.

6.4.3 Qualifikation des Evaluators

Die Evaluatoren müssen die TOE-Domäne und die aktuellen bewährten Sicherheitsverfahren kennen. Sie müssen in der Lage sein, die Dokumentation zu überprüfen und allgemeine Quellen für bewährte Verfahren für Sicherheitsfunktionalitäten zu recherchieren.

6.4.4 Workunits der Evaluatoren – Workunit 1

Der Evaluator muss verifizieren, dass der Zweck des TOE eindeutig definiert und klar beschrieben ist.

Die Evaluatoren müssen bestätigen, dass jede in den Sicherheitsvorgaben erwähnte Sicherheitsfunktionalität den aktuellen bewährten Sicherheitsverfahren sowohl für die Domäne als auch den allgemeinen bewährten Verfahren entspricht.

ANMERKUNG Das Schema (der Entwickler) muss die bewährten Verfahren definieren, z. B. die Verwendung von Interpretationsgruppen.

Die Evaluatoren müssen bestätigen, dass die in den Sicherheitsvorgaben genannte Sicherheitsfunktionalität für die potentiellen Endkunden verständlich ist.

6.5 Entwicklungsdokumentation

6.5.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, die Entwicklungsdokumentation (ggf. einschließlich der Dokumentation des Entwicklungsprozesses) und die dem Evaluator zur Verfügung stehenden Nachweise zu beurteilen.

In einigen anderen Methodologien ist diese Arbeitsaufgabe üblicherweise die zeitaufwendigste, und Schemata sollten diese Arbeitsaufgabe mit möglichst wenig Aufwand durchführen.

6.5.2 Evaluierungsverfahren

Bei dieser Evaluierungsarbeitsaufgabe handelt es sich um eine vollständige Analyse der durch die schemaspezifische Checkliste vorgegebenen Einträge. Dies kann folgende Verifizierungen umfassen:

- der Spezifikation der Funktionalitäten des Produkts auf einer groben Ebene oder bis hin zu den genauen Schnittstellenparametern;
- der Dokumentation des Entwicklungsprozesses einschließlich Anfälligkeits- und Patchmanagement;

- der Gestaltung des Produkts auf Teilsystem- oder Modulebene;
- einer zusätzlichen Beschreibung der Sicherheitsarchitektur (Secure Boot, Selbstschutz, Domänen-trennung usw.);
- des Quellcodes.

6.5.3 Qualifikation des Evaluators

Die Evaluatoren müssen die TOE-Domäne kennen und über Erfahrung mit sicheren Entwicklungsprozessen verfügen.

6.5.4 Workunits

6.5.4.1 Workunit 1

Die Evaluatoren müssen die Vollständigkeit der Dokumentation anhand der schemaspezifischen Checkliste prüfen.

6.6 Evaluierung der TOE-Installation

6.6.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu verifizieren, dass der TOE wie im sicheren Benutzerhandbuch beschrieben installiert werden kann.

ANMERKUNG Der TOE geht möglicherweise automatisch in den sicheren Zustand über. In diesem Fall besteht das Ziel dieser Evaluierungsarbeitsaufgabe darin, zu verifizieren, dass dieser Endzustand tatsächlich der vorgesehene sichere Zustand ist.

6.6.2 Evaluierungsverfahren

Diese Evaluierungsarbeitsaufgabe ist eine vollständige Installation des TOE. Es ist kein Zugriff auf die dokumentierten Informationen außer dem sicheren Benutzerhandbuch erforderlich.

6.6.3 Qualifikation des Evaluators

Die Evaluatoren müssen die Möglichkeit haben, die Installation des TOE zu verfolgen. Das Wissen und die Fertigkeiten, die für die Installation des TOE erforderlich sind, müssen mit denen der als Endbenutzer des TOE definierten Personen vergleichbar sein. Für den Fall, dass die Installation nicht wie beschrieben funktioniert, kann von den Evaluatoren zusätzliches Fachwissen verlangt werden, um die Installation trotz der Mängel in den Leitlinien abzuschließen.

6.6.4 Workunits der Evaluatoren

6.6.4.1 Workunit 1

Die Evaluatoren müssen prüfen, ob alle Systeme, die notwendig sind, um den TOE nach dem sicheren Benutzerhandbuch zu installieren und ihn für die in der ST beschriebenen Zwecke zu benutzen, vorhanden und korrekt eingerichtet sind. Die Einrichtung dieser zusätzlichen Systeme erfolgt ggf. in Zusammenarbeit mit dem Entwickler und ist für sich genommen nicht Teil der Evaluierung. Die Evaluierung darf erst fortgesetzt werden, wenn die Einrichtung zusätzlicher Systeme, falls vorhanden, erfolgreich abgeschlossen wurde.

BEISPIEL Der TOE benötigt einen Backend-Dienst aus der Cloud. In diesem Fall muss der Entwickler dem Evaluator Prüfkonto oder eine lokale (funktionierende) Cloud-Installation zur Verfügung stellen.

Der Evaluator muss den TOE nach dem sicheren Benutzerhandbuch einrichten. Wenn das sichere Benutzerhandbuch in mehreren Sprachen vorliegt, müssen für diese Einrichtung die Leitlinien in der Sprache der ST verwendet werden.

ANMERKUNG Die Sprache der ST wird durch das Schema oder die KBS definiert.

Der Evaluator muss im ETR aufzeichnen, ob der TOE nach Abschluss der TOE-Einrichtung wie in der ST (sicherer Zustand) beschrieben arbeitet.

Wenn sich der TOE nicht im sicheren Zustand befindet, müssen die Evaluatoren ihr allgemeines Fachwissen und die übrigen Informationen (außer dem sicheren Benutzerhandbuch) verwenden, um den TOE in den sicheren Zustand zu versetzen. Die Evaluatoren müssen die zusätzlichen (oder geänderten) Schritte im Vergleich zum sicheren Benutzerhandbuch im ETR aufzeichnen.

6.6.4.2 Workunit 2

Die Evaluatoren müssen prüfen, ob das sichere Benutzerhandbuch den geltenden Schemaanforderungen entspricht (falls vorhanden).

6.6.4.3 Workunit 3

Der Evaluator muss bestimmen, wie schwer es ist, den TOE aus dem sicheren Zustand herauszubringen, oder ob dem Benutzer eine Warnung angezeigt wird, wenn sich der TOE nicht mehr im sicheren Zustand befindet.

6.7 Konformitätsprüfung

6.7.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu verifizieren, dass der TOE die in der ST gemachten funktionalen Ansprüche erfüllt.

6.7.2 Evaluierungsverfahren

Bei dieser Evaluierungsarbeitsaufgabe handelt es sich um eine Konformitätsprüfung des TOE, bei der Laborausrüstungen verwendet werden.

Der Zugriff auf schemadefinierte externe Dokumente (z. B. Normen, branchenspezifische Mindestanforderungen, Baupläne) ist erforderlich. Der Zugriff auf schemaabhängige interne Dokumente ist erforderlich. Der Zugriff auf öffentlich verfügbare Spezifikationen ist erforderlich.

ANMERKUNG Für die CSA-Stufe „hoch“ schreibt das Schema in der Regel einige zusätzliche Informationen vor, z. B. eine Architekturübersicht oder eine strukturelle Übersicht über den Aktualisierungsmechanismus.

6.7.3 Qualifikation des Evaluators

Die Evaluatoren müssen über umfangreiches Wissen über die TOE-Domäne verfügen. Sie müssen in der Lage sein, die geforderten Konformitätsprüfungen durchzuführen. Evaluatoren müssen die Fähigkeit besitzen, alle Prüfungen unabhängig vom TOE-Entwickler durchzuführen (und möglicherweise die Prüfungen zu modifizieren), auch wenn sie unter normalen Umständen Teil einer größeren Prüfreihe oder eines Tools sind.

Für jede Schnittstelle, für die keine automatisierten Tools verfügbar oder durchführbar sind, müssen die Evaluatoren über umfangreiches Wissen zu solchen Schnittstellen verfügen, die in der TOE-Domäne verwendet werden. Sie müssen in der Lage sein, komplexe Spezifikationen zu verstehen und in Prüfungen umzuwandeln.

6.7.4 Workunits der Evaluatoren

6.7.4.1 Workunit 1

Der Evaluator muss einen Prüfplan ausarbeiten. Dieser Prüfplan muss die Anforderungen des Schemas hinsichtlich Abdeckung und Tiefe bzw. Aufwand erfüllen.

ANMERKUNG 1 Das Schema kann eine vollständige Abdeckung vorschreiben, unabhängig vom erforderlichen Aufwand oder einer Art von Probenahmestrategie, in der Regel innerhalb eines zeitlich begrenzten Zeitraums.

Wenn eine risikobasierte Probenahme verwendet wird, müssen die Evaluatoren eine geeignete Probenahmestrategie unter Berücksichtigung früherer Evaluierungsergebnisse, der von der Zertifizierungsstelle erhaltenen Informationen und der Erfahrungen mit ähnlichen TOEs festlegen. Die Evaluatoren müssen außerdem die gesamte für den TOE erhaltene Dokumentation verwenden.

ANMERKUNG 2 Die Entscheidung über die Probenahmestrategie ist eine Schemaentscheidung.

Im Zusammenhang mit der Konformitätsprüfung hat der Begriff „risikobasiert“ zwei Bedeutungen:

- a) die Wahrscheinlichkeit der Nichteinhaltung, d. h. wie wahrscheinlich eine Nichteinhaltung ist (unter Verwendung des fachlichen Urteils der Evaluatoren); und
- b) die Auswirkungen einer möglichen Nichtkonformität für den TOE.

Wenn Annahmekriterien verwendet werden, muss der Evaluator für jeden Prüffall verifizieren, dass ein „Bestanden“ auch die Erfüllung des jeweiligen Annahmekriteriums impliziert.

ANMERKUNG 3 Die Strenge der Prüfung hängt von der gewählten CSA-Stufe ab und wird durch das Schema definiert.

6.7.4.2 Workunit 2

Wenn kein Prüftool vorhanden ist, müssen die gegebenen funktionalen Sicherheitsanforderungen für den TOE durch den Tester in Prüffälle übertragen werden. Ein Prüffall muss mindestens mit den folgenden Merkmalen beschrieben werden:

- Prüfbeschreibung mit Prüferwartung, Prüfvorbereitung und Prüfschritten;
- Prüfergebnis;
- Beurteilung (bestanden/nicht bestanden).

Die Prüferwartung ist das erwartete Prüfergebnis, das bei korrekter Funktion der Komponente eintritt. Die Prüferwartung muss sich aus dem vorgesehenen Verhalten der Komponente ergeben, möglicherweise unterstützt von einem Annahmekriterium. Das Prüfergebnis ist das tatsächlich festgestellte Verhalten der Komponente während der Prüfschritte.

Das Prozessmodell für die Überführung von Anforderungen in Prüffälle setzt sich aus den folgenden Schritten zusammen:

- 1) Die Sicherheitsanforderungen an den Prüfplan werden bestimmt.
- 2) Gegebenenfalls werden die entsprechenden Annahmekriterien analysiert (siehe Anhang C).
- 3) Die entsprechenden Prüffälle werden festgelegt.

Bei der Konformitätsprüfung muss untersucht werden, ob die gewählte technische Umsetzung die erwarteten Ergebnisse liefert.

6.7.4.3 Workunit 3

Die Evaluatoren müssen die festgelegten Prüfungen aus dem Prüfplan durchführen, um Nichtkonformitäten des TOE in Bezug auf die ST zu finden. Für jede im Prüfplan genannte Sicherheitsanforderung müssen die Evaluatoren die festgelegten Prüfungen durchführen und die Ergebnisse aufzeichnen. Bei jeder nicht bestandenen Konformitätsprüfung müssen die Evaluatoren die Gründe für das Nichtbestehen überprüfen und die Ergebnisse aufzeichnen.

ANMERKUNG 1 Dies könnte den Evaluator dazu veranlassen, die Prüfung mit geänderten Parametern zu wiederholen.

Wenn das Prüfergebnis mit der Prüferwartung übereinstimmt, ist die Evaluierung erfolgreich (akzeptierte Entscheidung). Wenn das Prüfergebnis von der Prüferwartung abweicht, ist die Evaluierung erfolglos (ablehnende Entscheidung).

Wenn für eine Sicherheitsanforderung kein Prüffall festgelegt werden kann, z. B. wenn ein Implementierungsdetail nicht über eine externe Schnittstelle angesprochen werden kann, muss ein alternativer Nachweis der korrekten Implementierung erbracht werden. Dies kann im Rahmen eines anderen Evaluierungsverfahrens erfolgen.

Die Evaluatoren müssen zur Erfüllung dieser Arbeitsaufgabe nach Möglichkeit validierte Tools verwenden. Wenn Tools verwendet werden, muss deren Abdeckung analysiert und gegebenenfalls zusätzliche (manuelle) Prüfungen durchgeführt werden.

ANMERKUNG 2 Weitere Details zur Validierung und Kalibrierung von Geräten können EN ISO/IEC 17025:2017, 6.4 [4] entnommen werden.

Die Evaluatoren müssen die Prüfstrategie und die Ergebnisse im ETR aufzeichnen.

6.8 Anfälligkeitsüberprüfung

6.8.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu überprüfen, ob der TOE für die bestimmungsgemäße Verwendung in der vorgesehenen Umgebung nicht durch öffentlich bekannte Schwachstellen anfällig ist.

ANMERKUNG Das Schema könnte bestimmte „vordefinierte“ Quellen für potentielle Schwachstellen definieren (z. B. für niedrigere Evaluierungsstufen).

6.8.2 Evaluierungsverfahren

Bei dieser Evaluierungsarbeitsaufgabe handelt es sich um eine Suche nach öffentlichen Schwachstellen, möglicherweise unter Verwendung der vom Schema bereitgestellten Quellen. Die Evaluatoren müssen die verfügbare Dokumentation, die sie für den TOE erhalten haben, verwenden. Es ist kein Zugriff auf interne Dokumente erforderlich.

ANMERKUNG Bei der Betrachtung von Bedrohungen mit Angriffspotential „niedrig“ berücksichtigt der Evaluator nur öffentlich bekannte Schwachstellen/Schwachstellenklassen, frühere Evaluierungsergebnisse, von der Zertifizierungsstelle erhaltene Informationen und Erfahrungen mit ähnlichen TOEs.

6.8.3 Qualifikation des Evaluators

Die Evaluatoren müssen die TOE-Domäne kennen. Sie müssen in der Lage sein, Schwachstellenbeschreibungen zu überprüfen, um festzustellen, ob sie auf einen TOE zutreffen. Wenn keine vordefinierten Quellen durch das Schema vorgeschrieben sind, müssen sie in der Lage sein, effizient nach öffentlichen Schwachstellen in einer Vielzahl von Quellen zu suchen. Falls Nachweise aus dem Entwicklungsprozess vorhanden sind, müssen die Evaluatoren in der Lage sein, diese Nachweise zu überprüfen.

6.8.4 Workunits der Evaluatoren

6.8.4.1 Workunit 1

Wenn das Schema einen vordefinierten Satz von Quellen für Schwachstellen vorsieht, muss der Evaluator auf der Grundlage der ST diejenigen potentiellen Schwachstellen auswählen, die technisch auf den TOE zutreffen könnten.

Andernfalls müssen die Evaluatoren nach Schwachstellen suchen, indem sie die verfügbaren (öffentlichen und proprietären) Nachweise, einschließlich der ST, unter Berücksichtigung der TOE-Technologie analysieren.

Der Evaluator muss überprüfen, ob die ermittelten Schwachstellen auf den TOE zutreffen.

ANMERKUNG 1 Die Überprüfung kann durch den Vergleich von Versionsnummern von TOE-Teilen (z. B. Bibliotheken), die Prüfung auf Gegenmaßnahmen gegen die ermittelten Schwachstellen (z. B. zusätzliche Softwareteile wie Filter) oder einige begrenzte Prüfungen durchgeführt werden.

ANMERKUNG 2 Es werden hier nur Angriffe betrachtet, die in der in der ST festgelegten Betriebsumgebung möglich sind (einschließlich Annahmen über bestehende Maßnahmen).

6.8.4.2 Workunit 2

Diese Workunit ist nur anwendbar, wenn Nachweise aus dem Entwicklungsprozess vorhanden sind.

Die Evaluatoren müssen die verfügbare Dokumentation, die sie für den TOE erhalten haben, verwenden. Das Dokumentenbündel sollte Folgendes umfassen:

- Berichte über Schwachstellenscans, die nicht älter als drei Monate sind;
- Maßnahmen zur Behebung von Schwachstellen (zumindest ein Beispiel), die den internen Leitlinien der Organisation für die Handhabung von Schwachstellen beigelegt und in denen die Fristen für die Behebung klar angegeben sind;
- Risikomanagementanalyse, die mindestens 12 Monate vor der Evaluierung abdeckt. Das Dokument würde eindeutige Kennzeichnungen zur Versionsverfolgung tragen, um die Entwicklung des Dokuments widerzuspiegeln.

Zusätzliche relevante Dokumente können von den Evaluatoren angefordert werden, um die Einhaltung der im Zertifizierungsschema festgelegten Sicherheitsnormen durch den TOE zu festigen. Diese Evaluierungsarbeitsaufgabe kann auch eine Suche nach öffentlichen Schwachstellen unter Verwendung der vom Schema bereitgestellten Quellen beinhalten.

6.9 Anfälligkeitsprüfung

6.9.1 Ziel

Das Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu verifizieren, dass der TOE für die bestimmungsgemäße Verwendung in der vorgesehenen Umgebung nicht durch öffentlich bekannte Schwachstellen anfällig ist.

ANMERKUNG Das Schema könnte bestimmte „vordefinierte“ Quellen für potentielle Schwachstellen definieren (z. B. für niedrigere Evaluierungsstufen).

6.9.2 Evaluierungsverfahren

Bei dieser Evaluierungsarbeitsaufgabe handelt es sich um eine Suche nach öffentlichen Schwachstellen, möglicherweise unter Verwendung der vom Schema bereitgestellten Quellen. Die Evaluatoren müssen die verfügbare Dokumentation, die sie für den TOE erhalten haben, verwenden. Es ist kein Zugriff auf interne Dokumente erforderlich.

ANMERKUNG Bei der Betrachtung von Bedrohungen mit Angriffspotential „niedrig“ berücksichtigt der Evaluator nur öffentlich bekannte Schwachstellen/Schwachstellenklassen, frühere Evaluierungsergebnisse, von der Zertifizierungsstelle erhaltene Informationen und Erfahrungen mit ähnlichen TOEs.

6.9.3 Qualifikation des Evaluators

Die Evaluatoren müssen die TOE-Domäne kennen. Sie müssen in der Lage sein, die geforderten Prüfungen durchzuführen. Wenn keine vordefinierten Prüfungen vorhanden sind, muss der Evaluator in der Lage sein, Prüfungen für die Schwachstellen zu entwickeln. Wenn keine vordefinierten Quellen durch das Schema vorgeschrieben sind, müssen sie in der Lage sein, effizient nach öffentlichen Schwachstellen in einer Vielzahl von Quellen zu suchen. Falls Nachweise aus dem Entwicklungsprozess vorhanden sind, müssen die Evaluatoren in der Lage sein, diese Nachweise zu überprüfen.

6.9.4 Workunits der Evaluatoren

6.9.4.1 Workunit 1

Wenn das Schema einen vordefinierten Satz von Quellen für Schwachstellen vorsieht, muss der Evaluator auf der Grundlage der ST diejenigen potentiellen Schwachstellen auswählen, die technisch auf den TOE zutreffen könnten.

Andernfalls müssen die Evaluatoren nach Schwachstellen suchen, indem sie die verfügbaren (öffentlichen und proprietären) Nachweise, einschließlich der ST, unter Berücksichtigung der TOE-Technologie analysieren.

ANMERKUNG Es werden hier nur Angriffe betrachtet, die in der in der ST festgelegten Betriebsumgebung möglich sind (einschließlich Annahmen über bestehende Maßnahmen).

6.9.4.2 Workunit 2

Der Evaluator muss einen Prüfplan ausarbeiten. Dieser Prüfplan muss die Anforderungen des Schemas hinsichtlich Abdeckung und Tiefe bzw. Aufwand erfüllen.

ANMERKUNG 1 Das Schema kann eine vollständige Abdeckung vorschreiben, unabhängig vom erforderlichen Aufwand oder einer Art von Probenahmestrategie, in der Regel innerhalb eines zeitlich begrenzten Zeitraums.

Wenn eine risikobasierte Probenahme verwendet wird, müssen die Evaluatoren eine geeignete Probenahmestrategie unter Berücksichtigung früherer Evaluierungsergebnisse, der von der Zertifizierungsstelle erhaltenen Informationen und der Erfahrungen mit ähnlichen TOEs festlegen. Die Evaluatoren müssen außerdem die gesamte für den TOE erhaltene Dokumentation verwenden.

Im Zusammenhang mit der Anfälligkeitsprüfung hat der Begriff „risikobasiert“ zwei Bedeutungen:

- a) die Wahrscheinlichkeit einer Schwachstelle, d. h. wie wahrscheinlich eine solche Schwachstelle ist (unter Verwendung des fachlichen Urteils der Evaluatoren); und
- b) die Auswirkungen einer möglichen Schwachstelle für die Sicherheitsmaßnahmen des TOE.

ANMERKUNG 2 Die Entscheidung über die Probenahmestrategie ist eine Schemaentscheidung.

ANMERKUNG 3 Die Strenge der Prüfung hängt von der gewählten CSA-Stufe ab und muss durch das Schema definiert werden.

ANMERKUNG 4 Diese Workunit bietet nur eine eingeschränkte Probenahmestrategie. Für die CSA-Stufe „hoch“ und wenn eine weitere Vertrauenswürdigkeit erforderlich ist, steht die Evaluierungsarbeitsaufgabe „Penetrationstest“ zur Verfügung (als Ersatz).

6.9.4.3 Workunit 3

Für jede aufgeführte potentielle Schwachstelle, die ausgewählt wird, müssen die Evaluatoren eine oder mehrere Prüfungen erstellen.

ANMERKUNG Es werden hier nur Angriffe betrachtet, die in der in der ST festgelegten Betriebsumgebung möglich sind (einschließlich Annahmen über bestehende Maßnahmen).

Ein Prüffall muss mindestens mit den folgenden Merkmalen beschrieben werden:

- Prüfbeschreibung mit Prüferwartung, Prüfvorbereitung und Prüfschritten;
- Prüfergebnis;
- Beurteilung (bestanden/nicht bestanden).

Die Prüferwartung ist das erwartete Prüfergebnis, das bei korrekter Funktion der Komponente eintritt, d. h. die Schwachstelle nicht vorhanden ist. Die Prüferwartung muss sich aus dem vorgesehenen Verhalten der Komponente ergeben. Das Prüfergebnis ist das tatsächlich festgestellte Verhalten der Komponente während der Prüfschritte.

Bei der Anfälligkeitsprüfung muss untersucht werden, ob die gewählte technische Umsetzung nicht anfällig für bekannte potentielle Schwachstellen ist.

6.9.4.4 Workunit 4

Für jeden im Prüfplan genannten Prüffall müssen die Evaluatoren Prüfungen durchführen und die Ergebnisse aufzeichnen.

Die Evaluatoren müssen zur Erfüllung dieser Arbeitsaufgabe nach Möglichkeit validierte Tools verwenden. Wenn Tools verwendet werden, muss deren Abdeckung analysiert und gegebenenfalls zusätzliche (manuelle) Prüfungen durchgeführt werden.

Wenn das Prüfergebnis mit der Prüferwartung übereinstimmt, ist die Evaluierung positiv (bestanden). Wenn das Prüfergebnis abweicht, ist die Evaluierung negativ (nicht bestanden).

Bei jeder nicht bestandenen Anfälligkeitsprüfung müssen die Evaluatoren die Auswirkungen des Nichtbestehens überprüfen. Wenn die Auswirkungen nicht aus den Prüfergebnissen abgeleitet werden können, muss der Evaluator das entsprechende Angriffspotential berechnen.

ANMERKUNG Dies könnte den Evaluator dazu veranlassen, die Prüfung mit geänderten Parametern zu wiederholen.

Die Evaluatoren müssen die Prüfstrategie und die Ergebnisse im ETR aufzeichnen.

6.9.4.5 Workunit 5

Diese Workunit ist nur anwendbar, wenn Nachweise aus dem Entwicklungsprozess vorhanden sind.

Die Evaluatoren müssen die verfügbare Dokumentation, die sie für den TOE erhalten haben, verwenden. Das Dokumentenbündel sollte Folgendes umfassen:

- Berichte über Schwachstellenscans, die nicht älter als drei Monate sind;
- Maßnahmen zur Behebung von Schwachstellen (zumindest ein Beispiel), die den internen Leitlinien der Organisation für die Handhabung von Schwachstellen beigelegt und in denen die Fristen für die Behebung klar angegeben sind;
- Risikomanagementanalyse, die mindestens 12 Monate vor der Evaluierung abdeckt. Das Dokument würde eindeutige Kennzeichnungen zur Versionsverfolgung tragen, um die Entwicklung des Dokuments widerzuspiegeln.

Zusätzliche relevante Dokumente können von den Evaluatoren angefordert werden, um die Einhaltung der im Zertifizierungsschema festgelegten Sicherheitsnormen durch den TOE zu festigen. Diese Evaluierungsaufgabe kann auch eine Suche nach öffentlichen Schwachstellen unter Verwendung der vom Schema bereitgestellten Quellen beinhalten.

6.10 Penetrationstest

6.10.1 Ziel

Das Ziel dieser Evaluierungsaufgabe ist die Durchführung einer Probenahmeprüfstrategie auf der Grundlage der Methodologie der Mängelhypothese, dass der TOE keine Schwachstellen aus der Klasse der bekannten Schwachstellen enthält.

ANMERKUNG Diese Evaluierungsaufgabe ist eine Obermenge der Arbeitsaufgabe „Anfälligkeitsprüfung“.

6.10.2 Evaluierungsverfahren

6.10.2.1 Allgemeines

Diese Evaluierungsaufgabe ist ein Penetrationstest des TOE. Sie basiert auf Erfahrungen mit ähnlichen Produkten/Technologien und Bedrohungsanalysen und verwendet Verfahren wie Angriffsbäume und eine Suche nach öffentlich bekannten Anfälligkeiten. Der Zugriff auf schemadefinierte allgemeine Informationen über die TOE-Domäne ist erforderlich. Der Zugriff auf schemadefinierte interne Dokumente kann erforderlich sein. Je nach TOE könnte ein Zugriff auf öffentlich verfügbare Spezifikationen erforderlich sein.

ANMERKUNG Für die CSA-Stufe „hoch“ schreibt das Schema in der Regel einige zusätzliche Informationen vor, z. B. eine Architekturübersicht oder eine strukturelle Übersicht über den Aktualisierungsmechanismus.

6.10.2.2 Methodologie der Mängelhypothese

Die Methodologie der Mängelhypothese ist ein allgemeines Konzept zur Anfälligkeitsbewertung.

Das Konzept besteht aus mehreren Hauptschritten:

- 1) Der Evaluator erfasst zunächst die für die Sicherheit des TOE relevanten Informationen. Dazu gehören die verfügbare Entwicklerdokumentation, aber auch Nachweise, die vom Evaluator selbst während früherer Evaluierungsaufgaben erstellt wurden, sowie andere Informationsquellen wie z. B.:

- öffentliche Schwachstellen, die auf das Produkt zutreffen;
 - unerwartetes Verhalten des Produkts während der Konformitätsprüfungen;
 - Inkonsistenzen, die bei der Analyse der Sicherheitsvorgaben entdeckt wurden;
 - relevante Informationen umfassen den Stand der Technik für Technologien von Produkttypen, die mit dem TOE in Verbindung stehen:
 - öffentlicher akademischer Stand der Technik oder Normen;
 - Leitlinien oder Anforderungen aus dem Schema.
- 2) Der Evaluator stellt Hypothesen über Mängel des zu prüfenden Produkts auf. Da der Evaluator unmöglich alle möglichen Angriffe auf das Produkt prüfen kann, muss er:
- Angriffe ausschließen, von denen bereits bekannt ist, dass sie zu viel Aufwand erfordern, um berücksichtigt zu werden (die Aufwandsabschätzung stützt sich in der Regel auf die Berechnung des Angriffspotentials);
 - Angriffe ausschließen, die aufgrund des in den Sicherheitsvorgaben definierten Kontexts nicht möglich sind (z.B. werden physische Angriffe nicht bewertet, wenn eine Annahme in den Sicherheitsvorgaben besagt, dass das Produkt nur von vertrauenswürdigen Benutzern physisch erreicht werden kann);
 - die verbleibenden Angriffsszenarien priorisieren, um zu beurteilen, ob tatsächlich Schwachstellen vorhanden sind (der Evaluator kann sich z.B. dafür entscheiden, zuerst die Schwachstellen zu prüfen, die leichter auszunutzen sind, oder Schwachstellen, von denen angenommen wird, dass sie in der zu evaluierenden Produktfamilie häufiger auftreten).
- 3) Falls erforderlich, führt der Evaluator tatsächliche Penetrationstests durch, um das Angriffspotential, das zur Ausnutzung der Mängel erforderlich ist, weiter zu charakterisieren („Ausnutzung“ bedeutet hier „Verwendung des Mangels zur Gefährdung des Wirtschaftsgutes oder Realisierung einer Bedrohung, wie sie in den Sicherheitsvorgaben definiert sind“). Die Ergebnisse der Prüfung können erneut als Nachweis verwendet werden (siehe Schritt 1), um die Hypothesen zu aktualisieren und den Prüfplan in einer Feedbackschleife neu auszurichten.
- 4) Der Evaluator fasst schließlich seine Ergebnisse zusammen, indem er die Angriffsszenarien, die er für das Produkt für anwendbar hält, sowie deren Kosten in Bezug auf das Angriffspotential beschreibt.

Es wird nicht erwartet, dass die Evaluatoren jeden dieser Schritte strikt befolgen, aber sie sollten in der Lage sein zu zeigen, dass ihr angewandtes Konzept gleichwertig ist. Darüber hinaus können Zertifizierungsprogramme die Methodologie weiter präzisieren, insbesondere bei der Betrachtung einer kleineren Teilmenge von Produkttypen.

BEISPIEL Das JIL-Dokument [13] ist ein Beispiel für eine solche Einschränkung.

6.10.3 Qualifikation des Evaluators

Die Evaluatoren müssen in der Lage sein, die erforderlichen Angriffe auszuführen; sie müssen über umfangreiches Wissen über die TOE-Domäne verfügen. Sie müssen in der Durchführung von Penetrationstests geübt sein.

6.10.4 Workunits der Evaluatoren

6.10.4.1 Workunit 1

Die Evaluatoren müssen versuchen, die Sicherheitsfunktionalität des TOE zu umgehen oder zu brechen. Dazu müssen die Evaluatoren eine risikobasierte Probenahmestrategie in Anlehnung an die Methodologie der Mängelhypothese aufstellen und dabei öffentlich bekannte Schwachstellen/Schwachstellenklassen, frühere Evaluierungsergebnisse, von der Zertifizierungsstelle erhaltene Informationen und die Erfahrungen mit ähnlichen TOEs berücksichtigen. Die Evaluatoren müssen außerdem die gesamte für den TOE erhaltene Dokumentation verwenden.

ANMERKUNG 1 Umgehen bedeutet nicht, dass der Code zur Umgehung der Sicherheitsfunktionalität tatsächlich bereitgestellt wird. Es genügt der Nachweis, dass ein solcher Code mit einem Aufwand bereitgestellt werden könnte, der den zu erwartenden Fähigkeiten der Bedrohungsagenten (nach definiertem Angriffspotential) angemessen ist.

Die Evaluatoren müssen im ETR Folgendes aufzeichnen:

- die Pentesting-Strategie; und
- tatsächlich durchgeführte Prüfungen.

ANMERKUNG 2 Der Umfang und das Ausmaß der Penetrationstests hängt von der Stufe ab und muss vom Schema weiter präzisiert werden.

6.10.4.2 Workunit 2

Wenn der Evaluator eine potentielle Schwachstelle entdeckt hat, die an sich nicht ausgenutzt werden kann, der Evaluator aber der Meinung ist, dass eine solche Schwachstelle mit mehr Aufwand als in der Probenstrategie vorgesehen entwickelt werden könnte, muss der Evaluator eine Experteneinschätzung des zu erwartenden Aufwands im ETR erstellen.

Zusätzlich muss der Evaluator im ETR jede aufgeführte potentielle Schwachstelle und das Urteil des Evaluators über die Ausnutzbarkeit und Anwendbarkeit auf das Produkt aufzeichnen.

ANMERKUNG 1 Von den Evaluatoren wird nicht verlangt, dass sie die Sicherheitsfunktionalität tatsächlich umgehen, da die Entwicklung von Exploits kostspielig ist. Es reicht aus, basierend auf der Erfahrung des Evaluators (und der schemaspezifischen Leitlinien) den Aufwand abzuschätzen, der zur Umgehung erforderlich ist.

Wenn der Evaluator eine potentielle Schwachstelle entdeckt hat, die an sich nicht ausgenutzt werden kann, der Evaluator aber der Meinung ist, dass eine solche Schwachstelle mit mehr Aufwand als in der Pentesting-Strategie vorgesehen entwickelt werden könnte, muss der Evaluator eine sachverständige Beurteilung des zu erwartenden Aufwands im ETR bereitstellen.

ANMERKUNG 2 Der Umfang und das Ausmaß der Penetrationstests hängt vom Angriffspotential ab und muss vom Schema weiter präzisiert werden.

6.11 Grundlegende Kryptoanalyse

6.11.1 Ziel

Ziel dieser Evaluierungsaufgabe ist es, zu validieren, ob die vom TOE implementierte Kryptographie (z. B. Techniken, Verfahren und Dienste) mit den kryptographischen Spezifikationen des Antragstellers und den Leitlinien des Schemas übereinstimmt.

6.11.2 Evaluierungsverfahren

Bei dieser Arbeitsaufgabe handelt es sich um eine probabilistische Konformitätsprüfung, die auf kryptographische Protokolle und Algorithmen zugeschnitten ist. Dazu muss der Evaluator eine kryptographische Spezifikation erhalten.

ANMERKUNG 1 Der Schwerpunkt dieser Workunit liegt auf Konformitätsprüfungen, siehe 6.12.4.2 in Bezug auf die Probenahme.

ANMERKUNG 2 Die kryptografische Spezifikation kann Teil der ST sein.

6.11.3 Qualifikation des Evaluators

Die Evaluatoren benötigen ein fundiertes Wissen über die Kryptographie und die kryptographischen Anforderungen des Schemas. Die Evaluatoren müssen in der Erstellung von Prüfungen für kryptographische Protokolle und Algorithmen geübt sein.

6.11.4 Workunits der Evaluatoren

6.11.4.1 Workunit 1

Die Evaluatoren müssen versuchen, Nichtkonformitäten des TOE in Bezug auf die vom Schema vorgeschriebenen kryptographischen Anforderungen zu finden. Zu diesem Zweck müssen die Evaluatoren eine risikobasierte Probenahmestrategie unter Berücksichtigung früherer Evaluierungsergebnisse, der von der Zertifizierungsstelle erhaltenen Informationen und der Erfahrungen mit ähnlichen TOEs aufstellen. Die Evaluatoren müssen außerdem die gesamte für den TOE erhaltene Dokumentation sowie die Schemadokumente im Hinblick auf die Kryptographie verwenden.

Im Zusammenhang mit der Konformitätsprüfung hat der Begriff „risikobasiert“ zwei Bedeutungen:

- a) Die Wahrscheinlichkeit der Nichteinhaltung, d. h. wie wahrscheinlich eine Nichteinhaltung ist (unter Verwendung des fachlichen Urteils der Evaluatoren); und
- b) Die Auswirkungen einer möglichen Nichtkonformität für den TOE.

Die Evaluatoren müssen zur Erfüllung dieser Arbeitsaufgabe nach Möglichkeit validierte Tools verwenden.

BEISPIEL Wenn Eigenschaften auf einer Schnittstelle als zufällig behauptet werden, kann ein geeignetes Tool prüfen, ob offensichtliche Defekte im Zufallszahlengenerator oder Prozessor vorliegen.

Positive Prüffälle für kryptografische Algorithmen und Schemata sollten zufällig generierte Tests mit bekannten Antworten und ggf. iterierte Monte-Carlo-Tests umfassen. Die Prüfvektoren sollten von einer unabhängigen, bekanntermaßen guten Implementierung generiert oder verifiziert werden und nicht statisch sein. Algorithmen, die Eingaben mit variabler Länge akzeptieren, sollten mit Eingaben unterschiedlicher Länge (einschließlich Eckfällen wie Länge Null) geprüft werden.

Negative Prüffälle für kryptografische Algorithmen und Schemata sollten so gestaltet sein, dass sie bestimmte Fehlerzustände auslösen (z. B. unzulässige Wertefehler, Fehler außerhalb des zulässigen Bereichs, Padding-Fehler usw.).

Positive Prüfungen von kryptographischen Protokollen können durch Kommunikation mit einer unabhängigen, bekanntermaßen guten Implementierung durchgeführt werden. Die vom Protokoll verwendeten kryptografischen Algorithmen und Schemata sollten wie oben beschrieben separat geprüft werden.

Negative Prüfungen von kryptographischen Protokollen sollten Prüffälle für nicht spezifizierte Konfigurationen (nicht spezifizierte Chiffren, Downgrade der Protokollversion usw.), Prüffälle für unzulässige Eingaben (z. B. beschädigte Pakete, übergroße Pakete usw.) und Prüffälle für unzulässige Übergänge in der Protokollzustandsmaschine (z. B. Einfügen unerwarteter Pakete, Auslassen erforderlicher Pakete usw.) umfassen.

Zufällige Quellen sollten mit einer statistischen Prüfreihe geprüft werden.

Die Evaluatoren müssen die Prüfstrategie und die Ergebnisse im ETR aufzeichnen. Wenn bestimmte Algorithmen, Schnittstellen oder kryptographische Funktionen während der Probenahme nicht analysiert wurden, müssen die Evaluatoren eine Begründung dafür liefern.

6.12 Erweiterte Kryptoanalyse

6.12.1 Ziel

Ziel dieser Evaluierungsarbeitsaufgabe ist es, zu verifizieren, dass die verwendete Kryptografie mit der vom Antragsteller bereitgestellten kryptografischen Spezifikation und dem Stand der Technik der Kryptografie, wie er im Schema definiert ist, übereinstimmt. Sie besteht aus der Verifizierung des Mechanismus (richtige Auswahl) und der Verifizierung der Implementierung (Überprüfung auf Fehler in der Implementierung).

Der Schemaentwickler legt fest, welcher Stand der Technik vom Evaluator berücksichtigt werden sollte (z. B. SOG-IS Crypto [14], französisch RGS [9], deutsch TR 02102 [10], CCN-STIC 807 [11]).

6.12.2 Evaluierungsverfahren

Die Arbeitsaufgabe besteht aus zwei Schritten: Eine theoretische Analyse auf der Grundlage der zur Verfügung gestellten Dokumente und eine Verifizierung sowie eine Anfälligkeitsanalyse auf der Basis der Implementierung und des TOE.

Die theoretische Analyse stützt sich hauptsächlich auf das zur Verfügung gestellte Dokument. Ihr Ziel ist es, alle Anfälligkeiten in den kryptographischen Mechanismen zu erkennen, die zur Erreichung der Sicherheitsziele des Produkts in seiner Betriebsumgebung verwendet werden. Im Fall von kryptografischen Diensten muss die Widerstandsfähigkeit dieser Mechanismen in ihrem Nutzungskontext analysiert werden.

Der zweite Schritt besteht aus einer Verifizierung der Konformität der Implementierung für alle verwendeten kryptographischen Algorithmen und einer Anfälligkeitsanalyse des Quellcodes.

Dazu muss der Evaluator über das im ersten Schritt verwendete Dokument der kryptographischen Spezifikation und den Quell- oder Pseudocode der kryptographischen Routinen oder Funktionen (ggf. einschließlich der Aufrufparameter) verfügen. Wenn die Kryptographie in Hardware ausgeführt wird, sind die Hardwarespezifikationen (Schaltpläne) das Äquivalent zum Quellcode.

ANMERKUNG Der Schwerpunkt dieser Workunit liegt auf der unabhängigen Analyse, die über die Konformitätsprüfung von 6.12 hinausgeht. Bezüglich der Probenahme wird auf 6.13.4.1 verwiesen.

6.12.3 Qualifikation des Evaluators

Die Evaluatoren benötigen ein fundiertes Wissen über die Kryptographie und die kryptographischen Anforderungen des Schemas. Die Evaluatoren müssen die Analyse der Darstellung der Implementierung und die Erstellung von Prüfungen für kryptographische Protokolle und Algorithmen beherrschen.

6.12.4 Workunits der Evaluatoren

6.12.4.1 Workunit 1

Der Evaluator muss zunächst prüfen, ob die Dokumente, die zur Durchführung der Analyse geliefert wurden, mit den anderen Dokumenten, die zur Evaluierung des Produkts bereitgestellt wurden, übereinstimmen.

Der Evaluator muss die Spezifikation aller folgenden Arten von Mechanismen des TOE entsprechend dem für die Evaluierung gewählten Stand der Technik analysieren:

- 1) kryptografische Algorithmen, Funktionsweisen und Relevanz in Bezug auf die Ziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Leistung usw.);
- 2) kryptographische Protokolle, die darauf ausgelegt sind, die erwartete Sicherheitsfunktionalität zu erreichen;
- 3) Verfahren und Mechanismen zur Schlüsselerzeugung und Schlüsselverwaltung.

Zusätzlich muss der Evaluator auf der Grundlage der (Entwickler-)Beschreibung des Zufallszahlengenerators (RNG, en: random number generator) den Typ des RNG identifizieren, z. B. ob es sich um einen deterministischen RNG, einen physikalischen RNG mit/ohne kryptographischen Nachbearbeitungsalgorithmus oder einen nicht-physikalischen echten RNG handelt. Für deterministische RNGs (falls zutreffend) kann der Evaluator die Konformität oder eine teilweise Konformität mit den Empfehlungen der RNGs im angewandten Schema bestätigen.

Der Evaluator muss einen Analysebericht erstellen, in dem alle festgestellten potentiellen Schwachstellen oder Anfälligkeiten angegeben werden müssen. Der Evaluator kann Empfehlungen bezüglich des Einsatzes von Kryptographie aussprechen (z. B. ob Mechanismen bald durch bessere ersetzt werden könnten).

6.12.4.2 Workunit 2

Der Evaluator muss die Ergebnisse der vorangegangenen Analyse (falls zutreffend) berücksichtigen, um die Konformität der Implementierung zu verifizieren und nach möglichen Anfälligkeiten zu suchen. Der Evaluator muss feststellen, ob diese Schwachstellen in der Betriebsumgebung des Produkts tatsächlich ausgenutzt werden können. Die Analyse deckt Folgendes ab:

- Konformität der Kryptographie-Implementierung (auch für den Zufallszahlengenerator); die Form dieser Analyse hängt von den verfügbaren Nachweiselementen ab;
- Anfälligkeitsanalyse der Kryptographie-Implementierung (Lässt die Implementierung des Algorithmus unabhängig von seiner intrinsischen Resistenz Angriffe zu, die möglicherweise die Sicherheitszielsetzungen des TOE beeinträchtigen?).

Die Analyse erfolgt durch eine Prüfung und Quellcode-Analyse.

Sie enthält drei Hauptarbeitsaufgaben:

- 1) Die Evaluatoren müssen die Implementierungsdarstellung untersuchen, um festzustellen, ob die Implementierung mit dem in Workunit 1 verwendeten Dokument der kryptographischen Spezifikation konform ist.
- 2) Die Evaluatoren müssen für alle implementierten kryptographischen Mechanismen, die im System verwendet werden, Konformitätsprüfungen (Monte-Carlo-Test, Known-Answer-Tests (KAT) usw.) durchführen, um festzustellen, ob sie durch die Implementierung korrekt implementiert werden.

- 3) Der Evaluator muss eine Quellcodeanalyse durchführen und feststellen, ob die gefundenen Schwachstellen in der Betriebsumgebung des Produkts tatsächlich ausgenutzt werden können. Je nach Art der geforderten Analyse und in Anbetracht der Tatsache, dass der Evaluator nur über begrenzte Zeit verfügt, müsste der Evaluator wahrscheinlich auswählen, welche Schwachstellen untersucht werden sollen.

Zu diesem Zweck müssen die Evaluatoren eine risikobasierte Probenahmestrategie unter Berücksichtigung früherer Evaluierungsergebnisse, der von der Zertifizierungsstelle erhaltenen Informationen und der Erfahrungen mit ähnlichen TOEs festlegen. Die Evaluatoren müssen außerdem die gesamte für den TOE erhaltene Dokumentation sowie die Schemadokumente im Hinblick auf die Kryptographie verwenden.

Im Zusammenhang mit der Konformitätsprüfung hat der Begriff „risikobasiert“ zwei Bedeutungen:

- a) die Wahrscheinlichkeit der Nichteinhaltung, d. h. wie wahrscheinlich eine Nichteinhaltung ist (unter Verwendung des fachlichen Urteils der Evaluatoren); und
- b) die Auswirkungen einer möglichen Nichtkonformität für den TOE.

Die Evaluatoren müssen die Implementierungsdarstellung untersuchen, um festzustellen, ob die Implementierung mit der kryptographischen Spezifikation konform ist.

Wenn das Schema Anforderungen für sichere Kodierung enthält, muss der Evaluator die Darstellung der Implementierung untersuchen, um festzustellen, ob sie die Leitlinien für sichere Kodierung einhält.

Die Evaluatoren können automatisierte Tools verwenden, um die menschliche Analyse zu erleichtern (z. B. statische/dynamische Programmanalyse-Tools).

Die Evaluatoren müssen die Analyse der Darstellung der Implementierung durch geeignete Konformitätsprüfungen, wie in 6.7 festgelegt, ergänzen.

Die Evaluatoren müssen die Prüfstrategie und die Ergebnisse im ETR aufzeichnen. Wenn bestimmte Algorithmen, Schnittstellen oder kryptographische Funktionen während der Probenahme nicht analysiert wurden, müssen die Evaluatoren eine Begründung dafür liefern.

Wenn bei der vorangegangenen Analyse Empfehlungen zur Verwendung eines kryptografischen Dienstes ausgesprochen wurden, muss der Evaluator überprüfen, ob diese Empfehlungen in den Produktnutzungs- und/oder Administrationshandbüchern deutlich angegeben sind.

Anhang A (informativ)

Beispiel für die Struktur einer Sicherheitsvorgabe

A.1 Allgemeines

Der genaue Inhalt und Aufbau einer Sicherheitsvorgabe (ST) sollte durch das Schema präzisiert werden. Dieser Anhang fasst eine typische Gliederung einer ST zusammen und kann als Ausgangspunkt für Schemata verwendet werden.

Bei der Entwicklung der Anforderungen an das Schema sollte darauf geachtet werden, dass dem Entwickler möglichst wenig Aufwand auferlegt wird. Eine typische ST sollte für Entwickler „einfach“ zu erstellen sein. Sie sollte flexibel bleiben, kann aber bei Bedarf auch an die Domäne des Schemas angepasst werden.

Eine ST, die auf die CSA-Vertrauenswürdigkeitsstufe „niedrig“ abzielt, kann im Schema sogar noch weiter reduziert werden.

A.2 Beispiel für die Struktur

Eine typische ST kann die folgenden Abschnitte haben.

- 1) Einleitung
 - a) Kontext dieses Dokuments
 - b) Produktidentifikation
 - c) Verweisung/Akronyme
- 2) Produktbeschreibung
 - a) Allgemeine Beschreibung
 - b) Merkmale
 - c) Produktverwendung
 - d) Betriebsumgebung
- 3) Sicherheitsperimeter
 - a) Benutzer
 - b) Annahmen
 - c) Vermögenswerte
 - d) Bedrohungsmodell: Bedrohungsagenten und Bedrohungen
 - e) Sicherheitsfunktionen
 - f) Begründung
- 4) Grenzen der Evaluierung