Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B1, Version 2.0.1

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

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

Änderungshistorie

Version	*Datum*	*Herausgeber*	*Beschreibung*
2.0.1	01.03.2024	SZ 33	Deutsche Erstausgabe

Tabelle 1: Änderungshistorie

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

Inhalt

1 Hintergrund

1 Das Dokument Sicherheitsvorgaben (Englisch: Security Target, ST) beschreibt die Sicherheitsfunktionalität, die Schnittstellen, das Bedrohungsmodell und die (erwartete) Umgebung des Evaluierungsgegenstands (Englisch: Target of Evaluation, TOE). Dabei soll die im ST enthaltene Struktur und der erfasste Inhalt dem Kapitel 3 von diesem Dokument folgen. Das BSI veröffentlicht das ST zusammen mit der Ausstellung des Zertifikats. Aus diesem Grund ist es ratsam, eine finale Version des ST ohne eine Versionshistorie sowie ohne Informationen, die nicht für eine Veröffentlichung bestimmt sind, zu erstellen. Das Dokument muss im Einklang mit den für die Publikation geltenden und auf der BSI-Webseite veröffentlichten Anforderungen zur Barrierefreiheit stehen. Grundsätzlich müssen alle personenbezogenen Metadaten aus der finalen PDF-Version des Dokuments entfernt werden. Darüber hinaus sollte das Dokument gemäß den entsprechenden deutschen Vorschriften zur Barrierefreiheit [BITV 2.0] erstellt werden. Die Release-Version darf keine Änderungsmarkierungen aufweisen. Falls kryptographische Mechanismen Bestandteil der Sicherheitsfunktionalität sind, müssen diese gemäß Kapitel 4 in der kryptographischen Spezifikation aufgenommen werden. Wenn die kryptographische Spezifikation nicht zusammen mit dem ST veröffentlicht werden soll, kann sie in einem gesonderten Dokument bereitgestellt werden.

2 Spezifische Geltungsbereiche der BSZ beinhalten zusätzliche Anforderungen an den Inhalt für das ST.

3 Sämtliche im ST verwendeten Fachbegriffe, die nicht selbsterklärend sind, müssen definiert werden. Diese Definitionen können im Hauptteil oder durch Verweise auf zuverlässige und zugängliche öffentliche Quellen angegeben werden.

4 Bei der Beschreibung ist nach Möglichkeit auf unternehmensspezifische Terminologie zu verzichten. Sollten dennoch bestimmte unternehmensspezifische Fachbegriffe verwendet werden, muss für diese eine kurze Erläuterung bereitgestellt werden.

5 Wenn ein Produkt in einem vorherigen BSZ-Verfahren evaluiert wurde, besteht die Möglichkeit, den Evaluationsaufwand für ein neues BSZ-Verfahren zu reduzieren. Die Antragstellerin muss hierfür eine Änderungsbeschreibung mit Auswirkungsanalyse (Englisch: Impact Analysis Report, IAR) vorlegen, in der die Änderungen am TOE sowie die Änderungen an allen für die Zertifizierung relevanten Dokumenten beschrieben werden. Der IAR muss der im Kapitel 5 dargestellten Struktur folgen und die entsprechenden Inhalte bereitstellen.

6 Ein Softwarestückliste (Englisch: Software Bill of Materials, SBOM) ist eine Liste von Softwarekomponenten. Eine SBOM enthält Informationen zu den Elementen (z. B. Bibliotheken), die vom Hersteller selbst bereitgestellt werden, von Dritten erstellt wurden oder Open-Source-Softwarekomponenten sind. Daher ist eine SBOM ein wichtiges Instrument für die transparente Darstellung der Zusammensetzung der Software. Sie kann automatisch erstellt werden und sollte in Form einer maschinenlesbaren Datei vorgelegt werden. Die Anforderungen an den Inhalt der SBOM sind in Kapitel 6 festgelegt.

2 Spezifische Referenzen

1 [BSZ-Prod] Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Produkte, BSI

2 [BSZ-Prüf] Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Prüfstellen, BSI

3 [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess, BSZ-EP, BSI

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

5 [AIS B3] Anforderungen an die Benutzeranleitung, BSI

6 [AIS B4] Anforderungen an die Evaluierung gemäß BSZ, BSI

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

8 [AIS B6] Anforderungen an einen TOE, BSI

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

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

3 Sicherheitsvorgaben

7 In den folgenden Abschnitten wird ausführlich beschrieben, welchen Aufbau das Dokument Sicherheitsvorgaben haben muss und welche Inhalte in den verschiedenen Abschnitten erwartet werden. In einer separaten ST-Vorlage werden Beispiele sowie weitere Erläuterungen bereitgestellt [ST Vorlage].

8 Soweit nicht anders angegeben, muss das ST so verfasst werden, dass die erwarteten Endkundinnen und Endkunden, d. h. jene Personen, die über den Kauf des Produkts entscheiden, in der Lage sind, den Inhalt zu verstehen.

Hinweis: Bei einigen TOEs kann es sich dabei beispielsweise um einen Einkaufsleiter, bei anderen wiederum um einen Laien handeln. Um das Verständnis zu erleichtern, sollten geeignete Verweise auf zuverlässige Quellen bereitgestellt werden. Das ST kann sowohl auf Englisch als auch auf Deutsch verfasst werden und sollte ungefähr zehn Inhaltsseiten ohne Anhang umfassen.

3.1 Einleitung

3.1.1 Inhalt dieses Dokuments

Erforderlicher Inhalt

9 In diesem Unterabschnitt muss beschrieben werden, warum dieses Dokument erstellt und wie der Inhalt hergeleitet wurde.

10 In diesem Unterabschnitt muss das an der Entwicklung des ST beteiligte Schlüsselpersonal aufgelistet (d. h. Name und Funktion) oder referenziert (d. h. nur nach Funktion) werden.

3.1.2 Produktkennzeichnung

Erforderlicher Inhalt

11 In diesem Unterabschnitt müssen der eindeutige Name und die spezifische Version des TOE genannt werden, ggf. einschließlich des Verweises auf die unterschiedlichen Versionsnummern der Software und der Hardware. Darüber hinaus muss hier angegeben werden, wie die erwarteten Endkundinnen und Endkunden das Produkt eindeutig identifizieren können.

12 Bei integrierten Systemen mit hardwarebezogener Programmierung muss der Name des TOE lauten: „{Produktkategorie} [TOE-Name] – Softwareversion [X.X] des Unternehmens [Unternehmensname]“.

13 Bei Softwareanwendungen oder Anwendungen in virtualisierten Systemen muss der Name des TOE lauten: „[Softwareprodukt/virtualisiertes Produkt] [TOE-Name] – Version [X.X] ausgeführt auf [Name der Hardware-Plattform mit CPU-Modell] des Unternehmens [Unternehmensname] {für das System/die Maschine/selbst gewählten [Gerätenamen]} in der Produktkategorie [Kategorienname]“.

Hinweis: Der Inhalt in den {} - Klammern ist optional. Der Schrägstrich (/) ermöglicht eine Auswahl.

3.1.3 Referenzen / Akronyme

Erforderlicher Inhalt

14 In diesem Unterabschnitt müssen alle verwendeten Akronyme aufgenommen werden.

15 In diesem Unterabschnitt müssen sämtliche Verweise enthalten sein, d. h. Verweise auf implementierte Normen und weitere Dokumente des Herstellers. Bei Aufnahme von Verweisen auf weitere Dokumente des Herstellers müssen diese allen Kunden entgeltfrei zur Verfügung gestellt werden.

16 Sämtliche in diesem Dokument geforderten Inhalte müssen im ST selbst und nicht in den referenzierten Dokumenten enthalten sein, mit Ausnahme der kryptographischen Spezifikation, die separat bereitgestellt wird.

3.2 Produktbeschreibung

3.2.1 Allgemeine Beschreibung

Erforderlicher Inhalt

17 Dieser Unterabschnitt muss eine allgemeine Beschreibung des TOE enthalten, die für Veröffentlichungen auf Webseiten oder in Produktdatenbanken geeignet ist.

3.2.2 Funktionen und Schnittstellen

Erforderlicher Inhalt

18 In diesem Unterabschnitt müssen die für die BSZ-Evaluierung relevanten Funktionen und Schnittstellen des TOE aufgeführt und beschrieben werden. Die verwendeten Begriffe müssen definiert werden, sofern sie nicht selbsterklärend sind. Definitionen können im Hauptteil oder durch Verweise auf zuverlässige und zugängliche öffentliche Quellen angegeben werden.

19 Bei der Beschreibung soll, soweit möglich, auf unternehmensspezifische Terminologie verzichtet werden.

20 Jegliche Kommunikationsschnittstellen müssen ebenfalls in diesem Unterabschnitt aufgelistet und beschrieben werden.

21 Funktionen und Schnittstellen, die für Prüfungen nicht zugänglich sind, müssen deutlich als solche gekennzeichnet werden.

3.2.3 Produktnutzung

Erforderlicher Inhalt

22 In diesem Unterabschnitt muss die vorgesehene Produktverwendung in natürlicher Sprache beschrieben werden, damit die entsprechende Zielgruppe entscheiden kann, ob das Produkt für den vorgesehenen Einsatzzweck geeignet ist. Die Einzelheiten zur Betriebsumgebung sind in den nachfolgenden Unterabschnitten anzugeben.

3.2.4 Betriebsumgebung

Erforderlicher Inhalt

23 In diesem Unterabschnitt muss die erforderliche Betriebsumgebung des TOE angegeben werden, d. h. die technische Umgebung, die erwarteten Nutzerinnen und Nutzer sowie die erwarteten Bedrohungen.

24 In diesem Unterabschnitt muss die für den Betrieb des TOE erforderliche spezifische Hardware oder Software angegeben werden.

25 Falls mehrere Umgebungen möglich sind (z. B. mehrere Versionen einiger Hintergrundsysteme oder Betriebssysteme), muss eindeutig angegeben werden, welche Version für die Evaluierung herangezogen werden soll.

Für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

26 Die Systemumgebung muss beschrieben werden. Dies kann durch konkrete Spezifikationen für die zu verwendende Hardware und Software definiert oder durch Anforderungen und Abhängigkeiten, die der TOE an die Systemumgebung stellt, erfolgen.

Hinweis: Im Kontext von Softwareanwendungen und Anwendungen in virtualisierten Umgebungen adressiert die Systemumgebung die zugrundeliegende Hardware, während die Betriebsumgebung die weitere äußere Umgebung der zugrundeliegenden Hardware bezeichnet. Mit anderen Worten ist eine Softwareanwendung oder eine Anwendung in einer virtualisierten Umgebung in einer Systemumgebung eingebettet, die ihrerseits wiederum in einer Betriebsumgebung eingebettet ist.

Beispiel: X.Y ist eine Software-Lösung für einen Konnektor im Gesundheitswesen. Die Systemumgebung wird durch einen Rack Server der folgenden Hardware spezifiziert: [...]. Dieser Server wird in der Betriebsumgebung der Telematik-Infrastruktur eingebettet.

27 Wenn die Antragstellerin keine spezifischen Modelle oder Serien von Modellen für den TOE angibt, müssen Mindest- und, wenn notwendig, Höchstanforderungen für Hardware und Software für den sicheren Betrieb des TOE festgelegt und in der Hardware- und Softwarespezifikation angegeben werden.

Hinweis: Anforderungen an die Systemumgebung, die zu einer potenziell großen Zahl an Kombinationen in der Auslegung von Hardware und Software führen, können einen erhöhten Testaufwand erfordern und die Komplexitätsgrenze oder maximale Testdauer für eine Zertifizierung im BSZ-Verfahren überschreiten.

28 Wenn das Design der Hardware durch mehrere verschiedene Kombinationen von Komponenten realisiert werden kann, muss die Hardware-Spezifikation um eine Kompatibilitätsbeschreibung erweitert werden. Diese muss eine Beschreibung des erforderlichen Verhaltens der angegebenen Hardware in Bezug auf Abhängigkeiten an die Systemumgebung enthalten.

29 Vor der Auftaktbesprechung muss die Prüfstelle schriftlich spezifisch ausgewählte Hardware und Software als repräsentative Testumgebung für die Zertifizierung vorschlagen, die folgend in der Auftaktbesprechung verbindlich festgelegt wird. Die Auswahl muss auf der von der Antragstellerin bereitgestellten Hardware- und Softwarespezifikation basieren und für den TOE typisch sein.

Hinweis: Die Testumgebung kann mehr als eine spezifische Auswahl der Hardware- und Softwarespezifikation für die Bewertung des TOE repräsentieren.

30 Die Systemumgebung muss die Anforderungen der zu zertifizierenden Anwendung erfüllen, die im Dokument [AIS B6] unter Absatz 3.5 gelistet sind.

3.3 Sicherheitsbeschreibung

3.3.1 Nutzerinnen und Nutzer

Erforderlicher Inhalt

31 Dieser Unterabschnitt beschreibt die Nutzerinnen und Nutzer bzw. die Rollen, die vom TOE unterstützt werden. Dabei sind die Nutzerinnen und Nutzer bzw. die Rollen nicht auf die explizit im

TOE definierten beschränkt. Sie können auch implizit durch die Schnittstelle definiert sein, über die sie in Aktion treten (z. B. an einem bestimmten Port einer Firewall). Dieser Unterabschnitt beschreibt die Merkmale jeder Nutzerin und jedes Nutzers bzw. jeder Rolle, d. h. die Merkmale hinsichtlich der Art von Aufgaben, an denen sie beteiligt sind, ob sie im TOE über bestimmte Berechtigungen verfügen, ob der Zugriff auf bestimmte Ports beschränkt ist usw.

32 Für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen ist es notwendig, ein geeignetes Rollen und- und Berechtigungskonzept für den Betrieb des TOE in der Betriebsumgebung zu implementieren. Die obligatorischen Rollen sind der Benutzer des TOE, der Administrator des TOE und der Administrator der Betriebsumgebung:

- Der Benutzer der Anwendung ist der Benutzer des TOE und darf keine administrativen Rechte haben.
- Der Anwendungsadministrator hat erweiterte Rechte gegenüber dem TOE und ist für dessen Verwaltung und Installation verantwortlich.
- Der Systemadministrator muss die Berechtigung(en) haben, die Systemumgebung zu verwalten, zu installieren und zu administrieren und kann je nach Einrichtung der Systemumgebung um verschiedene autorisierte Administratoren erweitert werden.

- *Hinweis: Der Systemadministrator hat physischen Zugriff auf die Systemumgebung und ist für die Verwaltung, Administration und Bereitstellung des Systems innerhalb der Umgebung verantwortlich. Dies umfasst beispielsweise die Verwaltung von Domänen und Benutzern.*

Hinweis: Abhängig von der Komplexität des TOE oder seiner Betriebsumgebung können Rollen auch durch unterschiedliche Benutzer implementiert sein. Falls der TOE ebenso über andere interne Rollen wie bspw. Datenbankbenutzer verfügt, sollten diese im Detail beschrieben werden. Wenn mehrere Rollen zu einem einzelnen Benutzer gruppiert sind, ist es wichtig, dass die Zugangsberechtigungen separiert bleiben, d. h. die Softwareanwendung kann nicht mit den Berechtigungen eines Administrators ausgeführt werden.

3.3.2 Annahmen

Erforderlicher Inhalt

33 Der TOE benötigt möglicherweise eine bestimmte Umgebung, um seine Sicherheitseigenschaften zu erfüllen. Diese Umgebung kann aus personenbezogenen Eigenschaften (z. B. erforderliche Kenntnisse und Fähigkeiten bestimmter Nutzerinnen und Nutzer), logischen Anforderungen (z. B. Netzwerktopologie), physischen Maßnahmen (z. B. physische Zugangsbeschränkungen), organisatorischen Notwendigkeiten (z. B. Rechte und Rollen) oder IT-bezogenen Annahmen (z. B. Verschlüsselung, die bei Netzwerkverbindungen verwendet wird) bestehen. In diesem Unterabschnitt muss eine kurze umgangssprachliche Begründung für diese Annahmen angegeben werden.

Hinweis: Dieser Unterabschnitt muss mit allen anderen Unterabschnitten konsistent sein, insbesondere mit Unterabschnitt 3.2.3. Beispielsweise steht die Anforderung bestimmter TOE-Kenntnisse der Nutzerin oder des Nutzers im Widerspruch zu einer Produktbeschreibung, die vorgibt, dass das Produkt für die breite Öffentlichkeit bestimmt sei.

34 Jede Annahme muss eindeutig identifizierbar sein.

3.3.3 Werte

Erforderlicher Inhalt

35 In diesem Unterabschnitt müssen die Werte des TOE oder die vom TOE geschützten Werte aufgeführt und beschrieben werden, deren Sicherheitseigenschaften (d. h. Vertraulichkeit, Integrität oder Verfügbarkeit) schutzwürdig sind.

36 Jeder Wert muss eindeutig identifizierbar sein.

3.3.4 Bedrohungsmodell: Angreifer

Erforderlicher Inhalt

37 In diesem Unterabschnitt müssen die im Bedrohungsmodell angenommenen Angreifer beschrieben werden. Dabei muss es sich um die in der vorgesehenen Umgebung am wahrscheinlichsten zu erwartenden Angreifer des TOE handeln.

38 Jeder Angreifer muss eindeutig identifizierbar sein.

3.3.5 Bedrohungsmodell: Bedrohungen

Erforderlicher Inhalt

39 In diesem Unterabschnitt müssen Bedrohungen beschrieben werden, denen die Sicherheitsfunktionen des TOE entgegenwirken.

40 Jede Bedrohung muss eindeutig identifizierbar sein.

3.3.6 Sicherheitsfunktionen

Erforderlicher Inhalt

41 In diesem Unterabschnitt muss eine Spezifikation der sicherheitsrelevanten Funktionen des TOE enthalten sein. Hier muss bei Bedarf auf die technischen Informationen (z. B. Layer 2, Protocol xy) verwiesen werden, und zwar – soweit möglich – unter Bezugnahme auf die relevanten und aktiven Normen. Dabei sollten zuverlässige Online-Referenzen verwendet werden.

42 In diesem Unterabschnitt kann auf die Verwendung von Endkundensprache verzichtet werden, sofern Fachbegriffe verwendet werden, die für eine durchschnittlich fachkundige Person verständlich sind.

Für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

43 Der TOE muss ausreichend eigene Sicherheitsfunktionen haben, die über externe Schnittstellen evaluiert werden können.

44 Werden im ST Sicherheitsfunktionen aufgeführt, die vollständig oder teilweise von der Systemumgebung implementiert werden, sind diese im Dokument entsprechend auszuweisen. Die Abhängigkeiten zur Systemumgebung müssen an dieser Stelle beschrieben werden. Die Angabe eines Benutzers für die Sicherheitsfunktion aus dem Rollenmodell ist notwendig, wenn der TOE separate Rechte für den Aufruf oder die Implementierung der Sicherheitsfunktion benötigt. Es muss klar beschrieben werden, welche Teile der Sicherheitsfunktionalität von der Systemumgebung realisiert werden und wie diese Teile im TOE integriert sind oder vom TOE genutzt werden, um die zu testende Sicherheitsfunktion bereitzustellen.

45 Zusätzlich zu den Sicherheitsfunktionen, die vom TOE selbst zur Verfügung gestellt werden, müssen auch jene Sicherheitsfunktionen, die vollständig oder teilweise von der Systemumgebung implementiert werden, im ST als Sicherheitsfunktionen angegeben werden. Die Benennung der Sicherheitsfunktion muss eindeutig eine Unterscheidung zwischen den vom TOE selbst

bereitgestellten und der in der Systemumgebung implementierten Sicherheitsfunktion ermöglichen.

3.3.7 Mapping

Erforderlicher Inhalt

46 In diesen Unterabschnitt muss eine Tabelle aufgenommen werden, in der alle Bedrohungen den zugehörigen Angreifern, den betroffenen Werten und den involvierten Sicherheitsfunktionen zugeordnet werden. Bei komplexen Beziehungen kann eine kurz gefasste Erklärung hinzugefügt werden.

3.4 Grenzen der Evaluierung

Erforderlicher Inhalt

47 Dieser Abschnitt muss alle Funktionen, Aufgaben, Dienste und Schnittstellen enthalten, die nicht in den Geltungsbereich dieser Zertifizierung fallen. Die ausgegrenzten Gegenstände dürfen mit dem Verwendungszweck des TOE nicht im Widerspruch stehen.

48 Sollten für den Betrieb der TOE-Sicherheitsfunktionen dynamische Inhalte erforderlich sein (z. B. aus Ferndatenbanken), muss das ST eindeutig darauf verweisen, dass das Remote-System, das die Inhalte bereitstellt, nicht Teil der Evaluierung ist. Die Sicherheitsfunktion, die den Inhalt anfordert, muss dagegen in die Evaluierung einbezogen werden.

4 Separater Anhang: kryptographische Spezifikation

49 Die Evaluierung und Zertifizierung erfordern besondere Aufmerksamkeit, wenn das ST Sicherheitsfunktionalitäten umfasst, die mithilfe kryptographischer Mechanismen gewährleistet werden, oder wenn der TOE kryptographische Dienste bereitstellt, wie zum Beispiel: Verschlüsselungsroutinen, Generierung von Hashes, Generierung von Signaturen, Generierung von Zufallszahlen, Schlüsselgenerierung oder Kommunikationsprotokolle unter Verwendung von Verschlüsselung. Um etwaige Fehler aufgrund von Konformitätsproblemen zu vermeiden und den Zertifizierungsprozess zu optimieren, muss die Antragstellerin einen Überblick über alle enthaltenen Mechanismen und bereitgestellten Dienste vorlegen, die in der sicheren Konfiguration, wie im Benutzerhandbuch oder im Handbuch zur sicheren Benutzung beschrieben, aktiviert sind und die in den Umfang der Evaluierung fallen.

4.1 Liste der kryptographischen Mechanismen

Erforderlicher Inhalt

50 Die Antragstellerin muss für die kryptographischen Mechanismen, die zur Gewährleistung der Sicherheitsfunktionalität des TOE verwendet werden, eine kryptographische Spezifikation vorlegen. Eine Übersicht über die verwendeten kryptographischen Mechanismen ist in Form einer Tabelle gemäß dem nachstehenden Beispiel bereitzustellen.

Hinweis: Zu den kryptographischen Mechanismen können unter anderem (symmetrische/asymmetrische) Verschlüsselungsverfahren, Hashfunktionen, Message Authentication Codes, (passwortbasierte) Schlüsselableitungsfunktionen, digitale Signaturverfahren, Schlüsselerstellungsverfahren, (symmetrische/asymmetrische) Verifikation der Quelle [und Integrität] von Daten, (symmetrische/asymmetrische) Verfahren zur Authentisierung von Instanzen, Verfahren für die authentifizierte Verschlüsselung, (passwort-)authentifizierte Verfahren zur Schlüsselerstellung, Verfahren für Secret-Sharing, kryptographische Protokolle und deterministische Zufallszahlengeneratoren gehören.

51 Die vom TOE verwendeten kryptographischen Mechanismen sollten den vereinbarten Algorithmen aus dem SOG-IS-Katalog entsprechen [SCES-ACM]. Abweichende Mechanismen (insbesondere kryptographische Protokolle) müssen vor Beginn der Evaluierung von der Zertifizierungsstelle genehmigt werden. Von der Zertifizierungsstelle empfohlene kryptographische Protokolle umfassen die Empfehlungen der Technical Guideline [BSI-TR-02102] (Teile 2–4).

52 Die Beschreibung eines kryptographischen Mechanismus muss nach Schnittstellen kategorisiert sein und die folgenden Informationen enthalten:

- Verweise auf verfügbare Normen, die den Mechanismus eindeutig definieren, zusammen mit ausgewählten Optionen oder Parametern (z. B. Schlüssellängen, Domänenparameter usw.).
- Die vom Mechanismus erzwungene Sicherheitsfunktionalität (Zuordnung zu den im Dokument Sicherheitsvorgaben vorgegebenen Sicherheitsfunktionen).
- Das durch den Mechanismus erreichte Sicherheitsziel (z. B. Vertraulichkeit, Integrität, Authentizität usw.).

53 Die Definition eines kryptographischen Verfahrens oder Protokolls erfordert üblicherweise die Definition mehrerer Algorithmen (z. B. erfordern Verschlüsselungsverfahren die Definition eines Schlüsselgenerierungsalgorithmus, eines Verschlüsselungsalgorithmus und eines Entschlüsselungsalgorithmus).

Beispiele

1. Zweck	*2. Kryptographischer Mechanismus*	*3. Implementierungsnorm*	*4. Schlüsselgröße in Bit*
Vertrauenswürdiger Kanal an ... über HTTPS mit TLS 1.3 [RFC 8446]			
Authentizität	RSA-Signaturerstellung und -verifizierung (RSASSA-PSS) mittels SHA-256	[PKCS#1 v2.2] (RSA), [FIPS 180-4] (SHA)	Modullänge = 2048
Authentifizierung	RSA-Signaturerstellung und -verifizierung (für RSASSA-PSS)	[RFC 5246] (TLS) [RFC 3447] (PKCS#1 v2.1)	3072, 4096
Schlüsselvereinbarung	Elliptische Kurven (ECDHE): secp256r1, secp384r1	[RFC 5246] (TLS) [RFC 8422] (TLSECC) [IEEE P1363] (ECDH)	256, 384
Schlüsselvereinbarung	DHE-Gruppen: ffdhe3072, ffdhe4096	[RFC 5246] (TLS) [RFC 7919] (DHE)	3072, 4096
Vertraulichkeit	AES in GCM-Modus	[RFC 5246] (TLS) [RFC 5288] (AESGCM) [RFC 5289] (AES-GCM) [FIPS 197] (AES) [SP800-38D] (GCM)	128, 256
Vertraulichkeit	AES in CBC-Modus	[RFC 5246] (TLS) [FIPS 197] (AES) [SP800-38A] (CBC)	128, 256
Integrität	HMAC mit SHA-2	[RFC 5246] (TLS) [FIPS 180-2] (SHA)	256, 384
Zufallszahlengenerator	Deterministischer RNG DRG.3	[AIS-20]	
Vertrauenswürdiger Kanal an Command Line Interface (CLI) mit SSH [4251]			
Schlüsselaustausch (-Vereinbarung)	diffie-hellman-group15-sha512	[RFC 4253] (Schlüsselaustauschverfahren) [RFC 8268] (mehr DH für SSH) [RFC 3526] (Gruppenspezifikation)	3072
Authentifizierung	Elliptic Curve Digital Signature Algorithm mit SHA-256 und nistp256 (ecdsa-sha2-256)	[RFC 5656]	256
Vertraulichkeit	AES in CTR-Modus	[RFC 4344] (SSH Encryption Modes)	128, 192, 256
Integrität	HMAC mit SHA-2 (hmac-sha2-256)	[RFC 4253] (SSH) [RFC 6668] (SHA-2-Integration) [RFC6234] (SHA-2-Definition)	256
Zufallszahlengenerator	/dev/urandom		

Tabelle 2 Beispiel für eine Tabelle mit kryptographischem Mechanismus

4.2 Beschreibung der Rauschquelle

Erforderlicher Inhalt

54 Wenn in der kryptographischen Spezifikation Zufallszahlengeneratoren enthalten sind, muss die Antragstellerin für die Rauschquellen, die zum Seeding verwendet wurden, im separaten „Krypto-Anhang“ ein Kapitel zur Rauschquellenbeschreibung einfügen.

55 Die Beschreibung einer Rauschquelle sollte Informationen zu deren Art (physikalisch oder nicht-physikalisch) und zur Wirkungsweise enthalten.

56 Wenn mehrere Rauschquellen verwendet werden, sollte eine Begründung dafür vorgelegt werden, dass die Quellen unabhängig sind.

57 Die Beschreibung der Rauschquelle sollte eine Begründung dafür enthalten, dass die zum Seeding verwendeten Zufallsbits eine Mindestentropie von mindestens 125 Bits aufweisen. Bei Verwendung eines CC-zertifizierten physikalischen Zufallszahlengenerators genügt ein Verweis auf die Zertifizierungs-ID.

4.3 Beschreibung des Schlüsselmanagements

Erforderlicher Inhalt

58 Die Antragstellerin muss eine Beschreibung des Schlüsselmanagements in Form eines Kapitels im separaten „Krypto-Anhang“ vorlegen, in dem die Informationen über kryptographische Schlüssel sowie Parameter enthalten sind, die vom TOE für kryptographische Verfahren verwendet werden.

59 Die Beschreibung eines Schlüssels sollte Informationen über seinen Typ sowie seine Erzeugung, Verteilung, Verwendung, Speicherung, Zerstörung, Gültigkeitsdauer und Schutzanforderungen enthalten.

60 Die Beschreibung des Schlüsselmanagements muss zudem Informationen zu anderen relevanten Parametern enthalten, einschließlich Domänenparameter, Initialisierungsvektoren, Zähler und Tweaks.

61 Die Beschreibung des Schlüsselmanagements muss die zwischen Schlüsseln bestehenden hierarchischen Beziehungen hervorheben (z. B. ob ein Schlüssel von einem anderen Schlüssel abgeleitet ist oder ob ein Schlüssel mit einem anderen Schlüssel verschlüsselt ist).

4.4 Implementierungsdarstellung

Erforderlicher Inhalt

62 Die Antragstellerin muss der Prüfstelle für IT-Sicherheit (kurz Prüfstelle) für die kryptographischen Mechanismen, die zur Gewährleistung der Sicherheitsfunktionalität des TOE verwendet werden, eine Implementierungsdarstellung vorlegen. Kann die Antragstellerin die Implementierungsdarstellung für einen oder mehrere kryptographische Mechanismen nicht vorlegen, muss die Prüfstelle vor Beginn der Evaluierung mit der Zertifizierungsstelle die Eignung der Zertifizierung erörtern.

63 Die Implementierungsdarstellung sollte den Quellcode oder den Pseudocode umfassen. Bei Bereitstellung des Quellcodes muss es sich um den Code handeln, der bei der Erstellung des TOE verwendet wurde. Sollte ein Pseudocode bereitgestellt werden, muss dieser einen Detaillierungsgrad aufweisen, der der tatsächlichen Implementierung sehr ähnlich ist (insbesondere muss er Seitenkanal-Gegenmaßnahmen umfassen, falls solche Maßnahmen implementiert wurden).

64 Die Implementierungsdarstellung muss die Implementierung der kryptographischen Funktionalität selbst sowie jene Teile der Implementierung abdecken, in denen die kryptographische Funktionalität aufgerufen wird.

65 Wenn bei der Implementierung quelloffene kryptographische Bibliotheken verwendet werden, muss die Implementierungsdarstellung Informationen über deren Herkunft, die Version und alle von der Antragstellerin vorgenommenen Änderungen enthalten.

5 Änderungsbeschreibung mit Auswirkungsanalyse

66 Wurde ein Produkt bereits in einem früheren BSZ-Verfahren evaluiert, besteht die Möglichkeit, den Evaluierungsaufwand für ein neues BSZ-Verfahren zu reduzieren. Zu diesem Zweck reicht die Antragstellerin zusammen mit den Antragsunterlagen eine Änderungsbeschreibung mit Auswirkungsanalyse (Englisch: Impact Analysis Report, IAR) ein.

67 Die Antragstellerin muss im IAR die Änderungen bezüglich des TOE angeben sowie in den Antragsunterlagen eine Beschreibung zu den Änderungen beifügen. Der IAR muss hinreichend genau sein, um von den Evaluatorinnen bzw. Evaluatoren und Zertifiziererinnen bzw. Zertifizierern verstanden zu werden. Sämtliche Unterlagen, die zur Evaluierung des modifizierten TOEs erforderlich sind, aber nicht zur Evaluierung des ursprünglichen TOEs benötigt wurden, sind entsprechend zu kennzeichnen.

68 Der IAR ist nicht als Ersatz für die Aktualisierung der Unterlagen zu betrachten. Die Antragstellerin muss die an den Unterlagen vorgenommenen Änderungen eindeutig kennzeichnen, z. B. durch die Verwendung von Änderungsmarkierungen. Eine Klassifizierung der in den Unterlagen vorgenommenen Änderungen ist nicht erforderlich. Bei Verwendung von Änderungsmarkierungen gilt jeder nicht markierte Inhalt sowohl für den zuvor geprüften als auch für den geänderten/neu geprüften TOE; jeder markierte Inhalt ist entweder redaktioneller Natur oder betrifft nur den geänderten TOE.

5.1 Änderungen am Produkt im Vergleich zur vorherigen Evaluierung

Erforderlicher Inhalt

69 Im IAR muss eine Zusammenfassung enthalten sein, in der alle am Produkt vorgenommenen Änderungen beschrieben werden. Es muss ausdrücklich auf alle Probleme der letzten Evaluierung und alle weiteren Änderungen (z. B. etwaige Maintenance oder Produktverbesserung) eingegangen werden.

Beispiele

70 *Um Befund #5 (Schwachstelle “to long input strings”) zu adressieren, wurde die Bilbiothek XYZ von Version 1.0.1 auf Version 1.0.2 aktualisiert. Alle anderen Befunde (#1-#4 und #6) wurden von anderen gesonderten Code-Änderungen adressiert. Weiter behebt dieses maintenance release die Schwachstellen CVE 2020-06-23, CVE-2020-04-27 und CVE-2020-05-118 und implementiert eine Liste abzulehnender Unicode-Zeichen, um potentielle Auswirkungen auf die Sicherheit zu vermeiden.*

5.2 Beschreibung der Änderungen an den Unterlagen der Antragstellerin

5.2.1 Änderungen an der Sicherheitsvorgabe

Erforderlicher Inhalt

71 Die Antragstellerin muss angeben, ob die Änderung redaktioneller Natur ist (z. B. Produktname, Version) oder ob die Änderung Auswirkungen auf den Inhalt hat (z. B. Beschreibung des TOE, der Annahmen, Bedrohungen oder Sicherheitsanforderungen).

Beispiele

72 *Das Dokument Sicherheitsvorgaben wurde aktualisiert, um die aktuellen Versionsnummern anzuführen (TOE, SUG).*

5.2.2 Änderungen am Design und der Implementierung des Produkts

Erforderlicher Inhalt

73 Die Antragstellerin muss Änderungen am Design und der Implementierung angeben mit dem Ziel, den Bezug der Änderungen zur Sicherheitsfunktionalität einschließlich der Sicherheitsarchitektur darzulegen (z. B. neue Filterbibliotheken zur Verarbeitung von Eingaben). Je nach Umfang und Auswirkung der Änderung kann es sich hierbei um einen kurzen Verweis auf öffentlich zugängliche Quellen oder um einige Absätze handeln, in denen die Änderung beschrieben wird.

Hinweis: Ziel dieser Beschreibung ist es, ausreichende Details bereitzustellen, um eine effiziente Reevaluierung zu ermöglichen. Je nach Größe und Komplexität einer Änderung kann eine Beschreibung relativ abstrakt sein, z. B. durch Verwendung einer neueren Version einer Bibliothek oder Bereitstellung einer Beschreibung auf niedrigerer Ebene, einschließlich Auszüge aus dem Quellcode oder dem Pseudocode.

Beispiele

74 *Die network state machine wurde um eine neue Regel aktualisiert, welche diese priorisiert, um die Schwachstelle CVE 2020-06-23 zu beheben.*

75 *OpenSSL wurde zu Version 1.1.1.g aktualisiert, um CVE-2020-04-27 and CVE-2020-05-118 zu beheben.*

76 *Die Filter-Routine wurde aktualisiert, um Unicode-Zeichen im Bereich ... handzuhaben:*

```
// Before any processing is done:
for each input string
for each unicode character
if unicode character in (updated) blacklist then replace character by
NULL character
```

77 *Bibliothek XYZ wurde auf Version 1.02 aktualisiert, um überlange Zeichenketten zu vermeiden.*

5.2.3 Änderungen an den Anleitungsdokumenten

Erforderlicher Inhalt

78 Die Antragstellerin muss Änderungen an den Anleitungsdokumenten (z. B. Handbuch zur sicheren Benutzung) angeben.

Beispiele

79 *Klargestellt, dass Benutzernamen und Passwörter keine Unicode-Zeichen im Bereich (...) enthalten dürfen.*

80 *Befund #7 (verwirrende Beschreibung der Passwortrücksetzungsprozedur) der vorherigen Evaluierung wird durch Ergänzungen im Handbuch zur sicheren Benutzung behoben.*

5.2.4 Änderungen an den Anforderungen für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen

Erforderlicher Inhalt

81 Die Antragstellerin muss alle Änderungen am Rollen- und Berechtigungskonzept angeben, die sich auf das Verhalten des TOE in der Betriebsumgebung auswirken. Im Falle einer Rezertifizierung muss angegeben werden, ob bestehende Funktionalitäten an die Systemumgebung ausgelagert oder zu dieser hinzugefügt wurden, sowie ob sich Anforderungen oder Abhängigkeiten von der Systemumgebung geändert haben.

Beispiel:

82 *In der vorherigen Version 2.7.18 von FooApp verwaltete die Anwendung noch selbst die Benutzerdaten und verschlüsselte die Daten in einem entsprechenden kompilierten Benutzerverzeichnis für jeden implementierten Benutzer individuell. Mit der neuen stabilen Version 3.1.4 von FooApp wurde die Benutzerverwaltung an das Betriebssystem übertragen, das für die Erstellung der Benutzerrechte verantwortlich ist. Daher werden alle Benutzerdaten unter dem Dateipfad X/y/z zwangsläufig so gespeichert, dass nur der authentifizierte Benutzer auf seine eigenen Daten zugreifen kann.*

5.3 Erörterung der Auswirkung von Änderungen

Erforderlicher Inhalt

83 Während der Reevaluierung ist die Prüfstelle dafür verantwortlich, alle notwendigen Arbeiten durchzuführen, um die Vertrauenswürdigkeit des geänderten Produkts zu bestätigen. Die Erörterung der Antragstellerin ist dennoch hilfreich für den Evaluator, um den erforderlichen Aufwand abzuschätzen und die Vorbereitung der Auftaktbesprechung mit der Zertifizierungsstelle zu erleichtern.

84 Diese IAR-Erörterung muss explizit auf alle in der vorherigen Evaluierung festgestellten Probleme eingehen. Für den Fall, dass nicht jedes Problem von der Antragstellerin (vollständig) gelöst wird, ist eine Begründung anzugeben, warum dies nicht zu einem Sicherheitsproblem führt, z. B. Umsetzung weiterer/anderer Maßnahmen, die das Problem verhindern/abmildern. Die Prüfstelle muss diese Begründung bewerten, wodurch weitere Prüfaufwände entstehen.

Hinweis: Bei dieser Bewertung ist der Stand der Technik zu berücksichtigen und ferner die Frage danach, ob die Begründung aus Endnutzersicht tatsächlich akzeptabel ist.

Beispiele

1. *Die Änderungen an der Zustandsmaschine (state machine) betreffen ausschließlich den in CVE 2020-06-23 erwähnten Ausnahmefall. Es wurden keine weiteren Änderungen vorgenommen und der Ausnahmefall wurde zur in die Menge der Standardtests in verschiedenen Variationen aufgenommen. Daher ist der Einfluss auf die korrekte Verarbeitung von Netzwerkpaketen sehr gering und nur der Ausnahmefall wurde verändert.*
2. *OpenSSL 1.1.1g ist ein reines Maintenance-Release verglichen mit der vorherig genutzten Version 1.1.1f. Dies adressiert 35 CVEs, von denen ausschließlich CVE-2020-04-27 und CVE-2020-05-118 auf den TOE anwendbar sind. OpenSSL hat eine gute Erfolgsbilanz bei der Klärung von Änderungen und Maintenance-Releases sind streng auf die Behebung von Sicherheitsproblemen beschränkt (die eindeutig in den Veröffentlichungsnotizen beschrieben werden). Ebenso haben sich weder die restlichen OpenSSL Interna noch die produktspezifischen Standardtests geändert. Es wurden die obengenannten CVEs hinzugefügt. Die sicherheitsrelevanten Auswirkungen des*

Maintenance-Releases durch Implementierung neuer unbekannter Sicherheitsprobleme der OpenSSL Version 1.1.1g sind daher als gering einzuschätzen.

3. *Das Unicode Consortium veröffentlichte eine neue Version von Unicode mit einem umfangreicheren Zeichensatz. Da dieser mit großer Sicherheit nicht relevant für die Produktivsysteme ist, wurde der vorherige Filter für die Ablehnliste um diese Zeichen erweitert. Da somit ausschließlich die Ablehnliste erweitert wird, folgt aus dieser Änderung kein Sicherheitseinfluss.*
4. *Befund #1 wurde adressiert durch einen expliziten Timing-Mechanismus, um alle Antworten gleichzeitig auszusetzen – unabhängig davon, ob die Anmeldedaten (teilweise) korrekt waren. Ein neuer Standardtest deckt diesen Testfall ab. Die Überprüfung der Anmeldedaten selbst bleibt unverändert (die auch nicht Gegenstand eines Befundes war). Daher ist der Sicherheitseinfluss dieser Änderung gering.*
5. *Befund #2 …*
6. *Befund #5 wurde durch das Update der Bibliothek XYZ behoben. Die Version 1.02 akzeptiert nicht mehr Strings beliebiger Länge an jeder Stelle und gibt sofort einen Fehler zurück, der ordnungsgemäß in allen Instanzen des Codes behandelt wird. Da dies die einzige Änderung zur Version 1.01 ist und die Standardtests sowohl in der Bibliothek XYZ als auch für den TOE hinzugefügt wurden, besteht der Einfluss dieser Änderung in der Behebung des im ETR in Abschnitt X.Y.Z erwähnten Fehlers.*

6 Softwarestückliste

85 Die Antragstellerin muss eine Softwarestückliste (Englisch: Software Bill of Materials, SBOM) gemäß Abschnitt 6.1 bereitstellen. Für jede im TOE enthaltene Komponente, die der Hersteller des TOE selbst bereitstellt, muss die Antragstellerin einen entsprechenden SBOM-Eintrag erstellen.

86 Für jede Drittanbieterkomponente, die direkt in einer vom TOE-Hersteller bereitgestellten Komponente verwendet wird, muss ein entsprechender SBOM-Eintrag erstellt werden. Standardbibliotheken von Programmiersprachen, die direkt in vom TOE-Hersteller bereitgestellten Komponenten verwendet werden, fallen ebenfalls unter diese Regelung. Eine Softwarebibliothek A gilt dabei als direkt in einer Softwarebibliothek oder Anwendung B verwendet, wenn der Quellcode von B Aufrufe zu einer oder mehreren von A bereitgestellten Prozeduren enthält.

87 Wenn der TOE aus mehreren Anwendungen besteht oder solche einschließt, die entweder dauerhaft ausgeführt werden müssen (z. B. ein Webserver) oder als Reaktion auf ein oder mehrere Ereignisse (z. B. Ablauf eines Timers) eine oder mehrere Funktionen des TOE bereitstellen müssen, muss für jede dieser Anwendungen ein SBOM-Eintrag erstellt werden.

88 Wenn der TOE einen Betriebssystem-Kernel enthält, muss die Antragstellerin unabhängig davon, ob sie die Komponente selbst bereitstellt, einen entsprechenden SBOM-Eintrag erstellen.

89 Wenn die Lieferantin einer Drittanbieterkomponente, die von den oben genannten Bedingungen erfasst wird, eine offizielle SBOM für diese Komponente bereitstellt, die den in Abschnitt 6.1 gegebenen Definitionen entspricht, muss die offizielle SBOM auch der Prüfstelle zur Verfügung gestellt werden. In diesem Fall muss ein entsprechender Eintrag für die Drittanbieterkomponente in der SBOM für den TOE weggelassen werden.

90 Jeder SBOM-Eintrag muss der tatsächlich im Produkt enthaltenen Komponente entsprechen. Komponenten, die für Test- oder Debug-Varianten des Produkts verwendet werden, dürfen nicht in der von der Antragstellerin bereitgestellten SBOM enthalten sein.

91 Wenn eine bestimmte Komponente mehrmals im Produkt enthalten ist (z. B. eine bestimmte Version einer Softwarebibliothek, die in mehreren auf dem Produkt ausgeführten Anwendungen enthalten ist), ist nur ein entsprechender Eintrag in der SBOM erforderlich. Wenn hingegen mehrere verschiedene Versionen einer bestimmten Komponente von einer bestimmten Lieferantin im Produkt verwendet werden, muss für jede enthaltene Version der Komponente ein separater Eintrag erstellt werden.

6.1 Definition der SBOM

92 Eine SBOM ist eine Liste von Einträgen, die einem bestimmten Format entspricht, wobei jeder Eintrag Identifikationsinformationen über eine einzelne Komponente und möglicherweise weitere zugehörige Informationen enthält. Das für eine SBOM verwendete Format sollte entweder CycloneDX[2] (Version 1.4 oder höher) oder Software Package Data Exchange[3] (Version 2.3 oder höher) in einer beliebigen vom jeweiligen Format unterstützten Darstellung (z. B. JSON oder XML) sein.

93 Zusätzlich zur tatsächlichen Liste der Komponenteneinträge soll eine SBOM die folgenden Informationen enthalten:

Attribut	*Definition*	*Empfohlenes Formatfeld*	*Bemerkung*
Autorin	Name der Entität, die die SBOM erstellt hat.	SPDX: Creator/Creators[4] CycloneDX: "authors" property of "metadata" element[5]	Der Name der juristischen Person (z. B. der Unternehmensname) ist hinreichend als Autor-Information.
Zeitstempel	Datum und Zeit, wann die SBOM vom Autor erstellt wurde.	SPDX: Created[6] CycloneDX: "timestamp" property of "metadata" element[7]	Der Zeitstempel muss dem Format folgen, das durch das gewählte SBOM Format (z. B. SPDX oder CycloneDX) vorgeschrieben wird.

Tabelle 3: Notwendige Attribute für die Beschreibung einer SBOM

94 Eine Komponente ist eine Softwareeinheit, z. B. in Form einer Anwendung, einer Softwarebibliothek, eines Betriebssystems oder einer Firmware, die aus einer oder mehreren Dateien besteht. Der SBOM-Eintrag für jede Komponente muss mindestens die folgenden Informationen enthalten:

Attribut	*Definition*	*Empfohlenes Formatfeld*	*Bemerkungen*
Name der Lieferantin	Der Name der Entität, die die Komponente erstellt hat und/oder wartet.	SPDX: PackageSupplier[8] CycloneDX: "supplier" property of object under "components"[9]	Für proprietäre Komponenten ist der Name der juristischen Person (z. B. der Unternehmensname) hinreichend als Name der Lieferantin. Für Open Source Komponenten muss als Name der Lieferantin der Name der Entität, des Projektes oder Services bereitgestellt werden, von dem oder der die Komponente erhalten wurde, entweder als vorkompiliertes Paket oder als Quellcode (z. B. Python-Package Index, Debian, Ubuntu, Github).

[2] https://cyclonedx.org/specification/overview/
[3] https://spdx.dev/specifications/
[4] https://spdx.github.io/spdx-spec/v2.3/document-creation-information/#68-creator-field
[5] https://cyclonedx.org/docs/1.4/json/#metadata_authors
[6] https://spdx.github.io/spdx-spec/v2.3/document-creation-information/#69-created-field
[7] https://cyclonedx.org/docs/1.4/json/#metadata_timestamp
[8] https://spdx.github.io/spdx-spec/v2.3/package-information/#75-package-supplier-field
[9] https://cyclonedx.org/docs/1.4/json/#components_items_name

Attribut	*Definition*	*Empfohlenes Formatfeld*	*Bemerkungen*
Name der Komponente	Die der Komponente durch die Lieferantin zugeordnete Bezeichnung.	SPDX: PackageName**Fehler! Textmarke nicht definiert.** CycloneDX: "name" property of object under "components"**Fehler! Textmarke nicht definiert.**	Der angegebene Wert für dieses Feld soll den üblichsten und erkennbarsten Titel oder Namen der Komponente beschreiben.
Version der Komponente	Die durch die Lieferantin genutzte Kennung, um eine Änderung in der Software gegenüber der vorherig gekennzeichneten Version zu spezifizieren.	SPDX: PackageVersion**Fehler! Textmarke nicht definiert.** CycloneDX: "version" property of object under "components"**Fehler! Textmarke nicht definiert.**	Semantische Versionierung[10] sollte verwendet werden. Wenn keine offizielle Versionskennung für die beschriebene Komponente existiert, muss die Kennung der aktuellsten Version, auf die die beschriebene Komponente basiert, angegeben werden. Weiterhin muss die Antragstellerin eine Zusammenfassung der Änderungen zwischen der aktuellsten Version, auf der die beschriebene Komponente basiert, und der im SBOM-Eintrag beschriebenen Komponente in einem separaten Dokument zur Verfügung stellen.

Tabelle 4: Notwendige Attribute pro SBOM-Eintrag

95 Eine Komponente wird als "Drittanbieterkomponente" bezeichnet, wenn die Antragstellerin nicht die Bereitstellerin der Komponente ist.

96 Vorlagen, die zur Erstellung einer SBOM gemäß der obigen Definition verwendet werden können, sind auf Anfrage bei der Zertifizierungsstelle erhältlich. Diese Vorlagen enthalten die Mindestanzahl von Feldern in jeder SBOM-Repräsentation, die notwendig ist, um den oben genannten Anforderungen sowie denen des jeweiligen Formats zu entsprechen. Jeder Platzhalter in der Vorlage muss durch einen korrekten Eintrag ersetzt werden, der den Anforderungen des entsprechenden Formats entspricht.

[10] https://semver.org

6.2 Optionaler Schwachstellenbericht

97 Als Ergänzung zu jeder SBOM, die der Prüfstelle zur Verfügung gestellt wird, kann die Antragstellerin einen Schwachstellenbericht für eine oder mehrere in der SBOM aufgeführte Komponenten bereitstellen. Jeder solche Schwachstellenbericht sollte Schwachstellen umfassen, die im öffentlich verfügbaren CVE-Datensatz aufgeführt sind und auf die jeweilige Komponente zutreffen, sowie Schwachstellen, die nicht öffentlich aufgeführt sind. Es ist ratsam, einen Schwachstellenbericht einzureichen, um die Evaluierung zu beschleunigen, insbesondere wenn bekannt ist, dass Komponenten mit Schwachstellen im TOE vorhanden sind.

98 Für jede im Schwachstellenbericht für die jeweilige Komponente aufgeführte Schwachstelle sollte die Antragstellerin folgende Informationen bereitstellen:

Attribut	***Definition***	***Bemerkungen***
Kennung der Schwachstelle	Eine eindeutige Bezeichnung oder verwendete Verfolgungs-ID, um die Schwachstelle zu identifizieren.	Falls vorhanden, muss die MITRE Standard „Common Vulnerabilities and Exposures“ (CVE) Verfolgungsnummer für diese Schwachstelle angegeben werden.
Status der Schwachstelle	Eine Aussage über den Status der Schwachstelle, die entweder „Fixed“, „Not affected“, „Affected“ oder „Under investigation“ sein kann.	Eine Aussage kann folgende Bedeutungen tragen. • Behoben (fixed): Die referenzierte Schwachstelle wurde in dieser Version der Komponente behoben. • Nicht betroffen (not affected): Die referenzierte Schwachstelle kann für den gegebenen TOE nicht ausgenutzt werden (z. B. aufgrund von Korrekturen in anderen Komponenten oder da die betreffenden Funktionalitäten deaktiviert sind). • Betroffen (affected): Die referenzierte Schwachstelle kann für den gegebenen TOE ausgenutzt werden. • In Überprüfung (under investigation): Der Antragstellerin ist derzeit nicht bekannt, ob die Schwachstelle für den gegebenen TOE ausgenutzt werden kann.
Bemerkungen	Erklärungen bezüglich des Status der Schwachstellen.	Wenn “Not affected” als Status für eine Schwachstelle gemeldet wird, muss eine kurze Begründung hierfür vorgelegt werden. Für andere Status kann eine kurze Begründung vorgelegt werden.

Tabelle 5: Notwendige Attribute für einen Schwachstellenbericht

99 Das Format des Berichts kann dem VEX-Profil[11] des "Common Security Advisory Framework" (Version 2.0 oder höher) oder der "vulnerability" Eigenschaft entsprechen.[12].

[11] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#45-profile-5-vex
[12] https://cyclonedx.org/docs/1.4/json/#vulnerabilities

7 Referenzdokumente

1 [SCES-ACM] SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, aktuelle Version

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

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

4 [BITV 2.0] Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0)

5 [AIS B 6] Anwendungshinweise und Interpretationen zum Schema (AIS): Anforderungen an einen TOE

6 [ST Vorlage] ST Vorlage für den BSZ-Geltungsbereich "Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte"